Analisi di affidabilità umana

Andrea Maioli

20 Maggio 2002

1 Introduzione

Negli anni Sessanta e Settanta le indagini sugli incidenti tendevano a considerare prevalentemente gli aspetti tecnici come causa dell'incidente stesso; di conseguenza, le misure per il miglioramento della sicurezza erano volte esclusivamente a minimizzare i fallimenti tecnologici. In seguito, l'attenzione si è spostata verso la componente umana, ritenendo che fosse il fallimento di quest'ultima la principale causa scatenante: per migliorare la sicurezza divenne allora necessario operare non soltanto sulla dimensione tecnologica ma soprattutto su aspetti quali la formazione del personale, le interfacce uomo-macchina, i sistemi di supporto alle decisioni e quant'altro servisse a ridurre la possibilità di errore umano e, quindi, di incidente.

L'importanza di un'analisi attendibile sull'affidabilità dell'elemento umano è oggi sempre più importante, soprattutto nell'ottica della metamorfosi del compito richiesto all'operatore. Con il progredire della tecnologia, infatti, l'uomo si è visto allontanato dal compito fisico sul quale in precedenza interveniva in prima persona e che oggi è sempre più frequentemente gestito da sistemi automatizzati, TIS (*Task Interface System*), che esercitano un controllo a ciclo chiuso sulle componenti strutturali del compito (eliche, pompe, caldaie, interruttori, valvole, etc.) per mezzo di sottosistemi automatici (termostati, autopiloti, servosistemi, robot programmati, etc.); essi possono far sì che l'intero impianto giunga a predeterminati stati finali, che sono però incapaci di modificare, così come non sono in grado di intraprendere qualsiasi tipo di risposta adattativa. È dunque necessario un secondo sistema informatico che interagisca con l'uomo, HIS (*Human Interface System*) e che permetta la comunicazione tra l'operatore umano e i controllori del livello inferiore.

In questa situazione, nella quale l'uomo realizza in maniera preponderante compiti di supervisione che ne aumentano le responsabilità, diventa essenziale completare la PSA sistemica classica con metodi di analisi qualitativa e quantitativa delle procedure operazionali e del comportamento stesso degli operatori. Tali metodologie dovranno ovviamente essere in grado di modellizzare le situazioni incidentali e formalizzarne una rappresentazione

che fornirà la base per le applicazioni numeriche che saranno in grado di determinare la portata delle conseguenze. In altre parole, da un punto di vista affidabilistico, lo scopo di tali modelli è quello di ricavare il valore numerico di probabilità da associare a quell'evento base dell'albero dei guasti etichettato con la notazione: *l'operatore sbaglia*.

2 La I generazione

I modelli che attualmente risultano maggiormente utilizzati nell'analisi dell'affidabilità umana presentano forti analogie con le tecniche utilizzate per la PSA sistemica; le linee guida di tali modelli possono essere riassunte nella metodologia SHARP (*Systematic Human Action Reliability Procedure*) formalizzata da Hannaman e Spurging nel 1984 e che può essere schematizzata tramite i seguenti sette passi:

1. *Definition*: gli alberi logici sviluppati dall'analista del sistema sulla base delle descrizioni funzionali dell'impianto sono studiati a fondo con l'obbiettivo di identificare al meglio le interazioni e di assicurarsi che le diverse azioni umane legate alla procedura di controllo in oggetto siano accuratamente considerate.

2. *Screening*: gli alberi logici, arricchiti delle azioni umane, sono analizzati e rivisti per l'identificazione delle azioni più importanti da analizzare in dettaglio nel prosieguo dell'indagine affidabilistica.

3. *Breakdown*: ciascuna interazione, definita precedentemente come rilevante, è suddivisa in azioni, obbiettivi e sotto-obbiettivi (*task analisys*), con l'identificazione dei fattori più influenti per una modellizzazione completa.

4. *Representation*: le interazioni dettagliate sono modellate esplicitamente nella forma di alberi di evento o di guasto, includendo anche le alternative che si pongono all'operatore in modo tale da poter analizzare i possibili impatti sull'albero logico del sistema.

5. *Impact Assessment*: i possibili alberi logici derivanti dalle azioni identificate nel passo precedente sono sviluppati in maniera tale da permettere all'analista di sicurezza di valutarne l'impatto sul comportamento globale dell'impianto.

6. *Quantification*: le azioni sono quantificate in termini di probabilità per l'inclusione nel PSA.

7. *Documentation*: i risultati dell'analisi sono infine documentati con tutte le informazioni necessarie per future analisi e definizioni di errori umani.

I passi più critici tra quelli della metodologia SHARP sono ovviamente quelli relativi alla rappresentazione del comportamento umano e alla ricerca vera e propria dei valori numerici di probabilità.

2.1 La rappresentazione

La tecnica OAT (*Operator Action Tree*) è un modello per la rappresentazione delle sequenze di azioni che sono necessarie per raggiungere un determinato obbiettivo e si candida dunque per soddisfare alle necessità del quarto passo della metodologia SHARP. Un Action Tree non è altro che l'equivalente nell'ambito dell'affidabilità umana degli event tree utilizzati nel PSA per l'affidabilità sistemica; in questo caso, gli header dell'albero si focalizzano sul processo decisionale e vengono dunque identificate alternative sulla base di ambiguità o interpretazioni dell'operatore associate con le fasi di osservazione, diagnosi e selezione di risposte al sistema.

Un secondo metodo che permette la modellizzazione del comportamento umano in situazioni accidentali (e che può essere utilizzato con grande profitto nella fase iniziale della progettazione) è denominato PHECA (*Potential Human Error and Cause Analysis*) che non è altro che una HAZOP adattata al fattore umano e dove al posto delle keyword, tipiche della HAZOP, vengono indicati gli errori tipici che possono essere commessi.

2.2 La quantificazione

Il metodo più diretto per la quantificazione della probabilità degli errori umani (HEP *Human Error Probability*) è la metodologia APJ (*Absolute Probability Judgement*), che si basa sul giudizio di uno o più esperti in fattori umani; la maggior parte delle ricerche è peraltro basata sul lavoro di un gruppo di esperti, in quanto raramente esiste una sola persona capace di avere sufficiente conoscenza ed informazione per stimare completamente gli errori umani in procedure complesse. In questo caso le opinioni singole e la conoscenza di ciascun esperto sono combinate sia mediante metodi matematici che forzando i giudici al consenso su singoli problemi.

I passi fondamentali di questa metodologia, che concorre a soddisfare il sesto passo della metodologia SHARP, sono i seguenti:

1. selezione degli esperti;
2. identificazione della missione e relativa procedura;
3. preparazione di formati di risposta;
4. sviluppo di istruzioni per gli esperti;
5. raccolta dei giudizi singoli; questo è ovviamente il passo più critico e può essere assolto seguendo quattro metodologie differenti:

- *Aggregated individual method*: richiede stime individuali di esperti separatemente elicitati, tali stime vengono poi combinate statisticamente prendendone la media geometrica;
- *Delphi method*: gli esperti devono ancora proporre singolarmente ed autonomamente delle stime, salvo poi rivederle ed aggiustarle sulla base dei giudizi di altri esperti, i valori finali vengono combinati statisticamente come in precedenza;
- *Nominal group technique*: simile al metodo precedente, dove è però ammessa una certa discussione tra gli esperti;
- *Consensus group method*: si impone agli esperti di raggiungere valori consensuali di stime;

6. valutazione delle consistenza tra i giudizi;
7. aggregazione delle stime individuali;
8. valutazione delle incertezze.

Gli ultimi tre passi vengono ovviamente gestiti tramite metodi matematici.

La metodologia APJ presenta due svantaggi, dovuti principalmente al fatto che è completamente legata al giudizio di esperti: le alienazioni che possono generarsi a seguito di conflitti di personalità e problemi vari nel gruppo di esperti, e la tendenza alla stima approssimata cui gli esperti tendono molto spesso.

2.3 Una metodologia completa: THERP

La metodologia più famosa ed effettivamente utilizzata per l'analisi dell'affidabilità umana è nota come THERP (*Technique for Human Error Rate Prediction*), proposta nel 1983. Essa, benché antecedente, copre tutti i passi fondamentali della metodologia SHARP (con alcune modifiche), si basa sulla costruzione di alberi di evento per quanto riguarda la modellizzazione (*HRA-Even Tree*) e fa affidamento, per quanto riguarda la quantificazione, ad un data-base compilato da esperti che presenta il valore di HEP associato ad una vasta gamma di azioni umane. È importante sottolineare che tale data-base[1] contiene il valore di probabilità associato alle azioni base con le quali si costruisce la sequenza seguita dall'operatore, ricavato da studi decontestualizzati (nei quali, quindi, si è studiata solo l'azione base in quanto tale) ed è per questo necessario tentare di adattare le singole azioni al caso specifico in analisi introducendo degli appositi *Performance Shaping Factors* (PSF).

[1] Il data-base delle HEPs è riportato nel capitolo 20 della guida THERP

2.4 La critica

La critica di base all'adeguatezza dei metodi classici di affidabilità umana risiede nel fatto che questi approcci hanno una tendenza descrittiva degli eventi, in cui solo gli aspetti formali esterni del comportamento vengono osservati e studiati sotto il profilo degli errori, senza considerare le ragioni ed i meccanismi che li hanno indotti a livello di cognizione; per questo motivo i modelli di comportamento umano che accompagnano questi metodi affidabilistici sono spesso detti comportamentali. A seguito di questa totale decontestualizzazione (che richiede, per esempio, nel caso di THERP, l'utilizzo dei PSF) questi modelli non tengono in considerazione il livello di esperienza degli operatori e la situazione socio-tecnica dell'ambiente di lavoro; ciò causa sostanziali problemi quando si sia in presenza di cause comuni di guasto (*common cause failures*). Gli errori umani sono, per loro natura, eventi di cause comuni di guasto.

3 La II generazione

Negli anni Novanta, a seguito di analisi complesse di incidenti clamorosi (come quelli di Three Mile Island, Chernobyl, e quello che ha coinvolto lo Space Shuttle Challenger), si è arrivati a comprendere come gli incidenti non siano solamente generati da cause e fallimenti tecnici o da cause e fallimenti umani, ma dall'interazione di più componenti: tecnologiche, umane, organizzative, in relazione tra loro e con l'ambiente esterno nel quale l'organizzazione opera: il problema dell'affidabilità umana ha da allora innalzato il suo livello di complessità.

3.1 La complessità del problema

Il nuovo livello di complessità del sistema è ben esemplificato dai modelli organizzativi e socio-tecnici, tra i quali il modello SHELL (*Software Hardware Environment Liveweare Liveweare*), sviluppato da Frank Hawkins nel 1987, che suggerisce come, più che guardare in profondità ogni singola componente del sistema (hardware, software e liveweare, ovvero l'elemento umano), sia necessario guardare alle relazioni e interazioni tra gli elementi, individuando le potenziali configurazioni critiche che si realizzano in un complesso di lavoro.

Tale modello individua quattro interfacce:

- *Interfaccia L-H:* è l'area più classica della progettazione e si basa sulla considerazione che la tecnologia deve essere disegnata secondo le caratteristiche dell'utente umano e dei suoi limiti (fisici e cognitivi); è anche l'unico livello di cui si tiene pienamente conto nelle metodologie di I generazione.

- *Interfaccia L-S:* riguarda l'area delle interazioni tra l'uomo e le procedure e regole che ne orientano e definiscono le prestazioni. Per raggiungere condizioni di sicurezza progressive e operazioni efficaci, questa interfaccia richiede un'attenta progettazione, assumendo che le procedure non devono essere in conflitto con le caratteristiche umane e non devono definire regole complicate o impossibili da seguire o applicare.

- *Interfaccia L-E:* riguarda l'area dell'interazione tra l'uomo e l'ambiente esterno ed è ovviamente l'ambito che offre la minor possibilità di intervento per il progettista; comprende una serie di caratteristiche fisiche dell'ambiente quali la temperatura, il rumore, etc...

- *Interfaccia L-L:* è l'area delle relazioni interne tra la componente umana del sistema e riguarda il modo in cui le informazioni e la conoscenza sono scambiate tra le persone nella realizzazione dell'attività, nella distribuzione dei compiti e delle responsabilità, nei processi di comunicazione e di decisione.

Appare evidente come, volendo considerare tutti questi livelli, la modellizzazione del comportamento umano diventa decisamente complessa.

3.2 Un nuovo *modello* di operatore

La prima e più celebre modellizzazione *evoluta* del comportamento umano nell'ambito di situazioni di emergenza e in contesti con impianti produttivi rischiosi è stata formalizzata da Rasmussen nel 1984 (ed è noto come modello SRK).

Egli distingue tre diverse forme di comportamento, basato su abilità, regole e conoscenze.

- Livello basato sulle abilità (*skill-based*): il comportamento si basa sulla rilevazione di un segno (input) al quale corrisponde una determinata e appropriata risposta (preprogrammata) da parte dell'operatore. Non vi è retroazione o interpretazione dei segnali ambientali e non sono quindi necessarie procedure di riconoscimento. Gli errori, in questo livello, dipendono dalla variabilità intrinseca della coordinata temporale, dello spazio e della forza.

- Livello basato sulle regole (*rule-based*): il comportamento inizia con il riconoscimento di un segnale e l'attivazione da parte dell'operatore di una procedura appropriata per eseguire il compito. Gli errori in questo livello dipendono da un'errata classificazione della situazione e dalla conseguente adozione di procedure errate.

- Livello basato sulla conoscenza (*knowledge-based*): si ha in situazioni nuove per l'operatore dove le regole non sono d'aiuto nella risposta

ma è invece necessario definire un obiettivo ed un piano operativo per raggiungerlo. L'operatore deve identificare dei simboli, decidere in base alla conoscenza posseduta e alle esperienze precedenti, pianificare le operazioni e agire. Gli errori a questo livello derivano da fenomeni di razionalità limitata, carenza di informazioni, errata interpretazione dei simboli, etc...

Su questo modello di comportamento si innesta molto bene la teoria dell'errore umano di Reason (1990) secondo il quale esistono diverse tipologie di errore a seconda che derivino da azioni realizzate secondo le intenzioni o meno.

Al primo di questi due gruppi appartengono *slips* e *lapses*. I primi sono errori potenzialmente osservabili come azioni che comprendono azioni eseguite in modo diverso da come pianificato (intenzione corretta ed esecuzione sbagliata), mentre i secondi sono fallimenti della memoria relativi all'immagazzinamento di informazioni da parte di un operatore.

Al secondo gruppo, invece, appartengono i *mistakes*, ovvero fallimenti dei processi di giudizio che si manifestano quando un operatore intende perseguire un obiettivo corretto ma il piano che attua è sbagliato.

La combinazione del modello di Rasmussen e del modello di Reason permette una modellizzazione più realistica del comportamento umano.

4 Conclusioni

L'individuazione di un nuovo e più efficace metodo di rappresentazione del comportamento umano (proposto da Reason e Rasmussen e ulteriormente sviluppato in seguito) implica una revisione dei metodi di quantificazione delle HEP rispetto a quelli di I generazione. Questo è, attualmente, il compito principale della seconda generazione che, a tutt'oggi, ha prodotto alcuni modelli di quantificazione che però, ancora, non sono stati inquadrati in una metodologia generale.

Riferimenti bibliografici

[1] Barry Kirwan *A Guide to Practical Human Reliability Assessment.* Taylor&Francis, 1994.

[2] P.C. Cacciabue *Affidabilità umana e dinamica nei sistemi nucleari.* Tesi di dottorato.

[3] Maurizio Catino *Da Chernobyl a Linate - Incidenti Tecnologici o Errori Organizzativi?* Carocci, 2002.

[4] A.D. Swain, H.E. Guttmann *Handbook of Human Reliability Analysis with Emphasis on Nuclear Power Plant Applications. Final Report.* NUREG/CR-1278 SAND80-0200 RX, AN, 1983.

[5] Najmedin Meshkati *Human Factors in Large-Scale Technological Systems' Accidents: Three Mile Island, Bhopal, Chernobyl.* Industrial Crisis Quarterly, Vol. 5, pag. 131-154.

[6] G.E. Apostolakis *A Critique of Recent Models for Human Error Rate Assessment.* Reliability Engineering and System Safety, Vol.22, pag. 201-217, 1988