VALUTAZIONE DELLA VULNERABILITA' DI SITI INDUSTRIALI AD ATTACCHI ESTERNI

Cozzani, V.[1,3], Sabatini, M.[2], Zanelli, S.[2,3]
(1) Dipartimento di Ingegneria Chimica, Mineraria e delle Tecnologie Ambientali, Alma Mater Studiorum - Università di Bologna, viale Risorgimento 2, 40136 Bologna, Italy
(2) Dipartimento di Ingegneria Chimica, Chimica Industriale e Scienza dei Materiali, Università di Pisa, via Diotisalvi 2, 56126 Pisa, Italy
(3) CONPRICI, Consorzio Nazionale per la Prevenzione e la Protezione dai Rischi Chimico-Industriali, via Martelli 22/24, 40138 Bologna

SOMMARIO

Le potenziali conseguenze di attacchi esterni o di atti di sabotaggio a siti industriali in cui sono presenti quantitativi rilevanti di sostanze pericolose (industria chimica e di processo) o composti di elevatissima tossicità (industria farmaceutica) sono estremamente severe. A seguito degli eventi dell'11 settembre 2001 negli Stati Uniti e dell'11 marzo 2004 in Spagna il problema è diventato di forte attualità. Il presente studio è stato dedicato allo sviluppo di uno strumento per la valutazione quantitativa della vulnerabilità di un sito industriale ad attacchi esterni. Sono stati utilizzati metodi specifici per definire le tipologie di attacco esterno ragionevolmente ipotizzabili nell'attuale contesto. Sono quindi state identificate le possibili categorie di bersaglio. La disponibilità di modelli di danno per la valutazione della resistenza strutturale delle apparecchiature a sollecitazioni quali onde di pressione e proiettili, sviluppati in studi precedenti, è stata il presupposto per sviluppare modelli specifici di vulnerabilità delle diverse tipologie di apparecchiature rispetto ad attacchi esterni. Sulla base dei modelli di vulnerabilità sono stati definiti gli scenari di rilascio di riferimento. L'applicazione di modelli convenzionali per l'analisi delle conseguenze ha quindi consentito di identificare le zone di danno.

1 INTRODUZIONE

Le potenziali conseguenze di attacchi esterni o di atti di sabotaggio a siti industriali in cui sono presenti quantitativi rilevanti di sostanze pericolose (industria chimica e di processo) o composti di elevatissima tossicità (industria farmaceutica) sono estremamente severi. A seguito degli eventi dell'11 settembre 2001 negli Stati Uniti e dell'11 marzo 2004 in Spagna il problema è diventato di forte attualità. E' evidente come la protezione dei numerosi siti ed infrastrutture dell'industria di processo, spesso estremamente estese o disperse sul territorio, rappresenti un elemento fondamentale per la sicurezza della popolazione e per la compatibilità territoriale degli impianti di processo in sui siano presenti quantità rilevanti di sostanze potenzialmente pericolose. Una risposta basata solo sulla "security" è evidentemente insufficiente, data la complessità dei sistemi di protezione da mettere in campo e la difficoltà di proteggere strutture di notevoli dimensioni da attacchi potenzialmente condotti con mezzi potenzialmente anche tecnologicamente avanzati [1].

L'applicazione dei metodi di "security and vulnerability assessment" (SVA), normati dalla API o dalla SFK tedesca [2,3], rappresenta una prima risposta qualitativa al problema. Tuttavia, non è mai stato affrontato il problema della valutazione quantitativa della vulnerabilità di un sito ad attacchi esterni dal punto di vista della valutazione delle potenziali conseguenze degli scenari incidentali innescati. Un valutazione quantitativa delle distanze potenziali di danno rappresenta infatti un primo strumento per la valutazione del rischio associato a questa tipologia di eventi, nonchè per pianificare la risposta sul territorio ad eventuali emergenze.

Il presente studio è stato dedicato allo sviluppo di uno strumento per la valutazione quantitativa della vulnerabilità di un sito industriale ad attacchi esterni. I metodi SVA disponibili in letteratura sono stati utilizzati per definire le tipologie di attacco esterno ragionevolmente ipotizzabili nell'attuale contesto. Sono quindi state identificate le possibili categorie di bersaglio, attraverso un censimento delle diverse tipologie di apparecchiatura presenti in impianti di processo associato alla stima degli hold-up specifici (definiti come rapporti tra fluido potenzialmente rilasciato e volume dell'apparecchiatura) ed all'identificazione degli scenari di riferimento per il rilascio di sostanze pericolose a seguito delle diverse tipologie di attacco. La disponibilità di modelli di danno per la valutazione della resistenza strutturale delle apparecchiature a

sollecitazioni quali onde di pressione e proiettili, sviluppati in studi precedenti, è stata il presupposto per sviluppare modelli specifici di vulnerabilità delle diverse tipologie di apparecchiature rispetto ad attacchi esterni. Sulla base dei modelli di vulnerabilità sono stati definiti gli scenari di rilascio di riferimento. L'applicazione di modelli convenzionali per l'analisi delle conseguenze ha quindi consentito di identificare le zone di danno.

2 IDENTIFICAZIONE DEI POTENZIALI BERSAGLI

2.1 Identificazione delle installazioni critiche

Il punto di partenza nella stima del rischio dovuto ad attacchi esterni a siti in cui siano presenti sostanze pericolose (impianti di processo o stoccaggi) può essere diverso a seconda degli obiettivi dell'analisi. Gli attacchi possono essere suddivisi in "mass casualty attacks" (vale a dire attacchi il cui scopo è uccidere indiscriminatamente il maggior numero di persone) e "mass destruction attacks" (in cui si mira anche a distruggere insediamenti urbani e stabilimenti industriali). Per entrambe le tipologie di attacco, un primo approccio alla valutazione delle probabilità dello stesso, proposto tra gli altri da [4], è basato sulla determinazione di svariati fattori, quali il valore simbolico dello stabilimento da un punto di vista politico, il valore strategico ed economico dello stesso, la vicinanza o meno ad aree densamente abitate, il grado di sorveglianza dell'impianto, oltre naturalmente al tipo di danno che le sostanze presenti possono provocare. I metodi SVA sviluppati dalla API propongono di determinare in modo sistematico la probabilità di attacco esterno ad un sito in base ai seguenti fattori [2,5]:

- attrattività del bersaglio, che rappresenta il grado di interesse dell'avversario nell'attaccare il bersaglio
- entità delle minacce al bersaglio, dove con minaccia si intende l'esistenza di un avversario, dei suoi intenti, motivazioni, capacità e conoscenze specifiche
- vulnerabilità del bersaglio, definita come la probabilità di riuscita di un attacco riuscito condizionata al verificarsi dell'attacco stesso

Il fattore più complesso da valutare è però relativo all'attrattività del bersaglio. Nel metodo API/SVA [2] questa viene valutata sulla base dei seguenti fattori: l'utilità delle sostanze di processo come mezzo per causare un grave danno; la presenza di sostanze che possono essere usate come armi chimiche o come loro precursori; la prossimità dell'impianto ad istituzioni governative o luoghi simbolici; il grado di accessibilità e di sorveglianza del bersaglio; la fama e l'importanza del marchio o dell'azienda proprietaria; il valore simbolico del bersaglio; la riconoscibilità del bersaglio. Accettando questo punto di vista, perciò, si introducono nella valutazione forti fattori di incertezza dovuti alla necessità di stimare fattori aleatori, in particolare rispetto al valore simbolico ed alla riconoscibilità del bersaglio.

Un approccio più pragmatico al problema è stato proposto in Europa dalla Commissione Tedesca per gli Incidenti Rilevanti (Stör-fall Kommission, SFK) nell'ambito di una revisione della normativa in materia di sicurezza degli impianti chimici per valutare se essa fosse rispondente alle esigenze di security [3]. La commissione ha individuato due categorie di potenziali bersagli:

- Impianti soggetti ad obbligo di rapporto di sicurezza (articolo 8) rispetto alla Direttiva 96/82/EC ("Seveso II")
- Impianti soggetti ad obbligo di notifica (articolo 6) rispetto alla Direttiva 96/82/EC posti vicino ad installazioni sensibili (strutture destinate a contenere un grande numero di persone come scuole, punti di ritrovo, ospedali, stazioni, etc...) in cui un eventuale incidente o attacco possa dare luogo a conseguenze severe anche per tali strutture.

Questo secondo criterio è meno soggetto alla valutazione di fattori incerti o variabili nel tempo, e sembra prestarsi meglio all'identificazione dei possibili bersagli di attacchi esterni nel contesto europeo. L'applicazione del criterio richiede però l'analisi contestuale degli scenari incidentali potenzialmente provocati da attacchi esterni e della vulnerabilità del territorio intorno all'installazione individuata come potenziale bersaglio di attacco. Infatti gli scenari analizzati nei rapporti di sicurezza o nelle notifiche non sono in generale sufficienti a coprire l'insieme degli incidenti potenziali che hanno come evento iniziatore attacchi esterni.

E’ quindi evidente ai fini dell’identificazione dei bersagli potenziali l’importanza di sviluppare metodi specifici per valutare l’entità delle conseguenze attese di attacchi esterni in funzione della tipologia di attacco ipotizzabile e della vulnerabilità del bersaglio all’attacco.

2.2 Identificazione degli “asset critici”

Una volta identificata un installazione come possibile bersaglio di attacco esterno in generale è necessario valutare gli “asset critici” o i bersagli maggiormente vulnerabili all’interno dell’installazione. Infatti in generale tutti i metodi di “security” suggeriscono di adottare sistemi di protezione “stratificata”, vale a dire rendere più strette le misure di sorveglianza delle sezioni o zone di impianto in cui sono presenti apparecchiature a grande rischio potenziale o particolarmente vulnerabili ad attacchi esterni.

E’ evidente quindi la necessità di un approccio alla valutazione della criticità di una singola apparecchiatura, basata su criteri di inventario e di identificazione degli scenari potenziali conseguenti ad attacchi esterni. La sicurezza intrinseca della singola apparecchiatura è inoltre un fattore essenziale nella corretta valutazione della sua criticità rispetto ad attacchi esterni.

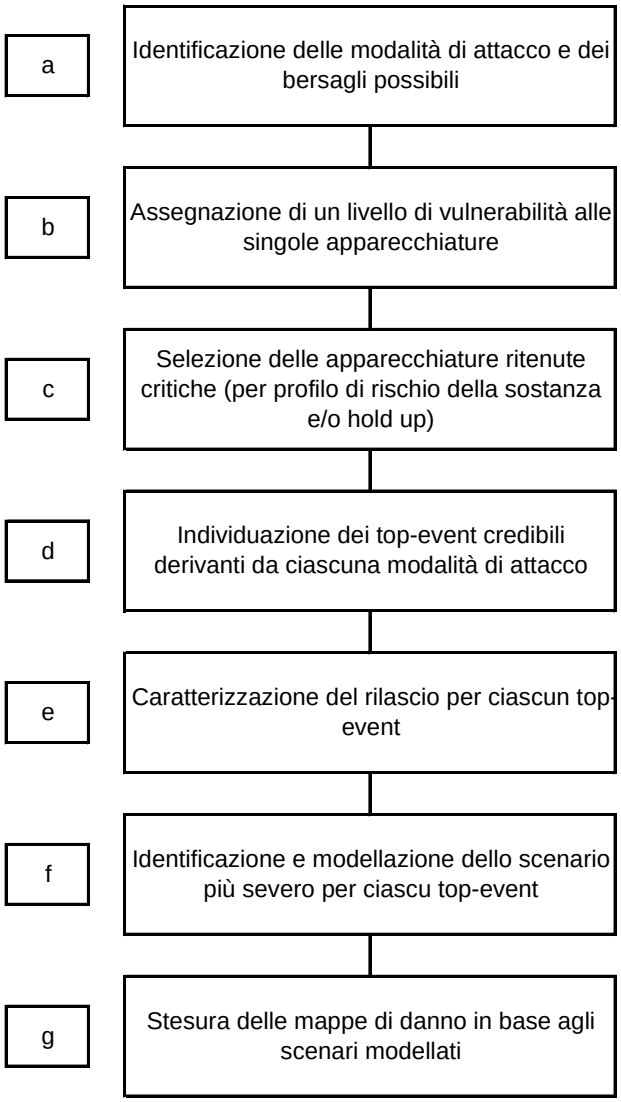


Figura 1. Procedura sviluppata per la valutazione delle conseguenze di attacchi esterni ad un sito industriale

2.3 Mitigazione degli impatti potenziali

Per "security" di un installazione industriale si intende la protezione delle unità produttive e logistiche da pericoli e da minacce, al fine di ridurre i rischi derivanti da azioni di vandalismo, sabotaggio o terrorismo. Alcuni autori [7,8] hanno introdotto quelli che vengono considerati gli step fondamentali della security:

- **Detect**, cioè rilevare la minaccia (intrusione, tentativo di attacco…);
- **Delay**, ritardare il più possibile l'attacco mediante le misure di security;
- **Response**, quindi reagire nel miglior modo e prima possibile;
- **Mitigate**, fare in modo di minimizzare le conseguenze mediante sistemi di sicurezza sia attiva che passiva.

In questo contesto, l'identificazione degli scenari potenziali a seguito di attacco esterno diventa quindi un elemento chiave anche per le fasi di risposta e mitigazione degli eventi.

Tabella 1. Tipologie di attacco esterno considerate.

Tipo di attacco	Descrizione
1. Sabotaggio	Effettuazione di operazioni errate: variazione delle condizioni di processo (concentrazione, temperatura pressione), apertura/chiusura valvole, disattivazione allarmi
2. Incidente provocato da veicolo	Danneggiamento di apparecchiature o strutture causato da impatto voluto con automezzo lanciato alla massima velocità possibile nel contesto di riferimento
2. Incidente provocato da aereo	Danneggiamento di apparecchiature o strutture causato da impatto voluto con un aereo di piccole dimensioni
3. Interferenza con mezzi improvvisati	Danni a sistemi di controllo e/o sicurezza; lievi danni ad apparecchiature e/o tubazioni (es fori di piccolo diametro)
4. Interferenza con strumenti o attrezzature specifiche	Danni a sistemi di controllo e sicurezza, danni di media entità ad apparecchiature e/o tubazioni
5. Incendio con mezzi improvvisati	Innesco di fluidi infiammabili presenti nel processo o incendio di installazioni periferiche dell'impianto quali uffici o simili
6. Incendio con bombe o sistemi incendiari	Incendio innescato mediante liquidi infiammabili esterni al processo, attraverso bombe incendiarie o dispositivi azionati a distanza
7. Esplosivi	Posizionamento di cariche esplosive all'interno o all'esterno dell'impianto
8. Attacco con armi da fuoco di piccolo calibro	Attacco alle apparecchiature dell'impianto con proiettili di piccolo diametro, in grado di causare danni ad apparecchiature o sistemi di controllo a distanza
9. Attacco con armi da fuoco di grosso calibro o missili	Attacco alle apparecchiature dell'impianto con proiettili di grosso calibro o missili

3 PROCEDURA SVILUPPATA PER LA VALUTAZIONE DI VULNERABILITÀ DI UN SITO

Deve preliminarmente essere precisato che nel presente contesto per "vulnerabilità" di un sito o di un'installazione si intenderà esclusivamente la possibilità di dare origine a rilasci seguiti da scenari incidentali severi a seguito di attacchi esterni. Non verranno quindi presi in considerazione gli elementi specifici relativi alla "security" (intelligence, controllo e limitazione degli accessi, sistemi anti-intrusione, etc.), che influenzano la probabilità di successo dell'attacco, ma solo gli elementi tecnologici (caratteristiche impiantistiche e strutturali delle apparecchiature, inventari di sostanze pericolose, sistemi attivi e passivi di protezione) che determinano le potenziali conseguenze di un attacco condotto con successo.

La metodologia sviluppata ha i seguenti obiettivi: caratterizzare i rilasci e gli scenari incidentali che possono seguire ad un attacco condotto con successo e determinare i raggi di danno degli scenari potenziali. Da questo punto di vista la procedura permette quindi di valutare il rischio intrinseco associato ad attacchi esterni ad un sito industriale, indipendentemente dall'efficacia delle misure di protezione specifiche messe in atto. I risultati costituiscono quindi un importante punto di partenza per definire una scala di criticità e di priorità di intervento, permettendo di individuare i siti critici e le installazioni da proteggere, nonchè le tipologie di scenari e quindi le misure di mitigazione da mettere in atto.

La figura 1 riporta lo schema concettuale della procedura sviluppata. La procedura sviluppata è basata sull'identificazione delle modalità di attacco e su una classificazione di criticità dell'apparecchiatura, basata su criteri di inventario, di pericolosità delle sostanze contenute e del relativo stato fisico. Sulla base dell'analisi di questi due elementi, è possibile caratterizzare l'entità e la tipologia del rilascio atteso, gli scenari incidentali conseguenti e le relative mappe di danno. Un punto essenziale della procedura è la valutazione della probabilità di successo dell'attacco in base ad una specifica modellazione della vulnerabilità dell'apparecchiatura.

Tabella 2. Esempio dei risultati dell'analisi delle diverse tipologie di attacco esterno

MODALITA' DI ATTACCO	Sabotaggio
BERSAGLI POSSIBILI	Valvole, sistemi di controllo e di allarme, situati sia in campo che in sala comandi.
EVENTO PROVOCATO	Funzionamento errato o mancato di un componente; errato svolgimento di operazioni di processo e/o una mancata segnalazione di anomalie. Nel caso di aperture/chiusure non previste di valvole si può avere un flusso di sostanze non previsto o mancato da o verso un'apparecchiatura.
TIPO DI RILASCIO ATTESO	Rilascio di tipo 1, causato da un aumento di pressione o temperatura da PSV o disco di rottura; in alternativa il trafilamento da una flangia. L'apertura intenzionale di dispositivi di drenaggio o depressurizzazione potrà causare il rilascio del contenuto dell'apparecchiatura o della tubazione
GRADO MINIMO DI CONOSCENZA NECESSARIO	Livello C: è necessaria una conoscenza dettagliata dei sistemi di controllo e di allarme dell'impianto, presumibilmente acquisita anche attraverso informazioni provenienti dall'interno.

4 IDENTIFICAZIONE DELLE TIPOLOGIE DI ATTACCO

4.1 Modalità di attacco esterno

Le tipologie possibili di attacco esterno o sabotaggio ad un sito industriale sono molteplici. Varie classificazioni sono state proposte nell'ambito degli approcci sviluppati per le SVA di un sito industriale. Nel presente approccio, le tipologie di attacco esterno prese in considerazione sono state derivate da una riorganizzazione ed integrazione di quelle considerate nella metodologia SVA proposta da API [2]. La tabella 1 riporta le tipologie di attacco esterno considerate e la relativa definizione.

La caratterizzazione delle conseguenze delle diverse tipologie di attacco ha richiesto un'analisi approfondita delle diverse modalità individuate in tabella 1, finalizzate a determinare in modo dettagliato i seguenti parametri:

- Bersagli possibili: quali apparecchiature, installazioni o zone dell'impianto possono essere oggetto del tipo di attacco in esame
- Evento provocato: effetto atteso dell'attacco sulle diverse tipologie di bersaglio individuate

- Tipo di rilascio atteso: entità del rilascio rispetto a 4 categorie specificamente definite al fine di poter quantificare le conseguenze dell'evento
- Grado di conoscenza richiesto: livello di informazioni richieste per poter organizzare e portare l'attacco con successo

La tabella 2 riporta un esempio dei risultati dell'analisi. La tabella 3 riporta la descrizione dei gradi di conoscenza definiti in funzione della possibilità di organizzare e condurre efficacemente l'attacco. La tabella 4 riporta la descrizione delle tipologie di rilascio considerate.

Tabella 3. Gradi di conoscenza richiesti per le diverse tipologie di attacco.

LIVELLO DI CONOSCENZA	DESCRIZIONE
A	Nessuna conoscenza specifica dell'impianto, a parte la sua localizzazione e la dislocazione delle apparecchiature
B	Conoscenza sommaria delle sostanze e del layout dell'impianto (acquisibile anche tramite osservazioni dall'esterno o visite guidate dell'impianto)
C	Conoscenza approfondita dell'inventario dell'impianto e dei dettagli del processo produttivo, acquisita presumibilmente attraverso informazioni fornite dall'interno

Tabella 4. Categorie di rilascio considerate nella classificazione.

TIPO DI RILASCIO	DESCRIZIONE	CARATTERISTICHE QUANTITATIVE
1	Rilasci continui da PSV, DR, valvole di drenaggio o di servizio	Diametro equivalente da 6 a 50 mm (massimo 2")
2	Rilasci continui da fori con diametro equivalente a quelli delle linee di processo	Diametro equivalente da 2" a 10"
3	Rilasci continui di grande portata e durata limitata	Hold up rilasciato in 10 minuti
4	Rilasci istantanei derivanti da rottura catastrofica	---

4.2 Modalità di identificazione dei bersagli

Le tipologie di bersagli credibili possono essere in alcuni casi relazionate alle tipologie di attacco esterno. Infatti la credibilità del successo dell'attacco è condizionata dalle caratteristiche del bersaglio. D'altronde, alcune tipologie di attacco possono portare a tipologie specifiche di bersaglio. D'altronde, anche le procedure per identificare, nell'ambito della procedura sviluppata, i potenziali bersagli sono funzione della tipologia di attacco esterno messa in atto.

La tabella 5 evidenzia le diverse modalità che possono essere adottate per l'identificazione dei bersagli o degli eventi di rilascio conseguenti alle diverse tipologie di attacchi esterni. Come mostrato nella tabella, nel caso delle tipologie più severe di attacco esterno (attacco con esplosivi, con dispositivi incendiari, con armi da fuoco di grande calibro) le modalità di identificazione dei bersagli critici devono essere basate su una valutazione specifica, che tenga conto della vulnerabilità del bersaglio e dei sistemi di protezione presenti, discussi nel paragrafo successivo. Per altre tipologie di attacco, meno severe e meno organizzate, quali il sabotaggio, l'urto di veicoli, la vulnerabilità dei bersagli è minore e questo porta alla possibilità di utilizzare metodologie quali l'analisi di operabilità o la ricognizione del lay-out per identificare i bersagli credibili.

Tabella 5. Modalità di individuazione dei potenziali bersagli di attacchi esterni.

Tipo di attacco	Modalità di individuazione dei bersagli
1. Sabotaggio	Mediante l'Hazop si possono individuare i top-event potenziali; la revisione dei moduli HazOp permette di identificare le cause possibili dovute a sabotaggio.
2. Incidente provocato da veicolo	Mediante analisi del layout di impianto possono essere individuate le apparecchiature soggette ad attacco con automezzi
2. Incidente provocato da aereo	Classificazione specifica della vulnerabilità basata sulla matrice apparecchiatura/stato fisico e su criteri di inventario
3. Interferenza con mezzi improvvisati	Mediante Hazop e analisi del layout relativa all'accessibilità delle apparecchiature da parte di esterni
4. Interferenza con strumenti o attrezzature specifiche	Classificazione specifica della vulnerabilità basata sulla matrice apparecchiatura/stato fisico e su criteri di inventario
5. Incendio con mezzi improvvisati	Sostanze infiammabili presenti nel processo (tubazioni o serbatoi); uffici o altre installazioni a rischio incendio per presenza di materiale infiammabile
6. Incendio con bombe o sistemi incendiari	Classificazione specifica della vulnerabilità basata sulla matrice apparecchiatura/stato fisico e su criteri di inventario
7. Esplosivi	Classificazione specifica della vulnerabilità basata sulla matrice apparecchiatura/stato fisico e su criteri di inventario
8. Attacco con armi da fuoco di piccolo calibro	Classificazione specifica della vulnerabilità basata sulla matrice apparecchiatura/stato fisico e su criteri di inventario
9. Attacco con armi da fuoco di grosso calibro o missili	Classificazione specifica della vulnerabilità basata sulla matrice apparecchiatura/stato fisico e su criteri di inventario

5 IDENTIFICAZIONE DEI BERSAGLI CRITICI E DEGLI SCENARI INCIDENTALI

5.1 Identificazione dei bersagli critici

L'identificazione dei bersagli critici e la valutazione della criticità di questi deve essere effettuata in base a. tre parametri:

- pericolosità delle sostanze contenute, che determina l'impatto potenziale di un rilascio
- stato fisico delle sostanze pericolose contenute, che determina gli scenari incidentali specifici attesi
- quantità di sostanze pericolose contenute, che determina l'estensione massima potenziale dei raggi di danno degli scenari attesi

La prima fase dell'analisi consiste nell'identificare i rilasci potenziali in una o più delle seguenti categorie: rilasci di sostanze tossiche o pericolose per l'ambiente; incendi; esplosioni. Questi sono legati alla presenza nell'inventario delle singole apparecchiature di sostanze tossiche, infiammabili o nocive per l'ambiente.

La seconda fase del lavoro è legata alla valutazione della modalità con cui lo stato fisico di una sostanza influenza gli scenari potenziali. E' noto infatti che gli scenari incidentali credibili sono grandemente influenzati dallo stato fisico, dalla temperatura e dalla pressione della sostanza al momento del rilascio. E' inoltre possibile associare alle diverse tipologie di apparecchiature, in funzione dell'operazione di processo effettuata, lo stato fisico in cui normalmente sono presenti le sostanze contenute.

Associando la tipologia di pericolo e lo stato fisico della sostanza alle condizioni operative della tipologia di apparecchiatura considerata è stato possibile ottenere la tabella 6, che mostra gli scenari incidentali attesi per sostanze infiammabili in funzione dello stato fisico e della categoria di apparecchiatura. Una tabella analoga è stata ottenuta per le sostanze tossiche, ma non è stata riportata per motivi di spazio. Ai fini dell'analisi condotta, sono state considerate solo le seguenti classi di apparecchiature: serbatoi; tubazioni di grande

diametro; colonne, sia di assorbimento che di distillazione, in cui la temperatura operativa è in genere maggiore di quella atmosferica; reattori e scambiatori.

Tabella 6. Matrice per la determinazione della criticità delle apparecchiature.

Stato fisico → / Apparecchiat. ↓	GAS LIQUEFATTO IN PRESS.	LIQUIDO EVAPORANTE	GAS / LIQUIDO IN FASE VAPORE	LIQUIDO CRIOGENICO	LIQUIDO STABILE
SERBATOI	Fire ball (ist.) Flash fire / VCE (cont.)	Flash fire / VCE	Flash fire / VCE	Fire ball (ist.) Flash fire / VCE (cont.)	Pool fire
TUBAZIONI GRANDE DIAMETRO	Fire ball (ist.) Flash fire / VCE (cont.)	Flash fire / VCE	Flash fire / VCE	Fire ball (ist.) Flash fire / VCE (cont.)	Pool fire
COLONNE	Fire ball (ist.) Flash fire / VCE (cont.)	Flash fire / VCE	Flash fire / VCE	Flash fire / VCE	Pool fire
REATTORI / SCAMBIAT.	Fire ball (ist.) Flash fire / VCE (cont.)	Flash fire / VCE	Flash fire / VCE	Flash fire / VCE	Pool fire

Il terzo fattore da considerare è ovviamente l'entità del rilascio ipotizzabile. Per le apparecchiature questo è funzione dell'hold-up assoluto e del grado di pieno specifico, cioè il volume assoluto di sostanza contenuto nell'apparecchiatura ed il massimo grado di pieno ipotizzabile per la stessa nelle normali condizioni operative. E' evidente infatti che, tra due apparecchiature di ugual volume contenenti la stessa sostanza nelle stesse condizioni operative e nello stesso stato fisico, può essere considerata più pericolosa quella in grado di rilasciare quantità maggiori di sostanza pericolosa. Per le tubazioni l'entità del rilascio ipotizzabile è in generale associabile al diametro.

Sulla base di considerazioni relative ai parametri discussi in precedenza, può essere formalizzata la seguente scala relativa ad entità decrescenti del rilascio atteso: serbatoi di stoccaggio; tubazioni di diametro superiore a 250mm; colonne; tipologie convenzionali di reattori e scambiatori.

Sulla base della severità attesa per gli scenari incidentali identificati nella tabella 6 e della scala di severità dei rilasci attesi è stato possibile ottenere la tabella 7, che riporta una classificazione del livello di criticità del bersaglio potenziale in funzione della tipologia di apparecchiatura e dello stato fisico della sostanza presente. A parità di livello di criticità potenziale, deve considerarsi più critica l'apparecchiatura con maggiore hold-up o in grado di provocare il rilascio di maggiore entità (vedi tabella 4). E' chiaro che la tabella permette solo una classificazione comparativa per apparecchiature che contengano sostanze con analogo profilo di rischio (infiammabilità, classificazioni equivalenti di tossicità, etc.). Nel caso di diversi profili di rischio (ad esempio tossicità verso infiammabilità), non è possibile determinare a priori una classificazione di criticità. Questa può essere ottenuta solo dal confronto dei raggi di danno degli scenari incidentali ipotizzabili. D'altronde, la classificazione permette di identificare e selezionare per l'analisi in modo semplice i bersagli più critici tra quelli che hanno lo stesso profilo di rischio, richiedendo invece di considerare comunque bersagli con diversi profili di rischio.

5.2 Vulnerabilità delle singole apparecchiature

La vulnerabilità delle diverse tipologie di apparecchiatura identificate è un elemento determinante per stimare la probabilità di successo di un attacco (ovviamente limitatamente all'aspetto tecnico, ovvero alla possibilità che l'attacco possa dar luogo ad un rilascio di sostanze pericolose nell'ambiente). La vulnerabilità dipende ovviamente dalle caratteristiche specifiche dell'apparecchiatura e del tipo di attacco portato e deve essere stimata caso per caso. E' possibile, tuttavia, per alcune tipologie di attacco, ottenere indicazioni

generali sulla possibilità di danneggiamento dell'apparecchiatura e sulle distanze critiche in funzione dell'intensità dell'attacco portato.

Tabella 7. Matrice per la determinazione della criticità delle apparecchiature.

Stato fisico → / Apparecchiat. ↓	GAS LIQUEFATTO IN PRESS.	LIQUIDO EVAPORANTE	GAS / LIQUIDO IN FASE VAPORE	LIQUIDO CRIOGENICO	LIQUIDO STABILE
SERBATOI	**4**	**3**	**3**	**2**	**1**
TUBAZIONI GRANDE DIAMETRO	**4**	**3**	**2**	**2**	**1**
COLONNE	**3**	**2**	**2**	**2**	**1**
REATTORI / SCAMBIAT.	**3**	**2**	**1**	**1**	**1**

Tabella 8. Matrice per la determinazione della criticità delle apparecchiature.

Tipo di attacco	**Criterio di danneggiamento**	**Distanza di sicurezza**
Incendio con mezzi improvvisati o attacco con dispositivi incendiari (5,6)	Apparecchiature atmosferiche: $\ln(ttf) = -1.13 \cdot \ln(I) - 2.67 \cdot 10^{-5} \cdot V + 9.9$ Apparecchiature in pressione: $\ln(ttf) = -0.95 \cdot \ln(I) + 8.845 \cdot V^{0.032}$ ttf: time to failure, s V: volume del vessel (m^3)	Apparecchiature atmosferiche: irraggiamento 15 < kW/m^2 Apparecchiature in pressione: irraggiamento 40 < kW/m^2
Attacco con esplosivi (7)	Apparecchiature atmosferiche: Pr = -18.96 + 2.44 ln(P) Apparecchiature in pressione: Pr = -42.44 + 4.33 ln(P) Pr: probit P: sovrappressione di picco (Pa)	Apparecchiature atmosferiche: R = 1.8 Apparecchiature in pressione: R = 2 $R = \frac{r}{\left(E/P_0\right)^{0.33}}$ r: distanza (m) E: energia (kJ) P0: pressione atm. (kPa)
Attacco con armi da fuoco con proiettili non esplosivi (8,9)	Spessore atteso di perforazione: $t = 3.06 \cdot 10^{-7} \cdot \frac{W^{2/3} \cdot u^{4/3}}{d}$ t: spessore perforazione (mm) W: peso proiettile (kg) u: velocità proiettile (m/s) d: diametro proiettile (m)	Non disponibili

La procedura messa a punto ha richiesto lo sviluppo di correlazioni specifiche per la valutazione della vulnerabilità dei singoli elementi di impianto alle diverse modalità di attacco esterno ipotizzabili. La tabella 8 riporta un esempio dei risultati del lavoro svolto. In particolare, la tabella riporta i modelli di vulnerabilità che possono essere utilizzati per verificare la possibilità di danneggiamento del bersaglio per tre modalità di attacco: attacco con dispositivi incendiari, attacco con esplosivi, attacco con proiettili non esplosivi. I modelli sono relativi al danneggiamento di apparecchiature non protette. I modelli mostrati nella tabella 8 permettono rispettivamente la stima dei tempi di cedimento di apparecchiature coinvolte in incendi, la stima della probabilità di danneggiamento di un'apparecchiatura a seguito dell'onda d'urto di un esplosione e la stima della profondità di penetrazione di proiettili. Per ciascuna tipologia di danneggiamento sono inoltre state calcolate, quando possibile, le distanze di sicurezza in funzione dell'intensità dell'attacco.

Sulla base delle correlazioni sviluppate è possibile individuare l'estensione delle zone di protezione richieste in funzione della modalità e dell'intensità prevista per l'attacco esterno. Le valutazioni relative alla possibilità di danneggiamento permettono inoltre di individuare i rilasci e gli scenari incidentali credibili in funzione delle tipologie di attacco ipotizzate

5.3 Analisi dei "layers" di protezione

Un secondo elemento che determina la possibilità di riuscita e le conseguenze finali dell'attacco è l'analisi dei "layers" di protezione delle singole apparecchiature. I "layers" di protezione sono barriere passive, attive o gestionali che intervengono ad impedire il successo dell'attacco o a mitigarne le conseguenze. E' evidente quindi che i "layers" di protezione da considerare siano diversi in funzione del tipo di attacco.

L'analisi sviluppata ha permesso di individuare i "layers" di protezione potenzialmente disponibili rispetto ai diversi tipi di attacco. La figura 2 riporta un esempio dei "layers" di protezione rispetto all'attacco con veicoli ed all'attacco con dispositivi incendiari. L'analisi condotta è stata mirata ad individuare sia i "layers" di protezione non specifici rispetto alla "security", che quelli messi in atto (o potenzialmente adottabili) in funzione della protezione dalla specifica tipologia di attacco esterno.

L'analisi dei "layers" di protezione effettivamente presenti sulle singole apparecchiature permette quindi, attraverso il confronto con i "layers" potenzialmente adottabili (vedi figura 2), di verificare la presenza e la completezza dei sistemi di protezione adottati. Per i bersagli critici è inoltre possibile effettuare un'analisi quantitativa della probabilità e dell'entità del rilascio basata su tecniche convenzionali di LOPA (Layer of protection analysis).

6 ANALISI DELLE CONSEGUENZE DEGLI ATTACCHI ESTERNI

6.1 Alberi degli eventi

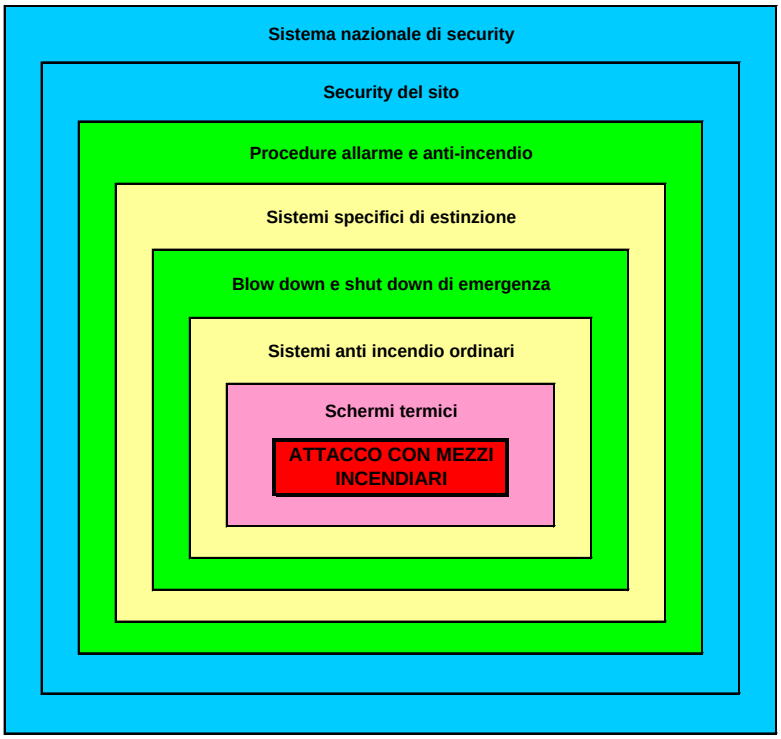
L'analisi delle conseguenze degli attacchi esterni è assolutamente analoga a quanto normalmente viene effettuato nell'analisi di sicurezza degli impianti di processo. In particolare, sulla base delle tipologie di rilascio (vedi tabella 4) attivate dalla modalità specifica dell'attacco esterno, nonchè dello stato fisico del fluido rilasciato, è possibile identificare gli scenari incidentali possibili con la tecnica dell'albero degli eventi.

Gli alberi degli eventi da adottare sono assolutamente analoghi a quelli normalmente utilizzati nell'analisi di rischio convenzionale. Tuttavia, nell'ambito della procedura sviluppata, al fine di permettere un'analisi comparativa dell'entità delle conseguenze attese, è stato definito un insieme di riferimento di alberi degli eventi da adottare in funzione della tipologia di rilascio e dello stato fisico della sostanza. La figura 3 mostra un esempio di albero degli eventi adottato come riferimento per il rilascio continuo di un liquido criogenico.

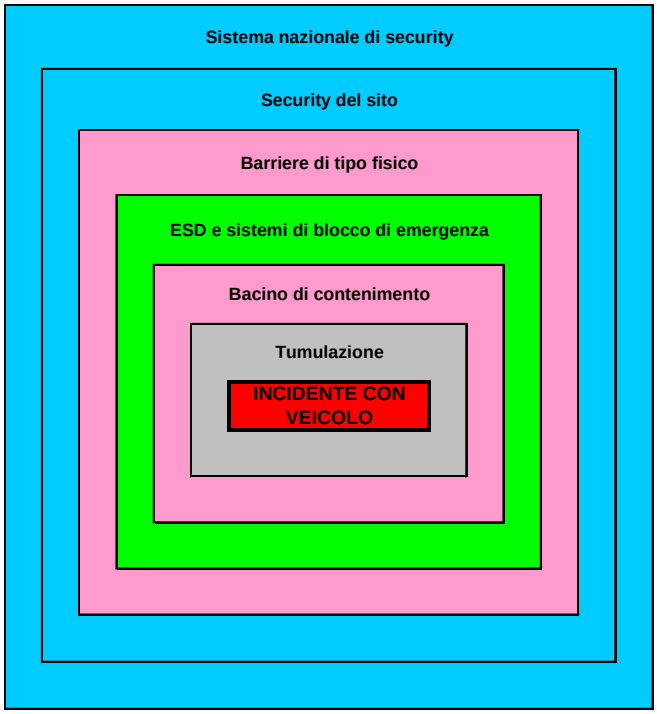
6.2 Mappe di danno

Sulla base dell'albero degli eventi e dell'entità del rilascio è possibile utilizzare i modelli convenzionali di analisi delle conseguenze per determinare le mappe di danno conseguenti ai singoli scenari incidentali. Le

mappe di danno così ottenute sono alla base dell'individuazione delle conseguenze degli attacchi esterni. Le mappe di danno relative alle apparecchiature critiche ed agli eventi più severe sono alla base delle attività di pianificazione dell'emergenza rispetto a questa tipologia di eventi.



(a)



(b)

Figura 2. "Layers" di protezione applicabili per due diverse tipologie di attacco esterno: (a) attacco con dispositivi incendiari e (b) attacco con veicolo

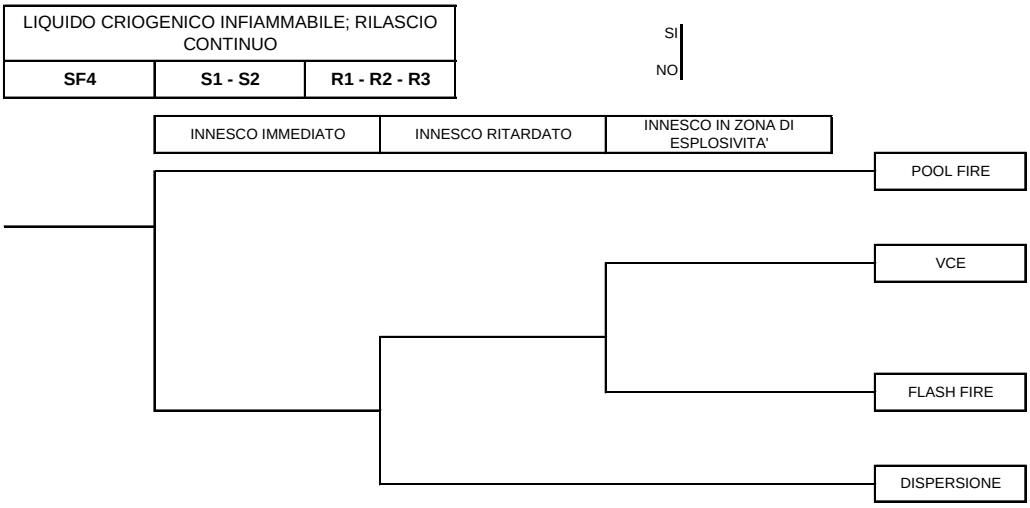


Figura 3. Esempio di albero degli eventi di riferimento adottato nell'analisi: rilascio continuo di liquido criogenico infiammabile

7 CONCLUSIONI

E' stata definita una metodologia per l'identificazione dei siti e dei bersagli critici rispetto ad attacchi esterni ad industrie di processo. La metodologia, che è stata applicata ad alcuni casi di studio (i cui risultati non sono stati riportati per esigenze di sintesi) permette di identificare le modalità credibili di attacco, la vulnerabilità e la criticità delle apparecchiature, gli scenari incidentali attesi a seguito del successo dell'attacco. I risultati ottenuti permettono sia di valutare la vulnerabilità di un sito e di prioritarizzare i bersagli potenziali da proteggere, che di impostare la pianficazione delle emergenze conseguenti ad attacchi esterni a siti industriali.

RINGRAZIAMENTI

Il presente studio è stato finanziato dalla Presidenza del Consiglio dei Ministri – Dipartimento della Protezione Civile, nell'ambito di una convenzione con il Consorzio CONPRICI.

RIFERIMENT

1. Moore, D.A., The new risk paradigm for chemical process security and safety, Journal of Hazardous Material 115, 2004, pp. 175 – 180.
2. American Petroleum Institute, National Petrochemical & Refinery Association, Security Vulnerability Assessment Methodology for the Petroleum and Petrochemical Industries, 2003.
3. Stör-fall Kommission (SFK), Report of the German Hazardous Incident Commission, SFK – GS – 38, www.sfk-taa.de
4. Coster, M.N., and Hankin, R.K.S., Risk Assessment of antagonistic hazard, Journal of Loss Prevention in the process industries 16, 2003, pp. 545 – 550
5. Moore, D.A., Application of the API/NPRA SVA methodology to transportation security issues, Journal of Hazardous Materials, 117, 2005, pp.130-138.
6. Bajpai, S., Gupta, J.P., Site security for chemical process industries, Journal of Loss Prevention 18, 2005, pp. 301 – 309.
7. Emerson, S.D., Nadeau, J., A coastal perspective on security, Journal of Hazardous Materials 104, 2003, pp. 1 – 13.