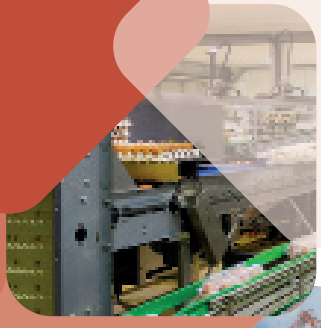
gli autori

LUCA FIORENTINI, ROSARIO SICARI

# ANALISI, VALUTAZIONE E GESTIONE OPERATIVA DEL RISCHIO

*Bow-Tie, Root Cause Analysis ed altri strumenti conformi alla ISO 31000 per la gestione sistemica del rischio nelle organizzazioni*

vai alla scheda del libro



EPC EDITORE

LUCA FIORENTINI, ROSARIO SICARI

# ANALISI, VALUTAZIONE E GESTIONE OPERATIVA DEL RISCHIO

*Bow-Tie, Root Cause Analysis ed altri strumenti conformi alla ISO 31000 per la gestione sistemica del rischio nelle organizzazioni*

EPC EDITORE

**ANALISI, VALUTAZIONE E GESTIONE OPERATIVA DEL RISCHIO**
ISBN 978-88-6310-920-7



Via Clauzetto, 12 - 00188 Roma

Servizio clienti: Tel. 06 33245277 - Fax: 06 33245248

Redazione: Tel. 06 33245264/205 - www.epc.it



Il codice QR che si trova sul retro della copertina, consente attraverso uno smartphone di accedere direttamente alle informazioni e agli eventuali aggiornamenti di questo volume.

Le stesse informazioni sono disponibili alla pagina:

https://www.epc.it/Prodotto/Editoria/Libri/Analisi-valutazione-e-gestione-operativa-del-rischio/4810

# INDICE GENERALE

CAPITOLO 5



CAPITOLO 6

*Pagine omesse dall’anteprima del volume*

CAPITOLO 1

# INTRODUZIONE

## 1.1 Intenti del libro

Questo libro intende avere una duplice valenza. Da un lato si propone come guida metodologica su due aspetti complementari della sicurezza: l'analisi e la valutazione del rischio e la valorizzazione dell'esperienza operativa attraverso lo studio di eventi incidentali e quasi incidenti. Dall'altro lato, intende essere un manuale introduttivo all'utilizzo dei principali metodi correlati a tali aspetti, fornendo così quelle conoscenze (sia di base che avanzate) che il lettore potrà anche sfruttare nell'utilizzo dei principali software in commercio, quali *BowTieXP* e *IncidentXP* di *CGE Risk Management Solutions*®, giudicati essere, dagli autori, ottimi strumenti sia per la didattica sia per la produttività.

Il volume medesimo risulta pertanto suddiviso in due parti, tra loro correlate, che possono essere tuttavia affrontate, secondo le esigenze specifiche del lettore, anche in ordine inverso. La prima parte è dedicata all'analisi e gestione del rischio con il metodo *Bow-Tie*. Il *Bow-Tie* è oggi uno dei metodi più diffusi per l'analisi del rischio. La sua forza risiede principalmente nella sua intuitiva e potente notazione grafica, che assicura una ineguagliabile capacità comunicativa nel trasmettere in maniera facile ed immediata le informazioni ivi contenute sia agli addetti ai lavori sia a tutti i portatori di interesse *("stakeholders")* presenti nella organizzazione e coinvolti a vario titolo nei processi decisionali e di gestione dei rischi, oltre che eventuali soggetti esterni altresì portatori di interesse. Tuttavia, considerare il *Bow-Tie* come un mero, pur potente, strumento di visualizzazione grafica della mappa dei rischi della organizzazione è assai riduttivo, come si mostrerà al lettore.

La definizione di una corretta strategia di gestione del rischio non può prescindere dalla valutazione di esso e naturalmente deve quindi essere condotta attraverso una serie di passaggi fondamentali ed ineludibili: analisi delle cause, identificazione delle conseguenze, individuazione delle barriere (tecniche ed organizzativo-gestionali) atte a prevenire o a mitigare

i pericoli, individuare le criticità del sistema in esame, creando parallelamente alternative di pianificazione strategica (la progettazione orientata all'ottenimento ed alla garanzia della prestazione). Risultano avere un ruolo fondamentale i livelli di protezione indipendenti ("barriere"), sia tecnici sia organizzativo-gestionali, sia intesi come misure preventive, sia intesi come misure mitigative delle conseguenze, ben rappresentate in un diagramma di valutazione *"Bow-Tie"*.

Questo libro intende illustrare dettagliatamente la metodologia *Bow-Tie*, oggi tra le più diffuse nel campo dell'analisi del rischio, unitamente a quegli aspetti a corredo che completano tale metodo. Verranno quindi trattati non solo la creazione dei diagrammi *Bow-Tie*, ma anche la loro valutazione quantitativa (integrando l'analisi LOPA), la tassonomia e, più in generale, la loro gestione nel tempo.

Parallelamente, il paradigma del miglioramento continuo dei sistemi di gestione impone alle organizzazioni di individuare le opportunità di miglioramento derivanti da incidenti, *"near miss"* o, più in generale, non conformità ed anomalie, al fine di sviluppare le azioni correttive da porre in essere per evitare il ripetersi di simili accadimenti. Una ricomposizione organica degli elementi che hanno caratterizzato l'evento negativo può essere ottenuta solamente adottando un approccio ingegneristico, strutturato e ad approfondimento crescente a partire dai principi che governano l'instaurarsi del pericolo, con chiaro riferimento alla valutazione del rischio ed allo studio del fattore umano, la cui conoscenza è oggi imprescindibile per non derubricare i fallimenti umani come "errori" e mantenere quindi intatta la possibilità di migliorare le prestazioni umane, in termini di affidabilità, a partire da una ricognizione dei fattori che ne determinano il risultato.

La seconda parte di questo libro illustra i principali strumenti di analisi degli incidenti, quasi-incidenti (o *near miss*), e non conformità (o anomalie), prendendo le mosse dai requisiti imposti dalle norme tecniche sui sistemi di gestione (ISO 45001, ISO 9001, ISO 14001 e altre) e dalle norme del nostro Paese in tema di salute e sicurezza (D.Lgs. 81/2008), rischio industriale (D.Lgs. 105/2015 e D.Lgs. 145/2015), prevenzione incendi (D.P.R. 151/2011, D.M. 3 agosto 2015, D.M. 7 agosto 2012, D.M. 9 maggio 2007) e di responsabilità amministrativa delle persone giuridiche (D.Lgs. 231/2001), tenendo conto della necessità per le organizzazioni di adottare un sistema di valorizzazione dell'esperienza operativa ed in particolare degli accadimenti negativi. Vengono quindi approfondite le metodologie più diffuse nel campo, incluse la *Root Cause Analysis* (RCA), *Tripod Beta* e la *Barrier Failure Analysis* (BFA).

Queste metodologie vengono oggi di gran lunga impiegate nei settori dell'industria chimica, petrolchimica, dell'energia, delle infrastrutture di trasporto, dell'aviazione e del mondo ospedaliero; tuttavia le informazioni e le metodologie discusse all'interno di questo libro, per via della loro universalità, sono applicabili a qualsiasi organizzazione, indipendentemente da tipo, entità, dimensione e complessità della stessa. I principi su cui si fonda la gestione del

rischio sono infatti indipendenti dal contesto di applicazione e tale attributo è anche condiviso con la struttura e il processo di gestione del rischio, a cui si applicano le metodologie qui presentate.

## 1.2 A chi è rivolto il libro

Il libro si rivolge ai professionisti operanti nel settore della sicurezza, sia nell'ambito di realtà aziendali strutturate che di singoli liberi professionisti. Le metodologie qui discusse sono applicabili a diversi settori dell'industria, dall'*Oil&Gas* alla sicurezza alimentare, dall'*Health Care alla Power Industry*, dalla sicurezza sui luoghi di lavoro all'aviazione, e così via. Per tale motivo, nella trattazione di questo libro si è cercato di preservare l'universalità dei contenuti, presentando dapprima i concetti in modo generale, attraverso definizioni svincolate dal contesto applicativo, salvo presentare, solo successivamente, degli esempi applicativi in determinati contesti di business.

## 1.3 Strumenti applicativi consigliati

Il lettore è incoraggiato ad applicare le nozioni apprese sulle metodologie trattate in questo libro, scaricando la versione dimostrativa di *BowTieXP* e *IncidentXP* di CGE *Risk Management* dal sito https://www.cgerisk.com.


Si tratta dei software tra i più diffusi al mondo per la creazione e la gestione dei *Bow-Tie* e l'analisi degli incidenti. Questo libro intende sia aiutare il lettore novizio a muovere i primi passi con il software che fornire una guida per un utilizzo che sfrutti al meglio tutte le potenzialità del software per la creazione di un sistema di gestione della sicurezza da una prospettiva *risk-based* basata sul *barrier thinking*.

In Appendice A sono riportate alcune schede sinottiche che sintetizzano i principali elementi chiave delle metodologie trattate in questo libro e che l'autore potrà trovare utili anche durante l'impiego dei software.

Questo libro è parte integrante del materiale didattico dei corsi di formazione promossi da Istituto Informa con TECSA S.r.l. e CHAOS Consulting S.r.l. sull'analisi e gestione del rischio con il metodo *Bow-Tie* e sull'analisi dell'esperienza operativa delle organizzazioni.

Di seguito si riportano i riferimenti delle due società, cui gli autori del presente volume fanno riferimento, coinvolte nella diffusione delle metodologie illustrate.


TECSA S.r.l. – Via Figino, 101 – 20016 Pero (MI)
e-mail: tecsa@tecsasrl.it – web: www.tecsasrl.it


CHAOS Consulting S.r.l. – Via dei Martiri, 3 – 20017 Rho (MI)
e-mail: info@chaosconsulting.it – web: www.chaosconsulting.it

*Pagine omesse dall’anteprima del volume*

Di contro, queste metodologie possono essere utilizzate per identificare solo singoli modi di guasto e non loro combinazioni. Infine, la loro applicazione richiede sovente molto tempo e si può rivelare difficile e tediosa per sistemi particolarmente complessi.

## 3.3 Analisi del rischio (risk analysis)

In questo paragrafo vengono presentate alcune metodologie generalmente impiegate nella fase di analisi del rischio, fermo restando la loro applicabilità (più o meno raccomandata) alle altri fasi del "*risk assessment".* Poiché generalmente le attività di analisi del rischio necessitano di un approccio "quantitativo" si sono selezionati alcuni metodi, citati dalla ISO 31010, che consentono approfondimenti numerici, anche, eventualmente quale approfondimento di studi qualitativi iniziali quali HAZID e HAZOP.

### *3.3.1 Albero dei guasti*

Questo metodo, creato nei laboratori della Bell Telephone agli inizi degli anni '60, mira a ricostruire l'esatta sequenza di eventi primari ed intermedi che portano ad un *top event* (ad es. il fallimento di un sistema o l'esecuzione di un errore nel corso di sistemi umani). È pertanto utile per riconoscere quelle situazioni che possono generare conseguenze indesiderate se combinate con alcuni eventi specificatamente identificati. La struttura tipica di un albero dei guasti (*Fault Tree Analysis* – FTA) è mostrata in Figura 3.1.


**Figura 3.1** – *Struttura base di un albero dei guasti*

La FTA è una tecnica analitica deduttiva per analizzare i guasti. Essa si concentra su un particolare evento indesiderato e cerca di determinarne le cause. In un albero dei guasti, l'evento indesiderato è detto "*top event":* generalmente si tratta di un fallimento completo (e

catastrofico) del sistema oggetto di analisi. Il top event rappresenta quindi l'effetto finale, ma è il punto di partenza di una FTA. Ciò rende chiaro il perché la formulazione del *top event* debba essere puntuale ed esaustiva: questo assicurerà la bontà dei risultati forniti dalla FTA. La schematizzazione grafica della FTA, ovvero l'albero dei guasti, è una rappresentazione delle catene di fallimenti, siano esse in parallelo o sequenziali, che conducono alla manifestazione dell'evento indesiderato predefinito (cioè il *top event*). Tipicamente, ogni guasto in una FTA è il risultato della combinazione dei fallimenti di sottosistemi (come guasti meccanici o errori umani) con le barriere inefficaci, mancanti o fallite poste per fermare la sequenza incidentale, rivelatesi incapaci di assolvere al loro compito per una determinata ragione.

È importante sottolineare che un albero dei guasti non tiene in conto di tutti i possibili fallimenti del sistema o di tutte le possibili cause potenzialmente alla base dell'evento analizzato. Invero, ogni albero dei guasti è progettato per un particolare *top event* che rappresenta il punto di partenza che definirà lo sviluppo del resto dell'albero: solo i modi di guasto che danno un contributo alla definizione del top event sono presi in considerazione. Ogni singolo guasto in una FTA è posto in combinazione con gli altri tramite porte logiche AND/OR. Altri operatori Booleani possono essere utilizzati, ma generalmente ciò non è richiesto. L'uso di connettori logici si rivela utile quando un singolo evento potrebbe essere causato da uno o più fattori che devono agire allo stesso tempo.

Una volta che il *top event* è identificato, l'analisi dei guasti procede gradualmente livello dopo livello. La tecnica è anche usata per l'analisi degli incidenti, di cui si dirà meglio nel capitolo 6 di questo libro: posto l'evento come *top event,* dapprima vengono considerate le possibili e più generiche cause immediate, sempre con il supporto delle evidenze raccolte. Potenziali guasti inizialmente esclusi perché non supportati dalle prime evidenze raccolte possono essere ulteriormente investigati, arrivando così a definire il secondo livello di cause. Il processo iterativo continua in questo modo anche quando la FTA è usata come strumento di analisi del rischio e si arresta quando i guasti identificati alle estremità delle ramificazioni sono considerati sufficientemente dettagliati, nel rispetto dello scopo, dell'ambito e del contesto definiti fin dall'inizio del processo di analisi.

Potrebbe anche accadere che tra un insieme di stessi eventi iniziatori (guasti all'origine) ed il *top event* vengano identificati più di un unico percorso. Quando ciò accade, il percorso più realistico tra viene definito *"minimum cut-set"* e coincide tipicamente con quello più breve tra i due estremi.

Un esempio di albero dei guasti (nella sua parte superiore) è mostrato in Figura 3.2.

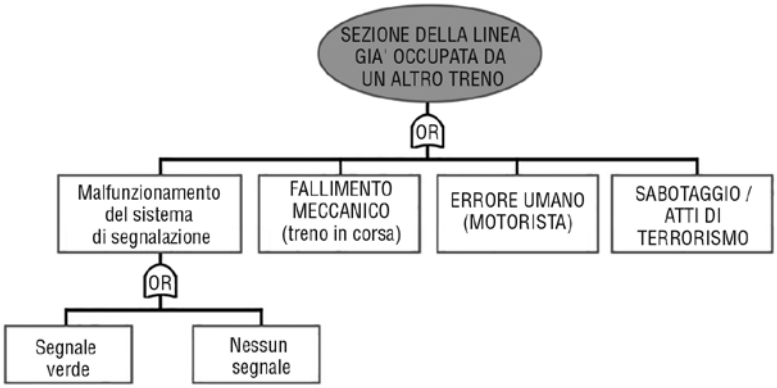



**Figura 3.2** – *Esempio di albero dei Guasti*

Gli alberi dei guasti, che possono essere considerati come il "contrario" dei diagrammi FMEA, sono usati per guidare l'analista di rischio attraverso un processo strutturato mirato ad identificare le possibili cause di un evento e tale funzione risulta altrettanto utile all'ingegnere forense che può così indirizzare i propri sforzi investigativi nelle cause più probabili.

La tecnica FTA ben si presta ad analizzare sistemi complessi riconducibili ad un insieme di componenti per i quali sono note le relazioni intercorrenti. Ciò, di fatto, consente anche una valutazione circa eventuali cause comuni di guasto riconducibili a componenti presenti in più sotto-sistemi o soggetti ad analoghe modalità di guasto.

Fino a questo momento, la descrizione dell'albero dei guasti sembra definire un'analisi di tipo qualitativo. Sebbene sia possibile lasciare l'albero dei guasti senza alcuna valorizzazione di tipo numerico, si ottengono vantaggi significativi se esso viene usato in un approccio quantitativo. Le probabilità di fallimento possono essere ottenute da database di dati storici (quando disponibili) o da linee guida fornite dai produttori del sistema in esame, o da pubblicazioni indipendenti. Ancora è possibile derivare queste informazioni numeriche dalla analisi statistica della esperienza operativa propria della organizzazione, eventualmente con stime fondate su metodi stocastici (es. Monte Carlo). Ovviamente, l'analista di rischio può oggi contare su un buon numero di software che eseguono, e quantificano, la FTA. I dati numerici sulle probabilità di errori umani, fallimenti di componenti o fattori ambientali sono combinati usando le regole matematiche della probabilità, a seconda delle porte logiche su cui convergono più cause. Per esempio, una porta "AND" implica che tutti i fattori precedentemente analizzati devono manifestarsi affinché possa generarsi l'evento successivo. Da un punto di vista probabilistico, ciò si traduce in una singola probabilità dell'evento successivo, ottenuta dalla moltiplicazione di tutte le probabilità delle singole cause che afferiscono alla medesima porta "AND", in accordo alle regole della probabilità combinata, nell'ipotesi di eventi iniziatori indipendenti). Invece, se la connessione avviene attraverso una porta "OR", la probabilità dell'evento risultante è uguale alla somma delle probabilità delle singole cause. Procedendo in

questo modo, si trova la probabilità di accadimento del *top event*. Nell'analisi del rischio, tale informazione si combina con la frequenza di accadimento delle cause iniziatrici, per avere la frequenza di accadimento (in termini di occasioni/anno) del *top event*. Tale dato è poi usato in combinazione con la sua severità (ottenuta, per esempio, da simulazioni numeriche nell'ambito di un approccio quantitativo) per valutare il rischio finale del *top event*.

Emerge chiaramente come la FTA sia uno strumento analitico per la definizione delle relazioni; esso non fornisce direttamente alcun dato numerico o alcuna informazione su come sviluppare l'albero. La forza dell'albero dei guasti, anche quando usato secondo un approccio qualitativo, risiede nella sua abilità di decomporre un evento nei suoi eventi iniziatori.

La conduzione di una FTA prevede quindi le seguenti fasi:

- definizione del *top event*;
- identificazione del primo strato di cause del *top event*, considerando componenti e procedure base;
- definire le relazioni tra il *top event* ed il primo strato di input, attraverso una o più porte logiche;
- valutare ogni elemento del primo strato identificando i propri input (secondo strato);
- definire le relazioni tra ogni singolo elemento del primo strato ed i propri input del secondo strato, tramite una o più porte logiche;
- continuare con questo processo per gli strati successivi, fino a quando il livello raggiunto viene considerato soddisfacente;
- se necessario, raccogliere informazioni addizionali per completare, integrare o eliminare alcuni rami o singoli elementi dell'albero;
- documentare i risultati della FTA in un *report*, evidenziando il *minimum cut-set,* le probabilità e le frequenze ottenute.

Nel seguito viene mostrato un esempio contestualizzato all'industria di processo ambito tipico di utilizzo degli alberi di guasto per la stima delle frequenze di accadimento di una ipotesi incidentale come prescritto dal corpo normativo vigente in materia di rischio industriale, che, ai fini della valutazione di accettabilità degli eventi incidentali, richiede la comparazione tra la frequenza attesa ed una frequenza di riferimento; traguardo positivo che garantisce la non necessità di effettuare calcolazioni circa gli effetti. Si consideri il sistema di stoccaggio di liquido infiammabile riportato in Figura 3.3. Il sistema è tenuto sotto pressione in azoto e viene usato un controllore di pressione per mantenere la pressione entro certi limiti operativi, altrimenti viene inviato un segnale di allarme in sala controllo. La valvola di sicurezza RV-1 apre all'atmosfera in caso di emergenza. La rottura del serbatoio per sovrapressione è il *top event* che si intende analizzare: il corrispondente albero dei guasti è mostrato in Figura 3.4.

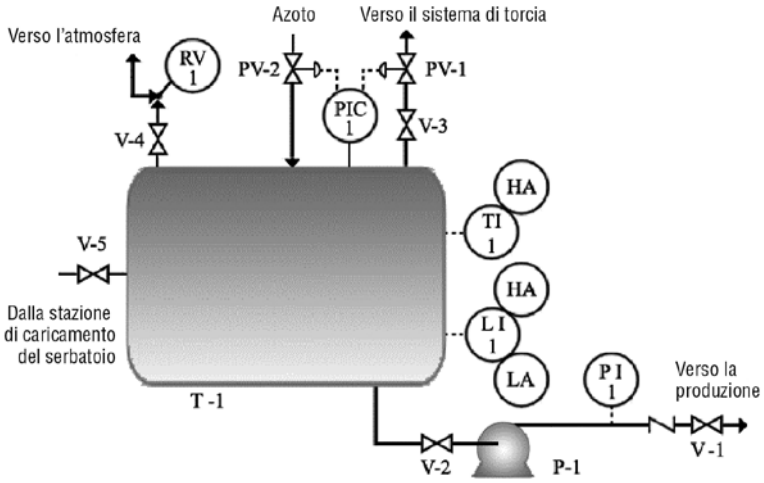



**Figura 3.3** – *Sistema di stoccaggio di liquido infiammabile (adattata da Fiorentini e Marmo, "Principles of Forensic Engineering applied to Industrial Accidents", Wiley, 2018)*

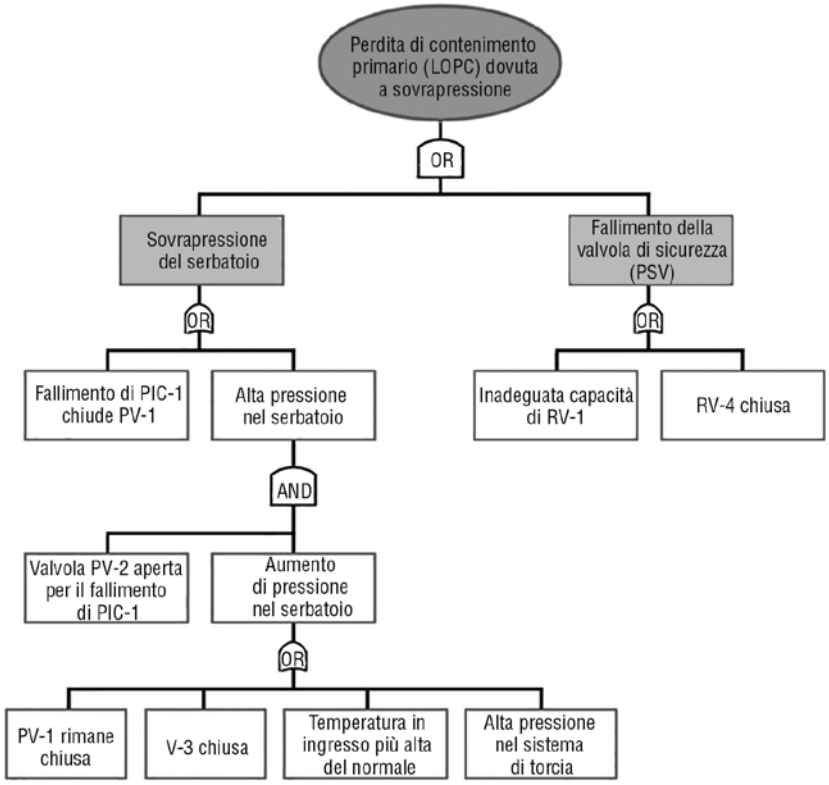



**Figura 3.4** – *Esempio di FTA relativa al top event "rottura serbatoio per sovrapressione"*

### 3.3.2 Albero degli eventi

L'albero degli eventi (*Event Tree Analysis* – ETA) è una tecnica, peraltro spesso impiegata a valle della definizione delle ipotesi incidentali con FTA per individuare gli eventi potenziali al variare delle condizioni al contorno, che permette di determinare le conseguenze potenziali di un evento iniziatore, in termini di scenari incidentali. Lo scopo della ETA è pertanto complementare a quello della FTA. Invero, una FTA spiega come un evento indesiderato possa essere il frutto di una serie di guasti nei sottosistemi che compongono il sistema analizzato, mentre la ETA esamina tutte le possibili conseguenze di tale evento indesiderato.

La struttura tipica di un albero degli eventi è riportata in Figura 3.5.

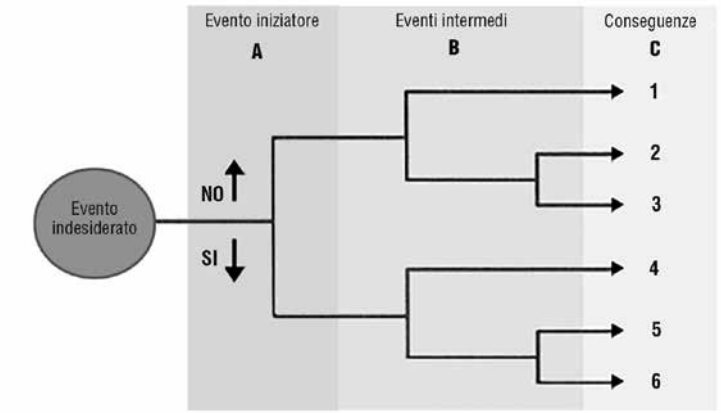



**Figura 3.5** – *La struttura di un tipico albero degli eventi (adattata da Fiorentini e Marmo, "Principles of Forensic Engineering applied to Industrial Accidents", Wiley, 2018)*

Questa tecnica è tra le più difficili da applicare nella pratica. Infatti, è possibile ottenere risultati significativi solo se gli eventi indesiderati (o persino desiderati) che portano alla ramificazione dell'albero (le condizioni al contorno) sono totalmente noti a priori. È pertanto chiaro che l'applicazione di questo metodo richiede una solida esperienza pratica, in modo tale da anticipare tutti i possibili eventi del sistema e di esplorare tutte le possibili conseguenze di tali eventi.

La sequenza degli accadimenti è generalmente definita dalle barriere che possono aver successo oppure no. Un esempio di ETA è mostrato in Figura 3.6.

L'ETA è una eccellente metodologia per l'analisi dei rischi, essendo impiegata per identificare i possibili scenari incidentali. Nell'ambito di una investigazione di un evento, si è soliti evidenziare il reale percorso sull'albero degli eventi che ha condotto alla manifestazione dello scenario, come fatto ad esempio in Figura 3.6.

Adottando un approccio quantitativo fondato sulla valorizzazione numerica, la frequenza di accadimento di ogni scenario incidentale è determinata a partire dalla frequenza dell'evento iniziatore. Tale dato è poi combinato con le probabilità accadimento degli eventi intermedi

(ad es. le probabilità di fallimento delle barriere) messi in corrispondenza dei nodi dell'albero, da dove quindi verranno prodotte le ramificazioni.

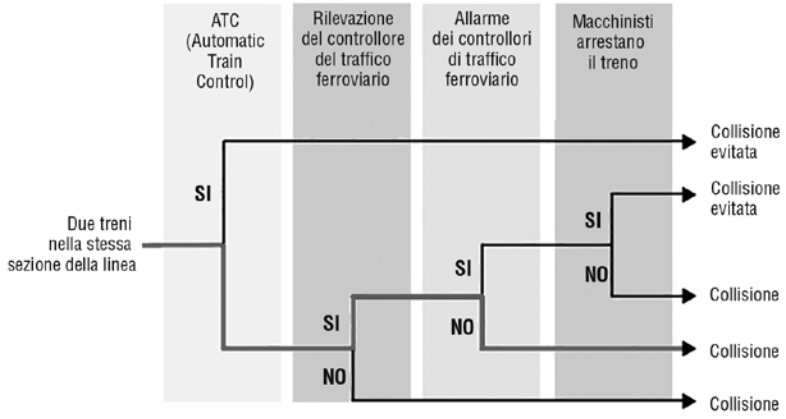



**Figura 3.6** – *Esempio di albero degli eventi per l'analisi di un incidente ferroviario (adattata da Fiorentini e Marmo, "Principles of Forensic Engineering applied to Industrial Accidents", Wiley, 2018)*

Anche in questo caso, così come visto per la FTA, si usano le regole della probabilità combinata. Spesso, la probabilità di accadimento dell'evento iniziatore (o anche le probabilità associate alle condizioni al contorno rispetto alle quali si vuole valutare la variabilità degli eventi) è ottenuta proprio da una FTA: in altre parole il *top event* di un albero dei guasti è il punto di partenza di un albero degli eventi. La combinazione dei due metodi costituisce il *"Bow-Tie"*, un ulteriore metodo di analisi del rischio che mira alla piena comprensione di un evento indesiderato, sia guardando alle sue cause (come per una FTA) che alle sue possibili conseguenze (come per una ETA). Si dirà di più sui *Bow-Tie* al paragrafo 3.3.4.1 e al Capitolo 4 e 5 di questo libro avendo gli autori del volume individuato questa metodologia quale la maggiormente idonea per la messa a punto di un sistema di gestione del rischio conforme alla ISO 31000 ad implementazione e grado di approfondimento progressivi rispetto a diversi ambiti di applicazione.

Una volta nota la probabilità di accadimento di un evento intermedio (nel caso di barriere, la probabilità di fallimento su domanda), la probabilità di non accadimento è data dal complemento a uno di tale valore. In altre parole, la probabilità che o la barriera fallisca o non fallisca è uno.

Consideriamo la tubazione connessa al serbatoio mostrata in Figura 3.7. Si vogliono analizzare le possibili conseguenze della rottura della tubazione nel punto "P". Il sistema è dotato di una *Excessive Flow Valve* (EFV) e di una valvola di segregazione controllata in remoto *(Remote Controlled isolation valve)*. L'albero degli eventi risultante è in Figura 3.8. In esso, la rottura della tubazione è l'evento indesiderato (A), con una probabilità PA, mentre il fallimento della EFV è un evento intermedio (B) con probabilità PB, al pari del fallimento della RCV che ha probabilità PC.

In accordo all'albero degli eventi sviluppato, la probabilità di una perdita continua è data da PA × PB × PC; la probabilità di una perdita di liquido fino ala chiusura della RCV è PA × PB × (1-PC); infine, la probabilità di una perdita minore è PA × (1-PB).

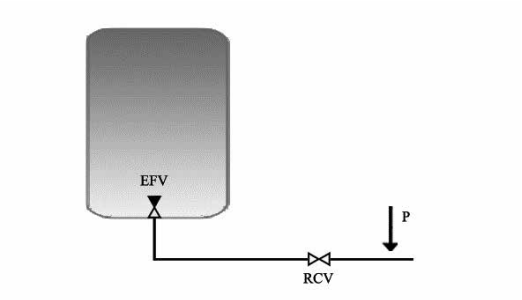



**Figura 3.7** – *Tubazione connessa ad un serbatoio (adattata da Fiorentini e Marmo, "Principles of Forensic Engineering applied to Industrial Accidents", Wiley, 2018)*

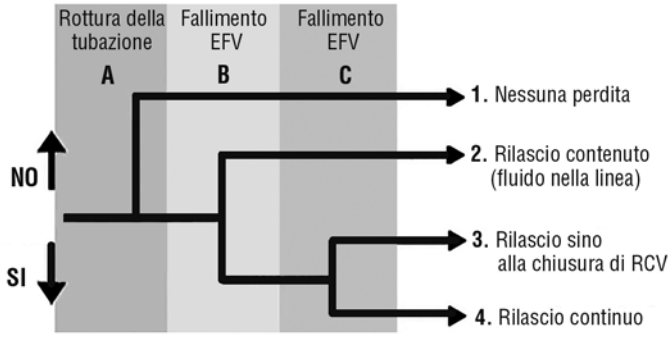



**Figura 3.8** – *Esempio di un albero degli eventi (adattata da Fiorentini e Marmo, "Principles of Forensic Engineering applied to Industrial Accidents", Wiley, 2018)*

### 3.3.3 Human Reliability Analysis (HRA)

La *Human Reliability Analysis* (HRA), ancorché possa dirsi non una singola metodologia quanto un compendio combinato di metodi e tecniche più o meno analitici anche impiegati in combinazione tra loro, consente di valutare l'impatto dell'uomo sulle prestazioni del sistema e può essere utilizzata per valutare l'influenza dell'errore umano sul sistema oggetto di analisi.

Molti processi sono potenzialmente esposti all'errore umano; si pensi, ad esempio, ai processi dove il tempo disponibile all'operatore per prendere una decisione è limitato. La probabilità che i problemi derivanti si sviluppino fino a diventare sufficientemente seri può anche essere bassa; tuttavia, l'azione umana è talvolta l'unica barriera capace di interrompere il progredire degli eventi che da un evento iniziatore porta ad un incidente. Anche per questo

motivo è cruciale analizzare il comportamento umano. A questo esempio si vanno ad aggiungere tutti quei casi in cui:

- gli operatori svolgono una attività critica (es. una procedura operativa complessa);
- agli operatori è demandata la sorveglianza o le attività di ispezione, controllo e manutenzione periodici di un sistema tecnico critico. La probabilità di fallimento su domande di componenti e sistemi tecnici potrebbe essere determinato proprio dalla efficacia del fattore umano in queste situazioni.

L'importanza della HRA è emersa in modo evidente nell'ambito dello studio di diversi incidenti in cui errori umani hanno contribuito in maniera critica alla catastrofica sequenza di eventi. Tali incidenti sono un monito rispetto a valutazioni del rischio che si concentrano esclusivamente sulle parti hardware e software di un sistema, trascurando l'influenza del fattore umano (sia come causazione di un evento sia come mancata o non efficace risposta ad una deviazione). Inoltre, gli studi HRA sono utili per evidenziare quegli errori che ostacolano la produttività, rivelando altresì i modi in cui questi errori e altri guasti (hardware e software) possono essere ripristinati dall'intervento di operatori e personale di manutenzione.

La HRA può essere condotta qualitativamente o quantitativamente. Nel primo caso, è usata per identificare il potenziale di errori umani e le loro cause, con l'obiettivo di ridurre poi la probabilità di errore. La HRA quantitativa è invece usata per fornire dati sui fallimenti umani ad una *Fault Tree Analysis* (FTA – Albero dei guasti) o altre tecniche.

L'esecuzione di una HRA richiede che siano fornite una serie di informazioni in ingresso:

- informazioni per definire i compiti che le persone dovrebbero eseguire;
- esperienza dei tipi di errore che accadono nella pratica aziendale rispetto al contesto preso a riferimento;
- competenza sul tema dell'errore umano e sulla sua quantificazione.

Il processo di conduzione di una HRA prevede le seguenti fasi:

- definizione del problema. Fino a dove occorre spingere l'analisi? Quali comportamenti/azioni dell'uomo vanno incluse e quali no?
- analisi del compito (spesso definito come *"task"*). Come dovrà essere eseguito il compito affidato all'uomo e quali tipi di aiuto saranno richiesti per supportare una buona prestazione?
- analisi dell'errore umano. In che modo l'esecuzione del compito può fallire (e la sua performance essere degradata)? Quali errori possono manifestarsi e come possono essere identificati e/o ripristinati?
- rappresentazione. Come questi errori possono essere integrati in altri hardware, software o eventi ambientali per consentire la quantificazione della probabilità di fallimento del sistema nella sua interezza?

- screening. Ci sono errori o compiti che non richiedono una quantificazione dettagliata?
- quantificazione. Quanto probabili sono gli errori umani? È sufficiente ipotizzare un ordine di grandezza?
- valutazione dell'impatto. Quali errori sono più importanti? Ad esempio, quali danno il maggior contributo nella definizione del rischio o dell'affidabilità?
- riduzione dell'errore. Come può essere raggiunta una più alta affidabilità sul comportamento umano?
- socumentazione. Quali dettagli della HRA devono essere documentati? Quali sono i limiti di validità della analisi e le giustificazioni delle assunzioni?

In esito a tale processo, la HRA fornisce le seguenti risultanze informative:

- una lista di errori umani che possono accadere e dei metodi con cui essi possono essere ridotti (preferibilmente, attraverso la riprogettazione del sistema);
- i modi e tipi di errore, le loro cause e conseguenze;
- una valutazione qualitativa o quantitativa del rischio connesso agli errori analizzati espresso come combinazione della probabilità di occorrenza e degli effetti diretti ed indiretti.

La HRA si presenta quindi come un metodo formale per includere l'errore umano all'interno della valutazione dei rischi associati con quei sistemi ove gli umani giocano spesso un ruolo importante. Tuttavia, la complessità e variabilità del comportamento umano possono rendere difficoltosa la definizione dei modi di fallimento o della probabilità associata al loro manifestarsi. Inoltre, molteplici attività degli umani non possono essere schematizzate secondo un semplice modello di "successo/fallimento", "on/off", "1/0"; ne consegue che l'applicazione della HRA può rivelarsi tediosa quando si analizzano problemi legati ad aspetti di qualità, di scarso "decision-making" e, più in generale, di fallimenti parziali.

Vista la complessità dell'argomento, approfondimenti di dettaglio sono forniti nel Capitolo 7 di questo libro.

Vale tuttavia la pena evidenziare che uno degli obiettivi principali di una HRA applicata ad un sistema tecnico è comprendere anche se esiste un equilibrio tra componenti e fattore umano, garanzia di resilienza di un sistema complesso.

### 3.3.4 Metodi basati sul concetto di barriere

La gestione del rischio una volta completate analisi del contesto e valutazione dei rischi si traduce quasi interamente nella gestione delle misure di controllo del rischio, ovvero delle barriere. Gestire il rischio nel tempo, assicurandosi che esso rimanga entro certi valori di accettabilità, significa di fatto assicurarsi che le misure poste in essere dall'organizzazione per contenere il rischio restino integre, efficaci ed efficienti nel tempo. Partendo da semplice

riflessione, vengono qui presentati due metodi di analisi del rischio basati sul concetto di barriere. Essi offrono quindi una prospettiva diversa della gestione del rischio, ponendosi come strumenti a supporto di un intero sistema di gestione del rischio che intenda adottare la prospettiva *barrier-based* che va affermandosi non solo nelle norme tecniche di adozione volontaria, come quelle citate al Capitolo 2, ma anche nelle leggi degli stati sovrani (si pensi, come recente esempio, all'obbligo imposto dalla L. 132/2018 di redazione del Piano di Emergenza Interno per i gestori degli impianti di stoccaggio e lavorazione dei rifiuti, ove si parla esplicitamente di individuazione e gestione delle misure di controllo del rischio). La barriera è quindi una misura di controllo o raggruppamento di elementi di controllo che, di per sé, può prevenire lo sviluppo di una causa in un *top event* (barriera preventiva) o può mitigare le conseguenze del *top event* una volta che questo si è manifestato (barriera mitigativa).

### *3.3.4.1 Bow-Tie*

Il *Bow-Tie*, grazie alla sua potente capacità di comunicare le informazioni graficamente, si è affermato come la tecnica principe di analisi del rischio basata sul concetto di barriere. Ad esso, quale metodologia privilegiata dagli autori del volume per la illustrazione dei principi della ISO 31000, sono dedicati interamente i Capitoli 4 e 5 di questo libro; in questo paragrafo si vuole quindi fornire una semplice introduzione al metodo.

La tecnica *Bow-Tie* prevede lo sviluppo di diagrammi logici di flusso sviluppati in tre zone distinte. Un esempio di diagramma *Bow-Tie* è riportato in Figura 3.9.

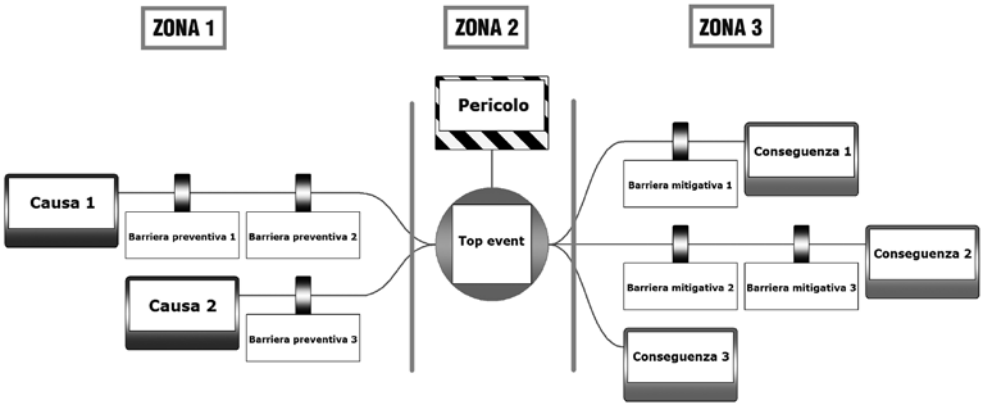



**Figura 3.9** – *Struttura Diagramma Bow-Tie*

- La **Zona 1** (Prevenzione) è rappresentata sul lato sinistro del diagramma; identifica tutte le cause (rettangoli di colore blu) associabili all'evento indesiderato e, per ognuna di esse, evidenzia tutti gli specifici sistemi di protezione (sia impiantistici che di controllo operati-

vo) che contribuiscono a prevenire l'evento indesiderato. La Zona 1 può essere considerata equivalente ad un albero dei guasti semplificato.

- La **Zona 2** *(Top Event)* è rappresentata al centro del diagramma e identifica in modo univoco il pericolo considerato (rettangolo a strisce gialle e nere) l'evento incidentale primario detto *Top Event* (cerchio di colore rosso); tale evento può a sua volta evolvere, in base alla dinamica dell'incidente in scenari incidentali alternativi tra loro.
- La **Zona 3** (Protezione) identifica tutti gli scenari incidentali potenzialmente generati (es: getto di gas incendiato, esplosione, *flash fire* ecc…) e la combinazione di tutti gli elementi che ne consentono lo sviluppo, includendo tutti i sistemi di protezione che possano mitigarne gli effetti. La Zona 3 può a tutti gli effetti essere considerata equivalente ad un albero degli eventi semplificato.

La tecnica *Bow-Tie* permette di identificare e valutare le frequenze e le conseguenze associate agli scenari e di quantificare il contributo dei sistemi protettivi e mitigativi (barriere) in condizioni di normale produzione. Anche questo aspetto è approfonditamente discusso nei successivi Capitoli del libro; tuttavia è bene prima introdurre la metodologia di analisi che è alla base della quantificazione in frequenza dei *Bow-Tie*: l'analisi LOPA.

### 3.3.4.2 Layer Of Protection Analysis (Analisi LOPA)

L'analisi dei livelli di protezione indipendenti (LOPA – *Layer of Protection Analysis*) è un metodo tipicamente utilizzato quale strumento di valutazione del rischio, talvolta anche utilizzato per l'investigazione di incidenti. Esso ha trovato particolare successo nell'industria di processo; in questo contesto è possibile identificare i livelli di protezione che riducono i rischi di eventi indesiderati. Essi sono raffigurati in Figura 3.10.

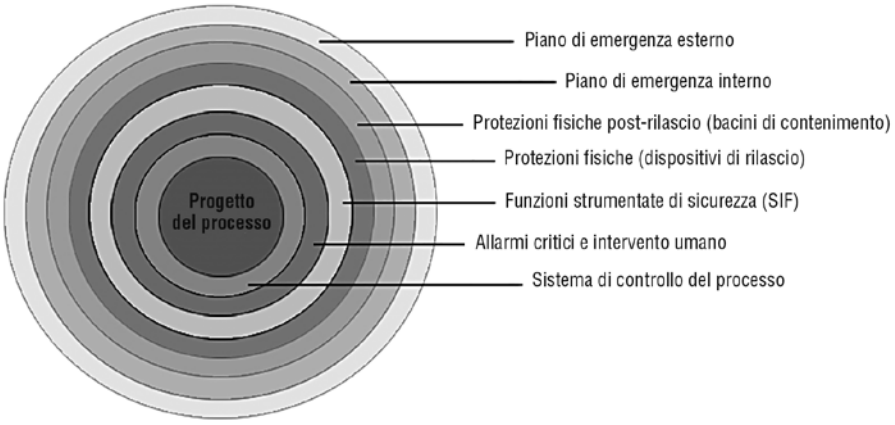



**Figura 3.10** – *Livelli di protezione indipendenti nell'industria di processo (adattata da Fiorentini e Marmo, "Principles of Forensic Engineering applied to Industrial Accidents", Wiley, 2018)*

Lo scopo dell'analisi LOPA è di analizzare l'efficacia delle barriere (livelli di protezione) proposte, confrontando il livello di rischio del sistema ipotizzato privo di barriere con il livello di rischio del sistema equipaggiato con le barriere, sempre avendo come riferimento un criterio di tollerabilità del rischio.

L'analisi LOPA può utilizzare anche solo ordini di grandezza sia della frequenza degli eventi iniziatori che per la probabilità di fallimento di un livello di protezione indipendente (IPL – *Independent Protection Layer)*, determinando così che le barriere esistenti sono sufficienti o meno per mitigare il livello di rischio di un determinato scenario incidentale al di sotto del limite di tollerabilità.

Le barriere possono essere classificate, al pari di come è possibile fare per l'analisi *Bow-Tie*, in barriere attive o passive, o preventive e mitigative. Deve tuttavia essere chiaro che mentre tutti gli IPL sono barriere, non tutte le barriere sono IPL. In generale, una barriera è un qualunque sistema, strumento o azione che può arrestare la catena di eventi conseguente ad un evento iniziatore. Per essere anche un IPL, una barriera deve essere: efficace (avere la capacità di intervenire in tempo), indipendente (non condividere cause comuni di guasto con altre barriere), e valutabile (per dimostrare che essa soddisfi i requisiti di mitigazione del rischio).

Citando ad esempio lo standard tecnico EN/IEC 61511-3 in materia di sicurezza funzionale:

- ogni IPL deve essere indipendente da qualunque altro IPL;
- ogni IPL deve essere differente da qualunque altro IPL;
- ogni IPL deve essere fisicamente separato da qualunque altro IPL;
- ogni IPL non deve condividere cause comuni di guasto con qualunque altro IPL;
- ogni IPL deve essere altamente disponibile;
- ogni IPL deve essere validato e *auditabile.*

Questo metodo può essere utilizzato lungo tutto il ciclo di vita della sicurezza di processo. È generalmente utilizzato per esaminare gli scenari provenienti da altri strumenti di PHA, come l'HAZOP, e definire i target SIL da raggiungere per soddisfare i criteri di accettabilità del rischio.

Può anche essere utilizzato nelle fasi iniziali di un progetto, allo scopo di valutare protezioni alternative, o identificare quelle critiche, ovvero quelle che mantengono il rischio all'interno della regione di tollerabilità. È anche utile per identificare i controlli amministratici critici (CAC – *Critical Administrative Control)*, ovvero le azioni o risposte dell'operatore che sono critiche per mantenere il rischio all'interno della regione di tollerabilità. È anche utilizzato per identificare gli scenari di rischio ALARP.

Risulta evidente che, in teoria, un singolo livello di protezione sia sufficiente a fermare la sequenza incidentale e prevenire quindi lo scenario di rischio. In verità, nessun livello

può essere considerato completamente affidabile (100%), nessuno è perfettamente efficace. Questo è il motivo per cui viene generalmente identificato un insieme di livelli di protezione per fornire la richiesta mitigazione del rischio. Se il rischio non è tollerabile, IPL aggiuntivi dovrebbero essere prescritti.

Per eseguire una analisi LOPA è necessario disporre di molti dati in ingresso, quali: dati sui ratei di guasto dei componenti di un apparecchio o sistema, frequenze di cause iniziatrici, ratei di errore umano, e così via, analogamente ad altre tecniche quantitative quali FTA ed ETA.

Così strutturata, la LOPA non è un metodo pienamente quantitativo; esso è piuttosto un approccio numerico semplificato per valutare l'efficacia dei livello di protezione per un preciso scenario incidentale. Il fatto che la LOPA utilizzi dei numeri non vuol dire che fornisce misure del rischio precise: fornisce solo un'approssimazione che può essere comunque utile (se non addirittura sufficiente) a seconda del contesto. Ad esempio per stimare l'ordine di grandezza della riduzione del rischio operata da una combinazione di misure rispetto a combinazioni alternative a supporto di un successivo studio ALARP e correlate analisi costi-benefici. Quale metodologia numerica di screening essa consente di definire priorità di approfondimento e/o di implementazione nell'ambito delle attività di pianificazione della riduzione dei rischi da porsi alla base dei riesami periodici.

Questa metodologia può essere vista in parallelo ad altri metodi di valutazione quantitativa del rischio, come l'albero degli eventi, come mostrato in Figura 3.11.

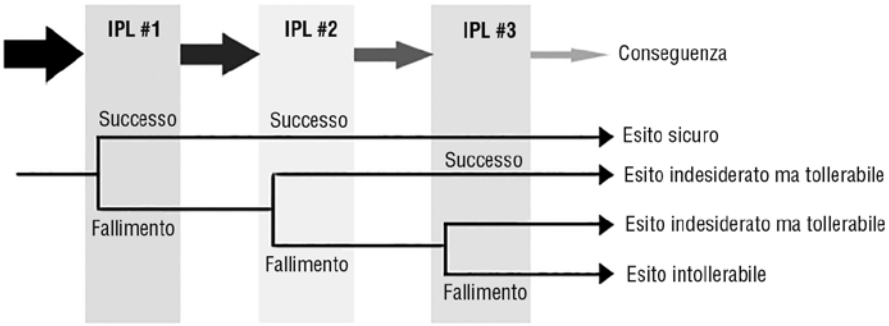



**Figura 3.11** – *Analisi LOPA in combinazione con ETA (adattata da Fiorentini e Marmo, "Principles of Forensic Engineering applied to Industrial Accidents", Wiley, 2018)*

In Figura 3.11, lo spessore della freccia rappresenta la frequenza dello scenario, che è ridotta progressivamente dall'efficacia delle barriere. È chiaro come LOPA e ETA condividano alcuni concetti alla base del comune ragionamento (*in primis*, come evidente, le due metodologie condividono l'individuazione delle misure di controllo quali elementi fondamentali per il riconoscimento degli insiemi di esiti possibili data una iniziale deviazione dalle normali condizioni operative atte al raggiungimento degli obiettivi prefissati).

Semplificando, la LOPA consiste delle seguenti fasi:

- raccolta degli scenari sviluppati in altri studi, come l'HAZOP;
- selezione di uno scenario incidentale e valutazione delle conseguenze;
- identificazione degli eventi iniziatori e delle loro frequenze;
- identificazione degli IPL e della loro probabilità di fallimento;
- stima del rischio, combinando la frequenza degli eventi iniziatori, la probabilità di fallimento degli IPL e la severità delle conseguenze;
- valutazione del rischio ed eventuale sviluppo di un piano di azioni per mitigare ulteriormente il rischio.

L'analisi LOPA non deve essere confusa con l'HAZOP: si tratta di tecniche differenti, con obiettivi diversi. L'HAZOP è utilizzata per fare *brainstorming* sui possibili pericoli ed identificare gli scenari incidentali, il cui rischio può essere valutato solo da un punto di vista qualitativo. Invece, durante la LOPA l'analista arricchisce queste informazioni con delle valutazioni quantitative, almeno per ordini di grandezza, quando non puramente qualitative. Come più volte accennato in questo volume non esiste una metodologia univoca per la valutazione del rischio. La selezione del metodo (ed eventuali tool a supporto) risulta essere un passaggio specifico, obbligato e fondamentale della strategia di gestione del rischio, da effettuarsi tenendo conto di risorse e competenze ma soprattutto dell'analisi iniziale dal contesto e degli obiettivi. Ciò detto spesso, anche a favore di un approccio ad approfondimento graduale, con la selezione di una metodologia per ciascun aspetto di rischio o di una combinazione di metodologie.

## 3.4 Valutazione del rischio (risk evaluation)

La valutazione del rischio rappresenta l'ultima delle tre fasi del più generale processo di *"risk assessment"*. Grazie alla "*risk evaluation"*, il livello di rischio ottenuto tramite la precedente fase di analisi viene tradotto, tramite i metodi descritti in questo paragrafo, in indici o valori che potranno essere confrontati con le soglie di accettabilità e tollerabilità definite in fase preliminare unitamente ai traguardi dell'analisi ed agli obiettivi generali della organizzazione, al fine di stabilire così se il rischio possa essere accettato (e ritrovarsi quindi nell'ambito del miglioramento continuo), tollerato (e ricade quindi nella cosiddetta regione ALARP) oppure se debba essere trattato ulteriormente.

### *3.4.1 Curve FN*

Le curve *F-N*, sovente utilizzate nell'ambito della sicurezza industriale legata ai rischi rilevanti connessi con incendi, esplosioni e rilasci tossici, sono una rappresentazione grafica bidimensionale della frequenza cumulata delle conseguenze lesive attesa in rapporto all'entità della loro magnitudo (sovente espressa in termini di numero di fatalità).

*Pagine omesse dall’anteprima del volume*