STRUMENTI PER LA VALUTAZIONE DI VULNERABILITÀ DI UNO STABILIMENTO INDUSTRIALE RISPETTO AD UN ATTACCO TERRORISTICO

Paolo Vestrucci 1,2, Marco Buldrini 1, Stefano La Rovere 1, Cristian Vercilli 1, Giovanni Zappellini 1
1 NIER Ingegneria S.p.A., via Altabella 3, 40123 Bologna (Italy)
2 Università degli studi di Bologna, Facoltà di Ingegneria, Viale del Risorgimento 2, 40136 Bologna

SOMMARIO

Lo studio proposto nella presente memoria, si pone l'obiettivo di testare l'applicabilità di alcuni strumenti classici dell'analisi di affidabilità e sicurezza in ambito industriale per valutazioni del rischio derivante da atti terroristici. Infatti, se da un lato le più diffuse metodologie di analisi del rischio terrorismo, nate spesso per la crescente necessità di proteggere tipologie di obiettivi giudicati di volta in volta vulnerabili, hanno per lo più origini molto diverse dall'ambito della sicurezza industriale, è indubbio che tecniche e metodologie quali ad esempio Hazop ed Alberi di Guasto, possano essere utilizzate efficacemente anche nel campo della security specialmente se applicate proprio all'analisi di vulnerabilità di attività industriali. L'applicazione del metodo di analisi Hazop o Fmea allo studio della vulnerabilità rispetto ad un atto di sabotaggio ha permesso di evidenziare alcune differenze di fondo rispetto ad una applicazione tradizionale di tali metodologie. Il caso di studio proposto, che ha tratto spunto da una comune analisi Hazop svolta su una sezione di distillazione, da un lato suggerisce una possibile metodologia che consente un'analisi antiterrorismo a partire dalle risultanze di un'analisi di safety, dall'altro mette in evidenza le differenze che emergono nel prendere in considerazione, ad esempio, i dispositivi di protezione e le loro cause comuni di "guasto", oppure, la collocazione spaziale, dei sistemi di controllo o delle protezioni, che assume nell'analisi antiterrorismo una rilevanza notevole. La tecnica degli alberi di guasto, infine, se da un lato viene privata della funzione di strumento utile per definire la probabilità d'accadimento di un determinato Top Event, dall'altro viene comunque valorizzata come tecnica efficace per ordinare le possibili catene di eventi che portano al verificarsi di un determinato scenario: dallo studio dei vari cut set, infatti, emerge la possibilità di ottenere informazioni importanti per l'individuazione delle criticità e per la definizione di adeguate contromisure.

1.0 INTRODUZIONE

L'esigenza di una maggior sicurezza rispetto al rischio di possibili atti terroristici ha prodotto una crescente spinta nella definizione di metodologie di analisi volte all'individuazione di adeguate misure di prevenzione e protezione anche per gli insediamenti industriali con particolare riguardo agli stabilimenti a rischio di incidente rilevante. Del resto, tale preoccupazione trova riscontro, ad esempio, nei dati tratti dal MIPT (National Memorial Institute for the Prevention of Terrorism - Terrorism Knowledge Base), dai quali si evince che le attività industriali o commerciali costituiscono uno degli obiettivi, su scala mondiale, percentualmente più colpiti da attacchi terroristici.

Una valutazione completa del rischio associato ad uno stabilimento a rischio di incidente rilevante, quindi, oltre a prendere in considerazione i rischi propri legati al processo produttivo, che possono essere causa di incidente, deve prendere in considerazione anche quelli di origine criminosa, che possono causare danni assai più gravi sia in termini di vite umane sia ambientali e patrimoniali.

2.0 DIFFERENZE FRA L'ANALISI DEL RISCHIO IN AMBITO SAFETY E SECURITY

Uno stabilimento a rischio d'incedente rilevante è, come noto, soggetto ad obblighi normativi che prevedono, fra l'altro, una costante analisi e verifica degli aspetti di sicurezza (intesa come safety) connessi con l'attività svolta. In particolare il D.Lgs. 334/99, ma ancor prima il DPR 175/88, prevede la realizzazione di un'analisi dei rischi approfondita che comporta, fra l'altro:

- l'individuazione degli eventi incidentali e dei rispettivi eventi iniziatori;
- il calcolo delle probabilità d'accadimento dei top event individuati;
- il calcolo delle conseguenze di danno attese mediante l'impiego di modelli specifici.

Gli eventi iniziatori in ambito safety sono essenzialmente guasti di componenti, malfunzionamenti di logiche di controllo o blocco, errori umani, ecc.: per ognuno di essi è possibile in linea di massima stimare una frequenza o probabilità d'accadimento. L'adozione di tecniche quali, ad esempio, Fault tree analysis ed Event tree analysis, permettono la schematizzazione delle relazioni tra gli eventi iniziatori che determinano l'accadimento del top event e il calcolo della frequenza o probabilità d'accadimento attesa per quest'ultimo.

Rispetto alle valutazioni del rischio in ambito safety, in una valutazione del rischio terrorismo vengono presi in considerazione eventi iniziatori definiti in termini di modalità d'attacco e, in linea di massima, non ci si addentra in stime di tipo probabilistico, procedendo, invece, a valutazioni di vulnerabilità. La complessità e l'eterogeneità delle valutazioni coinvolte nell'analisi, inoltre, determina l'esigenza di una metodologia sistematica e strutturata che permetta, sia una analisi esaustiva delle possibili modalità di attacco e delle vulnerabilità che il sistema analizzato presenta, sia una stima delle conseguenze di danno prevedibili.

Le *modalità d'attacco* sono definite coma le *tipologie d'azione intenzionale volte a recare un danno al sistema* [1, 2, 3]. La loro individuazione, strettamente legata alle attività di intelligence svolte dalle realtà governative preposte, può essere realizzata anche in assenza di indicazioni precise in tal senso; a tal fine, infatti, possono essere utilizzati hazard list [4, 5, 6] o databases, per lo più di origine americana ed inglese, che permettono la consultazione di reports su azioni terroristiche su scala mondiale e per un arco temporale considerevole. Entrambi gli approcci permettono di prescindere dall'identificazione e caratterizzazione dei gruppi terroristici, quindi dalla stima della probabilità di accadimento di un definito atto ostile [7].

Infine, possono essere fatte alcune precisazioni in ordine alle tipologie di contromisure individuabili nei due campi di safety e security. Come è noto, nell'ambito della sicurezza industriale, le misure atte a diminuire un rischio possono essere distinte in misure preventive e protettive. Un'altra possibile distinzione è, poi, fra misure attive (che, per essere efficaci, necessitano di un sistema di rilevazione e di comando/controllo attivi, ad esempio un impianto idrico antincendio) e misure passive (ad esempio un bacino di contenimento). Nel campo della security, invece, le contromisure possono essere suddivise in: Investigative (finalizzate a prevenire un atto terroristico); Deterrenti (finalizzate a scoraggiare un atto terroristico), Preventive (finalizzate a ridurre la vulnerabilità del target) e Mitigative (finalizzate a ridurre gli effetti di danno).

Lo studio proposto si colloca a valle dell'attività d'individuazione delle possibili modalità d'attacco, ed è incentrato sulla valutazione della vulnerabilità di un impianto industriale rispetto ad un possibile atto di sabotaggio; in quest'ottica, quindi, risultano d'interesse essenzialmente le misure preventive.

3.0 L'AMBITO D'INTERESSE

3.1 Modalità d'attacco: il sabotaggio

L'atto terroristico di sabotaggio viene inteso, nel presente studio, come un'azione, od una serie di azioni, volontarie poste in essere senza l'impiego di armi, ordigni, sostanze od altri dispositivi estranei alla realtà dello stabilimento e volte ad arrecare un danno al sistema colpito.

La scelta del sabotaggio quale modalità d'attacco da analizzare, certamente percepita come critica per uno stabilimento a rischio di incidente rilevante, permette di addentrarsi maggiormente negli aspetti tecnico-impiantistici e gestionali del sistema.

3.2 La vulnerabilità

La *vulnerabilità* può essere definita come la *manifestazione di stati intrinseci del sistema (fisici, tecnici, organizzativi, culturali, ecc.) che possono essere sfruttati da un avversario per colpire o danneggiare il sistema stesso* [1, 2, 3].

Nella memoria proposta, la vulnerabilità è studiata affrontando sia gli aspetti legati all'*accessibilità*, intesa come l'*insieme delle caratteristiche del sistema che influenzano la possibilità di portare un determinato attacco*, sia gli aspetti legati alla *capacità di danno* del sistema, intesa come l'*insieme di quelle caratteristiche che determinano le possibilità di produrre un danno di una certa gravità in seguito ad un determinato attacco.*

In pratica, quindi, un obiettivo può essere ritenuto vulnerabile sia in funzione della facilità con cui può essere colpito sia in funzione della gravità del danno atteso in seguito all'attacco, riferendosi sia ai danni "tangibili" quali la perdita di vite umane, i danni ambientali ed i danni patrimoniali, sia ai danni "intangibili" quali danni di immagine ed impatto sull'opinione pubblica.

3.2.1 La capacità di danno

Citando l'articolo 3 del D.Lgs. 334/99, uno stabilimento a rischio d'incidente rilevante è uno stabilimento in cui "[…] *è possibile il verificarsi di un evento quale un'emissione, un incendio o un'esplosione di grande entità, dovuto a sviluppi incontrollati che si verificano durante l'attività di uno stabilimento e che da luogo ad un pericolo grave, immediato o differito, per la salute umana o per l'ambiente, all'interno o all'esterno dello stabilimento, e in cui intervengano una o più sostanze pericolose*." Tali stabilimenti devono quindi essere considerati possibili obiettivi in relazione alla grande capacità di danno che li caratterizza.

La presenza di grandi quantità di sostanze pericolose, inoltre, non solo può permettere l'insorgere di scenari di danno molto estesi, ma determina la possibilità di arrecare tali danni senza la necessità di impiegare ordigni od armi particolari: una persona in possesso di determinate informazioni può produrre gravi conseguenze anche a "mani nude" [8, 9]. In seconda battuta, poi, non va sottovalutato, il fatto che, spesso, tali stabilimenti sono di proprietà di grandi società multinazionali, per cui un attacco potrebbe assumere in tal caso anche una connotazione simbolica e politica determinante [8, 9].

3.2.2 L'accessibilità delle informazioni

Se da un lato, le caratteristiche di vulnerabilità di uno stabilimento a rischio d'incidente rilevante legate alla capacità di danno, sono sicuramente evidenti, è altrettanto importante considerare gli aspetti particolari che li caratterizzano circa l'accessibilità delle informazioni. Si sottolinea, a tale proposito, che la legislazione comunitaria pone un forte accento sull'esigenza di predisporre adeguati strumenti ed intensificare la comunicazione e l'informazione sia verso chi, a vario titolo, ha accesso all'interno degli stabilimenti, sai nei confronti della popolazione. Tale aspetto, già presente nella Direttiva 96/82/CE (Severo bis) è stato di recente rafforzato con l'entrata in vigore della Direttiva 2003/105/CE recepita in Italia con il D.Lgs. 328/05. Un degli effetti più evidenti di questo indirizzo è che sono, di fatto, di pubblico dominio informazioni quali: la tipologia e le quantità di sostanze pericolose presenti; la descrizione e la disposizione planimetrica delle varie unità/impianti presenti all'interno di uno stabilimento; la tipologia ed l'estensione dei danni producibili.

4.0 IL CASO DI STUDIO: UN IMPIANTO DI PROCESSO

Come anticipato, il caso di studio di seguito presentato consiste nell'applicazione della metodologia HAZOP (Hazard and Operability Studies) [10] e della tecnica degli Alberi di guasto per l'analisi di vulnerabilità di un impianto di processo, rispetto ad un potenziale atto di sabotaggio. Oggetto dell'analisi è la sezione di distillazione di un impianto petrolchimico.

Nei limiti imposti dalle modalità funzionali e operative del processo, l'analisi è riferita ad una sezione limitata dell'impianto, comunque sufficiente a far emergere dall'analisi gli aspetti di carattere metodologico. Per ragioni di brevità, non sono riportate le informazioni relative alle fasi principali del processo ed alle apparecchiature presenti, i diagrammi di flusso ed i relativi P&I.

Nei successivi paragrafi sono singolarmente descritti i passi principali della metodologia proposta, unitamente ai principali risultati avuti. In particolare, sono riportate le valutazioni classicamente realizzate in ambito safety e, più in dettaglio, gli aspetti essenziali per la loro generalizzazione in ambito security.

4.1 Analisi HAZOP

Lo strumento utilizzato per l'individuazione dei fattori di rischio e dei conseguenti scenari di pericolo in ambito Safety è l'analisi di sicurezza ed operabilità (HAZOP), applicata secondo una interpretazione classica di tale metodologia.

Sulla base degli aspetti fisici, tecnici e funzionali dell'impianto e delle sue interazioni con le unità esterne cui è interfacciato, sono stati identificati i punti significativi (nodi) rispetto ai quali valutare l'insorgere e il propagarsi di deviazioni nei parametri fisici di processo: qualità, flusso, pressione, temperatura, livello. Applicando opportune parole guida a tali parametri, sono state definite le deviazioni da analizzare sistematicamente per ciascun nodo, secondo la comune relazione causa-conseguenza-contromisura.

Come ipotesi di base in ambito safety, tra le possibili cause delle deviazioni dei parametri di processo sono considerate unicamente le modalità di guasto proprio dei componenti dell'impianto:

- non è analizzata la manovra errata delle valvole manuali relative a bypass e sezionamenti di componenti e strumentazione, la cui manovra è prevista solo per manutenzione ad impianto fermo;
- il livello di dettaglio dell'analisi (definito con riferimento alla successiva quantificazione delle probabilità / frequenze di accadimento) è tale da includere nell'evento di "malfunzionamento di un sistema di controllo (di livello, portata, pressione, …)", il guasto di un qualsiasi componente (sensore, trasmettitore, controllore, …) capace di causare una deviazione nei parametri di processo.

L'analisi sistematica delle segnalazioni di allarme associate alle condizioni di funzionamento anomalo dell'impianto, permette di identificare le condizioni di guasto che possono determinare un mancato intervento (operativo) da parte dell'operatore preposto.

In Tabella 2 è riportata una delle schede di HAZOP sviluppate.

Tabella 2. Scheda HAZOP

N°	NODO	PAROLE GUIDA	DEVIAZIONI	CAUSE	CONSEGUENZE	SEGNALAZIONI	CONTROMISURE
49	Nodo 7	NO F	Nessuna portata al nodo 7	NO L al nodo 5	Mancato invio gpl a limite batteria Possibile HP al nodo 3		
				Guasto in chiusura FV-04			
				Guasto FC-04 o LIC-06 o FI-04			
				Guasto della pompa P-4303 A & mancato avvio dell'unità di riserva			
50	Nodo 7	HF	Elevata portata al nodo 7	Guasto in apertura FV-04	Nel tempo possibile NO L al nodo 5		
				Guasto FC-04 o LIC-06 o FI-04			
51	Nodo 7	BF	Bassa portata al nodo 7	Guasto in chiusura FV-04	Minore portata di gpl inviata a limite batteria Nel tempo possibile HL al nodo 5		
				Guasto FC-04 o LIC-06 o FI-04			

Il primo risultato avuto dall'applicazione della metodologia HAZOP all'impianto oggetto di studio è l'identificazione di un unico evento incidentale - Sovrappressione nella colonna di distillazione - e la produzione di una documentazione strutturata da cui desumere le informazioni relative alla sua realizzazione. La peculiarità del lavoro svolto consiste nella successiva integrazione e generalizzazione dell'analisi con gli aspetti di security; a tal fine, è realizzata una dedicata Analisi delle modalità di sabotaggio.

Con riferimento alle ipotesi di base dell'analisi HAZOP e dei risultati ottenuti, sono state analizzate tre tipologie di elementi costituenti l'impianto: valvole manuali, componenti principali e sistema di controllo e allarme. Le modalità di sabotaggio analizzate per le valvole manuali sono relative ad una indebita apertura o chiusura, in relazione alla condizione assunta di normale funzionamento dell'impianto. Al fine di focalizzare lo studio sui relativi aspetti metodologici, l'evento di sabotaggio di un componente principale dell'impianto (scambiatore di calore, serbatoi e relative valvole di sfogo) include tutte le manomissioni capaci di renderlo indisponibile (non capace di realizzare la/ le funzione/i assegnata/e).

In generale, la manomissione del sistema di controllo e allarme può comportare condizioni diverse dal normale funzionamento dell'impianto o "mascherare" pre-esistenti anomalie nel processo. Come possibili modalità di sabotaggio sono stati considerati gli interventi mediante DCS sulle valvole di regolazione e di blocco e sui valori di set degli allarmi e delle logiche master-slave.

La specifica modalità di sabotaggio di un componente è stata quindi messa in relazione con l'insorgere di deviazioni nei parametri di processo (in tal caso, si è fatto esplicitamente riferimento alla / alle riga / righe di HAZOP corrispondenti) e/o con l'inibizione di una o più segnalazioni di allarme.

In generale, l'analisi HAZOP è utilizzabile per valutare la propagazione delle deviazioni dei parametri di processo, permettendo così di identificare i potenziali eventi incidentali. A tal proposito, occorre sottolineare come la metodologia proposta permetta di individuare le modalità di sabotaggio che possono produrre gli eventi incidentali identificati mediante le analisi realizzate in ambito safety. Ne deriva che, per garantire l'effettiva considerazione di tutti i possibili scenari incidentali, è necessario che urante lo sviluppo dell'analisi HAZOP vengano analizzate tutte le deviazioni dei parametri, indipendentemente dall'esistenza di cause (guasto dei componenti) capaci di produrle.

Nel caso di studio, mediante le schede HAZOP è stato valutato se la deviazione prodotta dall'atto di sabotaggio può determinare o meno l'evento incidentale individuato (Sovrappressione nella colonna di distillazione). Contestualmente, sono identificate le segnalazioni di allarme coinvolte. I risultati avuti dalla suddetta attività di analisi sono stati formalizzati in una scheda dedicata; in Tabella 3 è riportato un esempio desunto dall'Analisi delle modalità di sabotaggio.

Tabella 3. Analisi delle modalità di sabotaggio

COMPONENTE	MODALITÀ SABOTAGGIO		DEVIAZIONE	TOP	IMPATTO SU SEGNALAZIONI
Valvola manuale 1FV-04	Chiusura indebita		NO F al nodo 7 (Hazop riga 49)	x	-
Valvola manuale 2FV-04	Chiusura indebita		NO F al nodo 7 (Hazop riga 49)	x	-
Psv-02 A/B	Indisponibilità operativa		-	x	-
Logica di controllo/allarme LIC-06	Modifica da DCS valore di set LAH-06	Aumento indebito della soglia di allarme	-	-	Inibizione allarme LAH-06
		Diminuzione indebita della soglia di allarme	HF al nodo 7 (Hazop riga 50	-	Provocato allarme LAH-06
	Modifica da DCS valore di set LAL-06	Aumento indebito della soglia di allarme	NO F al nodo 7 (Hazop riga 49)	x	Provocato allarme LAL-06
		Diminuzione indebita della soglia di allarme	-	-	Inibizione allarme LAL-06
Logica di controllo FI-04	Modifica da DCS del valore inviato a slave	Aumento indebito del valore inviato	HF al nodo 7 (Hazop riga 50)	-	-
			HT al nodo 7 (Hazop riga 54)	-	
		Diminuzione indebita del valore inviato	NO F al nodo 7 (Hazop riga 49)	x	-
			BT al nodo 7 (Hazop riga 55)	-	

Un ulteriore elemento esplicitamente considerato nell'analisi è l'operatore (o gli operatori) preposto alla gestione dell'impianto; in relazione a tale elemento sono state considerate due distinte circostanze: aggressione dell'operatore o operatore che, intenzionalmente, manomette l'impianto.

4.2 Alberi di guasto e Alberi delle vulnerabilità

La tecnica degli Alberi di guasto è utilizzata in ambito safety con l'obiettivo di analizzare le condizioni di "guasto multiplo" e valutar la frequenza / probabilità di accadimento dello scenario incidentale.

L'architettura di un Albero di guasto formalizza e struttura il contenuto dell'analisi HAZOP: mediante un procedimento "Top-down è sviluppato l'Albero di guasto relativo al Top event in oggetto, desumendo le relazioni causa-effetto dalle schede prodotte, fino alla identificazione degli eventi di base (BE: Basic Event).

In ambito safety, questi corrispondono alle modalità di guasto proprio dei componenti. Ai singoli eventi primari sono stati attribuiti i relativi parametri di affidabilità (tasso di guasto, secondo una distribuzione esponenziale per la relativa densità di probabilità di guasto) ricavati da banche dati specializzate. I tempi medi di riparazione (nel caso di componenti riparabili) e le frequenza di test (per la rilevazione di guasti latenti) sono stati attribuiti mediante "giudizio ingegneristico".

In primo approccio le condizioni di guasto sono assunte tra loro indipendenti; le cause comuni di guasto, che possono rendere vane le ridondanze previste, sono identificate e tenute in conto quantificandone la frequenza di accadimento (in relazione al tasso di guasto proprio del componente).

Per ragioni di brevità non è riportato l'Albero di guasto sviluppato, preferendo presentare la sua generalizzazione in ambito security; a titolo informativo, la frequenza di accadimento risultata per il top event è pari a 3E-8 eventi l'anno; una simile frequenza d'accadimento viene di norma considerata "oltre il limite di credibilità" permettendo di valutare come marginale il rischio associato al relativo scenario.

La generalizzazione della metodologia HAZOP mediante integrazione con l'Analisi delle modalità di sabotaggio ha permesso lo sviluppo di un "Albero delle vulnerabilità", finalizzato alla analisi delle condizioni di "sabotaggio multiplo".

In accordo con le valutazioni riportate nel §2, in tema di security si rinuncia, generalmente, alla quantificazione della probabilità / frequenza di accadimento di un atto ostile. Mediante sviluppo dell'Albero delle vulnerabilità è comunque possibile ottenere un insieme di informazioni significative mediante le successive Analisi dei cut set (per l'identificazione delle combinazioni di eventi necessari e sufficienti per la realizzazione dello scenario incidentale) e Analisi d'importanza (per l'identificazione di eventi/componenti "critici" nella realizzazione dello scenario incidentale).

Nelle successive figure è riportata una parte dell'Albero delle vulnerabilità complessivamente sviluppato per l'evento "Sovrappressione nella colonna di distillazione", consistente per le successive valutazioni.

Il quadro che emerge dall'Albero delle vulnerabilità permette di sottolineare, ancora una volta, come lo scenario incidentale in oggetto assuma criticità rilevante non solo in relazione a possibili guasti dei componenti dell'impianto ma anche alla possibilità di provocarlo, in modo intenzionale, mediante una adeguata strategia di sabotaggio.

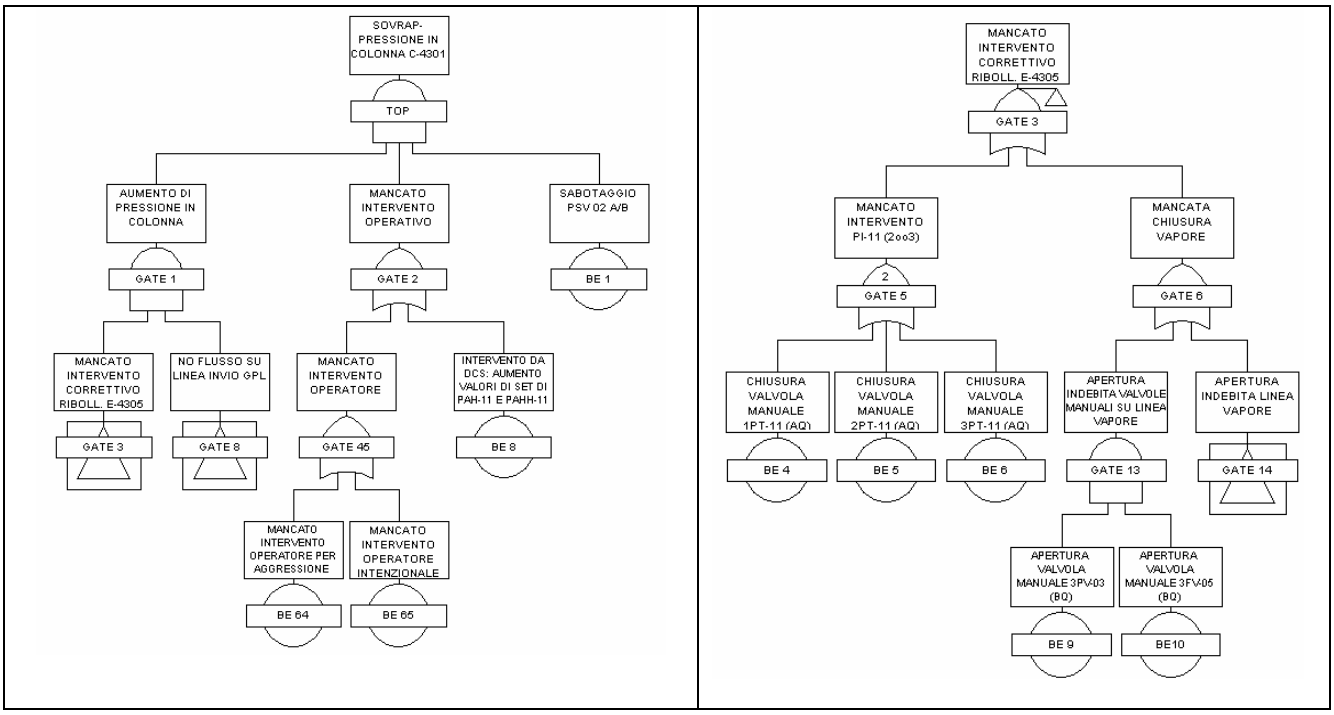

Figura 1. Albero delle vulnerabilità: Top event e Gate 3

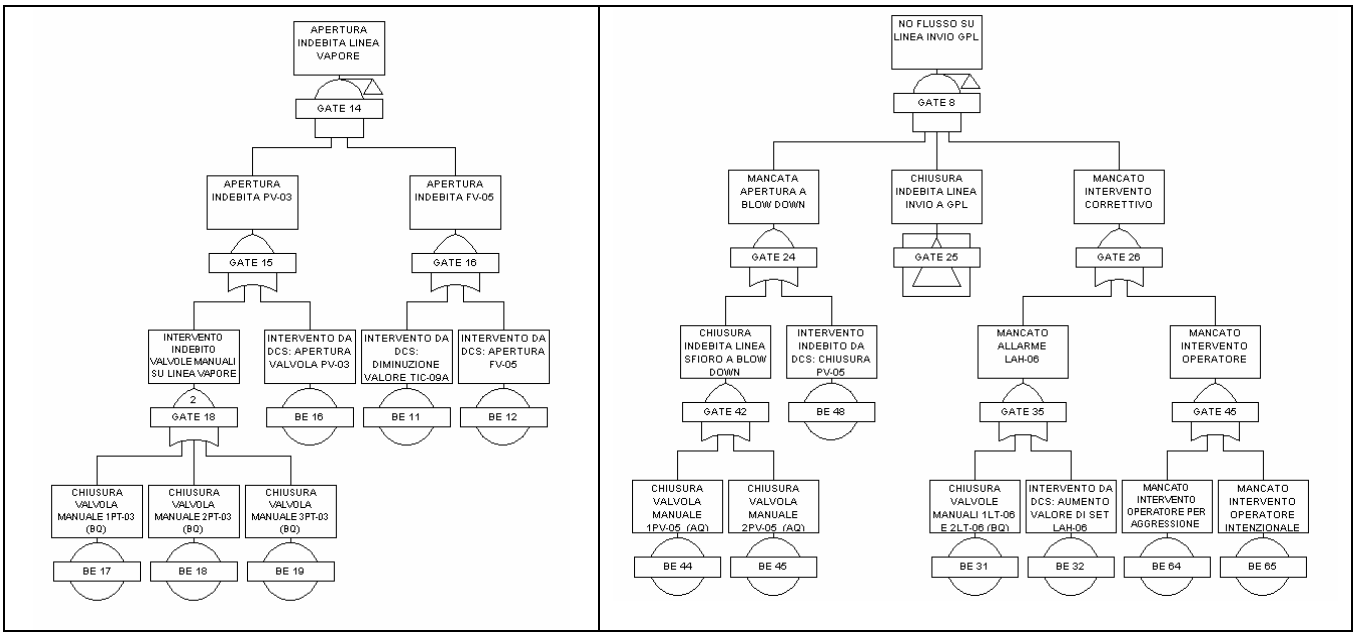

Figura 2. Albero delle vulnerabilità: Gate 14 e Gate 8

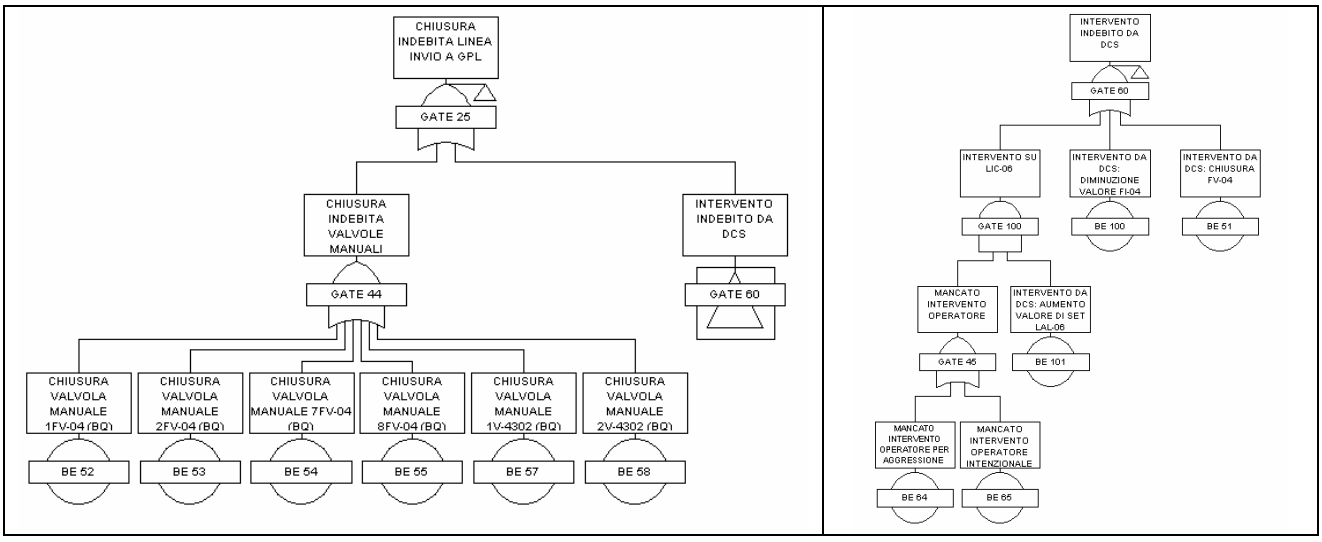

Figura 3. Albero delle vulnerabilità: Gate 25 e Gate 60

Le relazioni esistenti tra i singoli eventi di sabotaggio sono state valutate mediante Analisi dei Cut set dell'Albero delle vulnerabilità. Sono stati identificati 1224 Minimal cut set di cui 324 di ordine 6, 612 di ordine 7 e 288 di ordine 8.

In Figura 4 sono riportati i risultati avuti dall'Analisi di importanza dei singoli eventi di base, realizzata mediante misura Fussel-Vesely, assumendo per tutti gli eventi un uguale valore per la frequenza di accadimento pari ad 1 e un tempo di missione sufficientemente lungo da osservare il valore a regime della frequenza d'accadimento del top. L'indice d'importanza così calcolato coincide con il rapporto tra il numero di minimal cut set ove compare l'evento in oggetto ed il numero complessivo di minimal cut set.

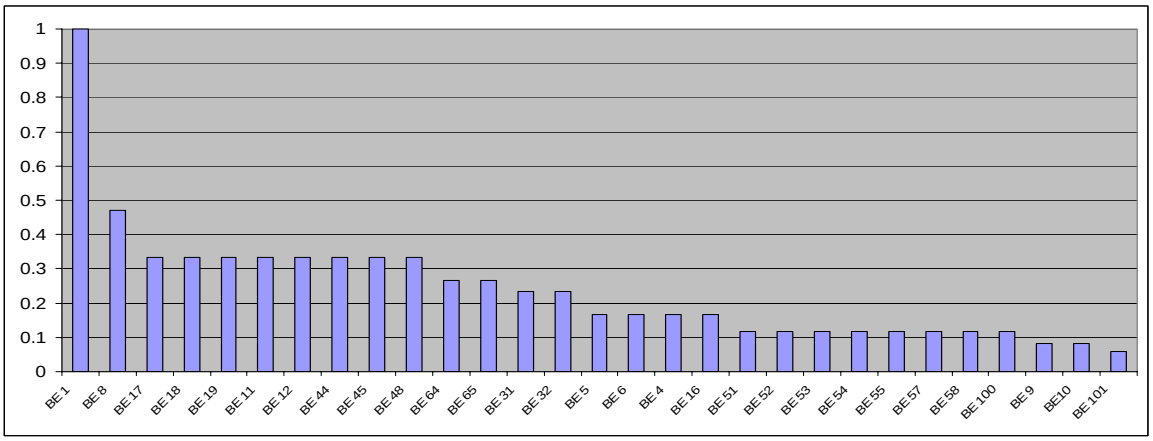

Figura 4. Analisi di importanza dei singoli eventi di base

Gli eventi maggiormente significativi risultano il sabotaggio delle valvole di sfogo (PSV-02 A/B) della colonna di distillazione (BE1) e l'aumento dei valori di set di PAH-11 e PAHH-11 (BE8) mediante intervento da DCS; questi costituiscono sostanzialmente il fallimento delle principiali protezioni contro una sovrappressione in colonna.

Gli eventi di base dell'Albero delle vulnerabilità, ancor più che quelli del corrispondente Albero di guasto, presentano una evidente dipendenza in relazione alla tipologia dei componenti coinvolti ed alla loro "accessibilità". L'approccio proposto per formalizzare le dipendenze tra i singoli eventi di sabotaggio consiste nel definire opportune categorie di eventi. Gli eventi appartenenti a diverse categorie sono considerati tra loro indipendenti. Eventi caratterizzati dalla stessa accessibilità fisica dei componenti coinvolti e delle informazioni sensibili necessarie per una efficace manomissione, sono considerati appartenenti alla stessa categoria. In tal modo è possibile considerare la diversa accessibilità dei componenti (ad esempio, fisicamente installati a quote diverse dell'impianto) ovvero la dipendenza tra i singoli eventi di sabotaggio (ad esempio, la manomissione di componenti dislocati in una zona comune del sito industriale). Le categorie individuate per i singoli eventi di sabotaggio sono le seguenti:

- A: tale categoria comprende unicamente l'intervento indebito sulle PSV-02 A/B, considerato come un evento distinto dagli altri per le particolari condizioni e modalità di sabotaggio richieste

- B: appartengono a questa categoria le operazioni illecite sulle valvole manuali collocate ad una quota elevata dell'impianto;

- C: appartengono a questa categoria le operazioni illecite sulle valvole manuali collocate a bassa quota e sui componenti di processo analizzati (anch'essi, supposti collocati tutti a bassa quota);

- D: rientrano in questa categoria gli interventi indebiti eseguiti a DCS;

- E: comprende esclusivamente il mancato intervento dell'operatore per aggressione;

- F: comprende esclusivamente il mancato intervento intenzionale dell'operatore.

La definizione delle suddette categorie e le successive valutazioni sono realizzate sulla base delle seguenti ipotesi: il DCS è installato in una sala controllo fisicamente distinta dal Locale impianti; i componenti principali dell'impianto sono tutti installati a "bassa quota", con l'eccezione della colonna di distillazione ed in particolare delle relative valvole di sfogo; le valvole manuali sono tutte installate a "bassa quota", con l'eccezione della valvole manuali presenti sulla "linea testa colonna" e sulla "linea sfioro a blow down ".

L'evento di categoria A richiede la capacità di accesso fisico al componente interessato e la conoscenza delle informazioni (sensibili) necessarie per una efficace manomissione; possibili azioni mitigative sono relative al "controllo accessi" nel Locale impianti (in particolare nella parte superiore della colonna di distillazione,

dove è installata la valvola di sfogo) e al "controllo" (limitata divulgazione) della documentazione tecnica del componente (Specifica tecnica, Manuale di installazione e manutenzione, Analisi di affidabilità, …).

Gli eventi di categoria B e C richiedono la capacità di accesso fisico al Locale impianti e, in generale, la conoscenza delle informazioni (sensibili) necessarie per una efficace strategia di sabotaggio; possibili azioni mitigative sono relative al "controllo accessi" nel Locale impianti, al "controllo" della documentazione tecnica dell'impianto (Schemi di processo, P&I, …) ed alla "ottimizzazione" della segnaletica predisposta sull'impianto (es: identificazione valvole manuali) tra le opposte esigenze di informazione (per ragioni di safety) e non divulgazione (per ragioni di security). In particolare, la distinzione tra le categorie B e C sottintende una diversa accessibilità delle valvole manuali disposte ad una quota elevata dell'impianto dai restati componenti. L'aggressione dell'operatore preposto (categoria E) richiede, in primo luogo, la capacità di accesso fisico al sito industriale; le misure da adottare sono evidentemente relative al "controllo accessi", alla video-sorveglianza ed alla vigilanza in genere del sito. Dal punto di vista impiantistico, i risultati dell'analisi costituiscono un valido supporto alla identificazione delle possibili modifiche al sistema di controllo, tali da implementare "logiche di blocco" efficaci nel condurre il sistema in condizioni di sicurezza anche a fronte di sequenze "intelligenti" di malfunzionamenti (sabotaggi), potenzialmente trascurati in ambito safety sulla base di valutazioni probabilistiche.

I Minimal cut set precedentemente identificati dall'Albero delle vulnerabilità sono stati quindi rielaborati utilizzando le suddette categorie di eventi. I risultati ottenuti sono riassunti in Tabella 3.

Tabella 3. Cut set elaborati per categorie di eventi

Ordine	Cut set					Percentuale	
2	A	D				0,33%	0.3%
3	A	D	E			0,57%	14.7%
	A	D	F			0,57%	
	A	C	D			11,44%	
	A	B	D			2,12%	
4	A	B	D	E		3,19%	59.5%
	A	B	D	F		3,10%	
	A	B	C	E		3,92%	
	A	B	C	F		3,92%	
	A	C	D	E		6,12%	
	A	C	D	F		6,04%	
	A	B	C	D		33,17%	
5	A	B	C	D	E	12,75%	25.5%
	A	B	C	D	F	12,75%	

Dalla lista dei cut set identificati in tabella 3 è possibile desumere l'insieme dei Minimal cut-set. Questi rappresentano i "macro-scenari" di sabotaggio, risultati dall'analisi:

- A-D: sabotaggio PSV & Intervento su DCS;

- A-B-C-E: Sabotaggio PSV & valvole manuali ad "alta quota" & valvole manuali / componenti a "bassa quota" & aggressione operatore;

- A-B-C-F: Sabotaggio PSV & valvole manuali ad "alta quota" & valvole manuali / componenti a "bassa quota & intervento intenzionale dell'operatore.

Si può osservare come la dislocazione delle valvole manuali e le caratteristiche proprie del processo richiedano, per la realizzazione dell'evento incidentale, la manomissione delle valvole manuali e dei componenti principali installati a bassa quota e la contestuale manomissione delle valvole manuali disposte a quota elevata. L'efficacia di tale misura e l'effettiva indipendenza delle categorie in oggetto (B e C) è il risultato delle barriere fisiche predisposte e della politica di controllo accessi adottata per l'area interna del Locale impianti.

In Figura 5 sono riportati i risultati avuti dall'Analisi di importanza dei singoli eventi di base, realizzata a valle dell'introduzione delle categorie di eventi, per i soli cut set di ordine 2.

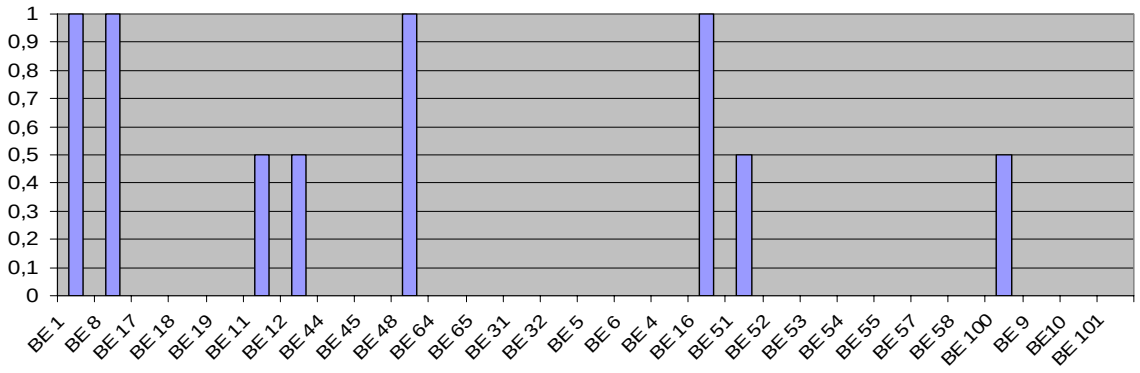

Figura 5. Analisi di importanza: cut set ordine 2

In Figura 6 sono riportati i risultati avuti dall'Analisi di importanza dei singoli eventi di base, realizzata a valle dell'introduzione delle categorie di eventi, per i soli cut set di ordine 3.

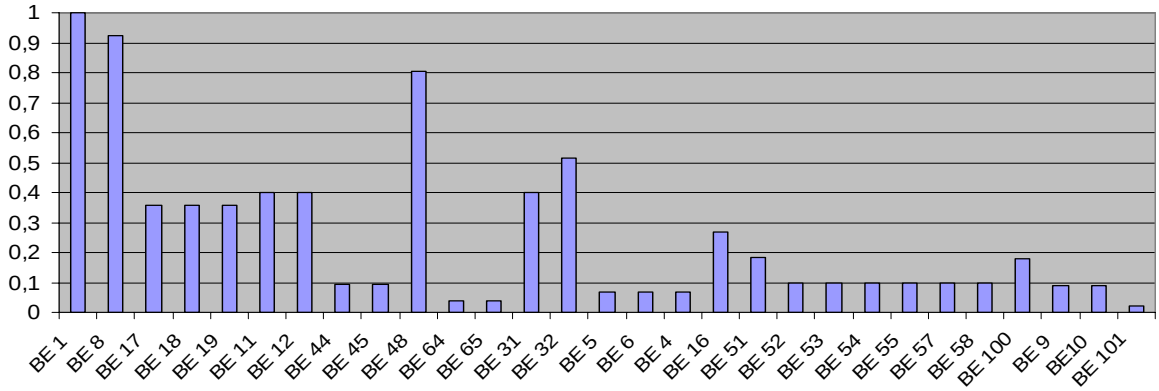

Figura 6. Analisi d'importanza: cut set ordine 3

In Tabella 4 sono riportati in dettaglio i cut set di ordine 2 risultati dall'analisi.

Tabella 4. Cut set di ordine 2

Eventi di base		Categoria
Identificativo	**Descrizione**	
BE 1	SABOTAGGIO PSV 02 A/B	A
BE 100	INTERVENTO DA DCS: AUMENTO VALORE DI SET LAL-06	D
BE 8	INTERVENTO DA DCS: AUMENTO DEI VALORI DI SET DI PAH-11 E PAHH-11	D
BE 16	INTERVENTO DA DCS: APERTURA VALVOLA PV-03	D
BE 11	INTERVENTO DA DCS: DIMINUZIONE VALORE TIC-09A	D
BE 48	INTERVENTO INDEBITO DA DCS: CHIUSURA PV-05	D
BE 1	SABOTAGGIO PSV 02 A/B	A
BE 100	INTERVENTO DA DCS: AUMENTO VALORE DI SET LAL-06	D
BE 8	INTERVENTO DA DCS: AUMENTO DEI VALORI DI SET DI PAH-11 E PAHH-11	D
BE 16	INTERVENTO DA DCS: APERTURA VALVOLA PV-03	D
BE 12	INTERVENTO DA DCS: APERTURA FV-05	D
BE 48	INTERVENTO INDEBITO DA DCS: CHIUSURA PV-05	D
BE 1	SABOTAGGIO PSV 02 A/B	A
BE 51	INTERVENTO DA DCS: CHIUSURA FV-04	D
BE 8	INTERVENTO DA DCS: AUMENTO DEI VALORI DI SET DI PAH-11 E PAHH-11	D
BE 16	INTERVENTO DA DCS: APERTURA VALVOLA PV-03	D
BE 11	INTERVENTO DA DCS: DIMINUZIONE VALORE TIC-09A	D
BE 48	INTERVENTO INDEBITO DA DCS: CHIUSURA PV-05	D
BE 1	SABOTAGGIO PSV 02 A/B	A
BE 51	INTERVENTO DA DCS: CHIUSURA FV-04	D
BE 8	INTERVENTO DA DCS: AUMENTO DEI VALORI DI SET DI PAH-11 E PAHH-11	D
BE 16	INTERVENTO DA DCS: APERTURA VALVOLA PV-03	D
BE 12	INTERVENTO DA DCS: APERTURA FV-05	D
BE 48	INTERVENTO INDEBITO DA DCS: CHIUSURA PV-05	D

I cut set di ordine 2 sono tutti corrispondenti ad uno stesso scenario: sabotaggio della PSV e intervento indebito mediante DCS; con riferimento agli eventi di categoria D, le possibili azioni mitigative sono in primo luogo relative al "controllo accessi" alla sala controllo.

Gli eventi di base BE 8, BE 16, BE 48 risultano comuni a tutti i cut se di ordine 2 (è opportuno osservare come BE8 era già stato identificato, in sede di analisi d'importanza, come evento particolarmente significativo). Una possibile misura preventiva consiste quindi nel limitare la possibilità di modifica (ad esempio mediante l'utilizzo di password) dei valori di set degli allarmi PAH-11 e PAHH-11 e di comando da remoto delle valvole di regolazione PV3 e PV5 (allarmi e controlli "protetti").

Ripercorrendo l'Analisi dei cut set dell'Albero delle Vulnerabilità, occorre definire 2 distinte categorie di sabotaggio: D' - intervento mediante DCS su allarmi / controlli "semplici"; D" - intervento mediante DCS su allarmi / controlli "protetti". L'evento di categoria D' richiede la capacità di accesso fisico alla Sala controllo e la conoscenza delle informazioni sensibili necessarie per una efficace manomissione dell'impianto. L'evento di categoria D" richiede la capacità di accesso fisico alla Sala controllo e la conoscenza delle informazioni sensibili necessarie per poter accedere agli allarmi / controlli "protetti" (password) e realizzare una efficace manomissione dell'impianto. In seguito alla adozione di una tale misura di prevenzione, i cut set in oggetto assumono ordine 3.

In Figura 7 sono riportati i risultati avuti dall'Analisi di importanza dei singoli eventi di base, realizzata a valle dell'introduzione della suddetta misura preventiva, per i cut set di ordine 3. L'approccio sopra descritto può quindi essere adottato per identificare e valutare l'efficacia di ulteriori misure di riduzione del rischio.

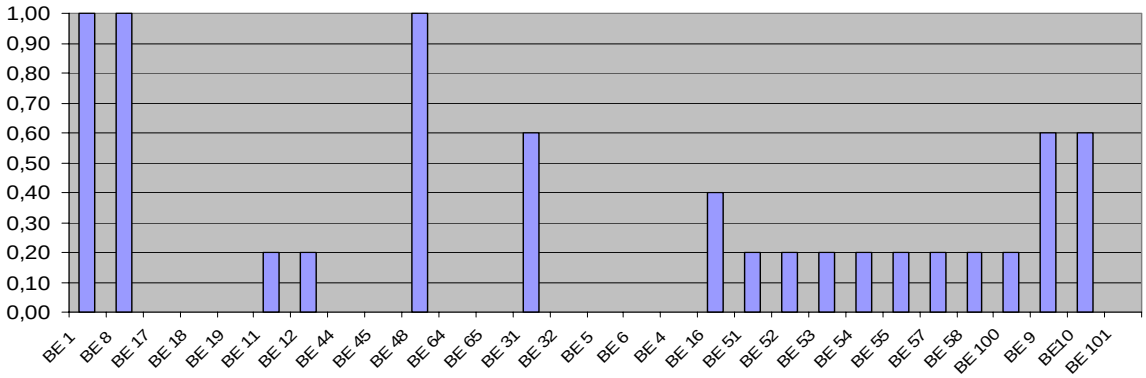

Figura 7. Analisi d'importanza: cut set ordine 3

5.0 CONCLUSIONI

L'esperienza condotta ha permesso di mettere a fuoco alcuni aspetti che da un lato distinguono l'approccio classico della risk analysis in ambito safety da quello proposto in ambito security e dall'altro permettono di ottenere risultati utili in campo antiterrorismo partendo da quanto già di norma sviluppato dagli stabilimenti a rischio per ottemperare agli obblighi normativi in materia d'incidenti rilevanti.

Innanzitutto, si è riscontrato come, di norma, un'analisi condotta al fine di individuare i top events possibili per un impianto industriale, ad esempio mediante la metodologia Hazop, venga condotta in ambito safety facendo alcune assunzioni che non possono essere valide in ambito security. Nel caso studiato, ad esempio, le principali differenze in proposito sono state:

- le valvole d'intercettazione manuale delle linee e della strumentazione escluse dall'analisi safety, come sovente accade se non è previsto il loro impiego per la normale operatività dell'impianto, debbono necessariamente essere considerate se si analizzano le possibili azioni di sabotaggio;

- le distinzioni fra diverse modalità di guasto di componenti, utile in ambito safety per una corretta quantificazione del rischio, non hanno una corrispondenza biunivoca con le modalità di sabotaggio ipotizzabili in ambito security.

D’altro canto la metodologia proposta permette di individuare le modalità di sabotaggio che possono produrre gli eventi incidentali identificati mediante le analisi realizzate in ambito safety a patto che, durante lo sviluppo dell’analisi HAZOP, siano state analizzate tutte le deviazioni dei parametri indipendentemente dall’esistenza di cause (guasto dei componenti) capaci di produrle.

La generalizzazione della metodologia HAZOP mediante integrazione con l’Analisi delle modalità di sabotaggio ha permesso lo sviluppo di un “Albero delle vulnerabilità”, finalizzato alla analisi delle condizioni di “sabotaggio multiplo”.

Gli eventi di base dell’Albero delle vulnerabilità presentano una evidente dipendenza in relazione alla tipologia dei componenti coinvolti ed alla loro “accessibilità”. L’approccio proposto per formalizzare le dipendenze tra i singoli eventi di sabotaggio consiste nel definire opportune categorie di eventi. Gli eventi appartenenti a diverse categorie sono considerati tra loro indipendenti. Eventi caratterizzati dalla stessa accessibilità fisica dei componenti coinvolti e delle informazioni (sensibili) necessarie per una efficace manomissione, sono considerati appartenenti alla stessa categoria. Lo sviluppo dell’albero delle Vulnerabilità ha permesso l’identificazione delle combinazioni di eventi necessari e sufficienti per la realizzazione dello scenario incidentale (Analisi dei cut set) e l’identificazione di eventi/componenti “critici” (Analisi d’importanza). Il quadro che emerge dall’Albero delle vulnerabilità permette di sottolineare, ancora una volta, come lo scenario incidentale in oggetto assuma criticità rilevante non solo in relazione a possibili guasti dei componenti dell’impianto ma anche alla possibilità di provocarlo, in modo intenzionale, mediante una adeguata strategia di sabotaggio. Inoltre, i risultati ottenuti permettono di identificare in dettaglio possibili misure preventive da adottare e di misurarne l’efficacia nel ridurre la vulnerabilità dell’impianto.

In conclusione, il lavoro svolto ha permesso di verificare come sia effettivamente possibile condurre, per un impianto a rischio d’incidente rilevante, un’efficace analisi antiterrorismo a partire dalle valutazioni già svolte in ambito safety. Inoltre, non si ritiene superflua un’integrazione in tal senso in quanto, in generale, non c’è corrispondenza fra il contributo che gli scenari identificati in ambito safety ed in ambito security possono avere sul livello di rischio complessivo. Infine, un successivo sviluppo delle metodologia esposta può consistere nella generalizzazione dell’Analisi d’importanza a partire da una stima “semi-quantitativa” delle caratteristiche di accessibilità dei componenti coinvolti e delle informazioni sensibili associate.

RIFERIMENTI

1. Haimes, Y.Y., Horowitz, B.M., Modeling interdependent infrastructures for sustainable counterterrorism, Journal of Infrastructure System, 10, pp. 33-42.
2. Petterson, S.A., Apostolakis, G.E., Identification of critical locations across multiple infrastructures for terrorist action, Safeguarding National Infrastructures: Integrated Approaches to Failure in Complex Networks, University of Glasgow, August 25-27, 2005
3. Apostolakis, G.E., Lemon, D.M., A screening methodology for the identification and ranking of infrastructure vulnerabilities due to terrorism, Risk Analisys, 25, No. 2, 2005, 361-376.
4. Brown, M.D., Lowe, A.S., Reference Manual to Mitigate Potential Terrorist attacks against Buildings, Federal Emergency Management Agency (FEMA), Risk Management Series, 426, December 2003.
5. Krimgold, F., Hattis. D.B., Whiddon, W.I., Insurance, Finance and Regulation Primer for Terrorism Rick Management in Buildings, Federal Emergency Management Agency (FEMA), Risk Management Series, 429, December 2003.
6. Chapman, R.E., Leng, C.J., Cost-Effective Responses to Terrorist Risks in Constructed Facilities, National Institute of Standards and Technology (NIST), NISTIR 7073, March 2004.
7. Bardazza, M., Vestrucci, P., Zappellini, G., Adinolfi, P., Buldrini, M., La Rovere, S., Vercilli, C., Application of a Systematic Methodology to Terrorism Risk Management, SAFE2005, Rome.
8. Vestrucci, P., Zappellini, G., Buldrini, M., Vercilli, C., La Rovere, S., Analisi del rischio terrorismo per un sito industriale, 3ASI Conference 2005, Rome.
9. Vestrucci, P., Zappellini, G., Buldrini, M., Vercilli, C., La Rovere, S., A systematic methodology to terrorism risk analysis, PSAM8, New Orleans, May 2006.
10. A guide to hazard and operability studies, Chemical Industries associated Ltd (CIA), CISHEC/8906/1000, London UK.