PROPOSTA DI UN SISTEMA INTEGRATO DI GESTIONE DELLA SICUREZZA E DELLA SECURITY (SGSS) PER IMPIANTI A RISCHIO DI INCIDENTE RILEVANTE

Geri F. [1], Luccone L.G.[2]
[1]Dipartimento Protezione Civile, via Ulpiano, Roma
[2]Dip. Ingegneria chimica, Università di Roma "La Sapienza", via Eudossiana 18, Roma, 00184

SOMMARIO

Dopo i fatti dell'11 settembre e altri attentati perpetrati contro impianti di processo e pipeline, l'approccio classico all'analisi del rischio industriale, e più in generale di tutte le analisi di rischio, è profondamente mutato. Gli aspetti e i problemi relativi alla Security, cioè quelli relativi alla protezione e alla prevenzione di possibili attacchi terroristici contro gli impianti industriali, devono sempre di più essere inclusi nel percorso di analisi del rischio attraverso la valutazione di nuovi parametri quali il "grado di attrazione", la vulnerabilità, la raggiungibilità di un determinato bersaglio inteso come centro di pericolo. Negli impianti industriali, i centri di pericolo, e quindi possibili target per attacchi intenzionali, costituiscono a loro volta una fonte di rischio in quanto la loro distruzione implica in primo luogo l'interruzione della produzione da parte dell'azienda ma in secondo luogo, e più importante, possono innescare effetti domino e rilascio di sostanze pericolose che possono a loro volta generare catene incidentali di ben più vasta portata. Si vuole qui presentare la proposta di un metodo di valutazione della vulnerabilità in termini di Security e l'integrazione della stessa Security nel tradizionale sistema di gestione della sicurezza.

1.0 INTRODUZIONE

Questo lavoro presenta un possibile approccio per l'implementazione di un sistema per la gestione della sicurezza e della Security (SGSS) a partire da quanto richiesto dalla normativa comunitaria Seveso ormai arrivata alla terza versione e dalle norme volontarie esistenti in ambito di gestione della sicurezza industriale (UNI EN 10617). È stato introdotto, poi, un nuovo parametro complessivo per stimare la criticità di un target, che viene determinato in maniera agevole a partire dalle sue caratteristiche in termini di Security (grado di attrazione, vulnerabilità e raggiungibilità). Il potenziale di danno risultante da un attacco intenzionale su un target può essere valutato con un approccio worst-case scenario con l'ipotesi che gli attentati terroristici provochino uno scenario catastrofico che coinvolge gran parte della quantità di sostanza confinata nell'unità di processo o nello stoccaggio. La procedura sopra descritta è di facile applicazione a partire dai risultati dell'analisi di rischio classica, anche se generalmente i rapporti di sicurezza includono solo una limitata quantità di scenari incidentali, ma anche in assenza di questi dati essa permette, con la sola conoscenza dei dati di base dell'impianto, di ottenere una valutazione di massima del grado di Security delle diverse unità.
Questo metodo speditivo, oltre a dare importanti informazioni sulla prioritizzazione degli interventi e delle contromisure, permette una razionalizzazione delle necessità dell'impianto in termini di Security e costituisce il dato in ingresso per la costruzione del sistema integrato di gestione della Safety e della Security (SGSS). Il sistema presentato nel lavoro è concepito con un approccio PDCA che fa tesoro degli schemi concettuali presenti nelle norme ISO 14001:2004, ISO 16017 e OHSAS 18001:1999 e tiene conto di quanto stabilito del DM 9.8.2000. Il sistema deve essere pensato come una serie di barriere in parallelo e include la definizione della struttura organizzativa, le responsabilità, il programma, l'analisi dei possibili scenari a seguito di attacchi, il grado di previsione degli stessi, i requisiti minimi in termini di procedure e di prestazioni per l'applicazione della "politica per la Safety e la Security". La procedura proposta può essere molto utile per gli impianti esistenti in quanto permette una revisione e una ridiscussione critica di possibili eventi incidentali. La visione allargata – che può far sì che il metodo possa essere utilizzato in sede di modifica di impianti esistenti o di definizione di layout per impianti nuovi – parte dalla valutazione di specifici parametri di singoli scenari incidentali. Altri parametri che permettono di raffinare il grado di pericolosità potenziale e che devono essere valutati in sede di stesura del rapporto di sicurezza integrato sono: accessibilità del sito, visibilità, possibilità di effetti domino, efficacia e tempestività dei soccorsi e delle azioni di mitigazione.

1.1 Definizioni operative

L'FBI definisce terrorismo come "*the unlawful use of force or violence against persons or property to intimidate or coerce a Government, the civilian population, or any segment thereof, in furtherance of political or social objectives*". Il Dipartimento di Giustizia Usa successivamente ha ben circostanziato la possibilità di attacco a stabilimenti chimici ponendo l'attenzione sulla potenzialità che queste azioni hanno di determinare rilasci di sostanze pericolose: "*Terrorists or other criminals are likely to view the potential of a chemical release from an industrial facility as a relatively attractive means of achieving [their] goals… breaching a containment vessel of an industrial facility with an explosive or otherwise causing a chemical release may appear relatively simple to such a terrorist. Therefore, someone seeking to cause the damage associated with weapons of mass destruction may instead seek to cause a chemical release from an industrial facility*".

Un *avversario* è un individuo, un gruppo, un'organizzazione, un governo, e i suoi servizi segreti, che perpetra attività che hanno lo scopo e la possibilità di apportare danni ai beni dell'azienda e della comunità.

Il *livello di minaccia* può essere definito il grado di attenzione [1,2] che deve essere mantenuto dal gestore dell'impianto per scongiurare la possibilità di attacchi terroristici. Una minaccia è definita come un'indicazione, una circostanza o un evento che ha il potenziale di danneggiare la proprietà.

In generale i possibili avversari possono essere raggruppati in tre gruppi principali:

- Interni;
- Esterni;
- Interni che lavorano in cooperazione con gruppi esterni.

Per *vulnerabilità della Security* [2] si intende ogni possibile debolezza che può essere penetrata da un avversario per raggiungere in maniera non autorizzata un bene, una risorsa, un elemento critico per la sicurezza (in definitiva tutto ciò che ha un valore positivo per l'azienda). La vulnerabilità di sicurezza va considerata in senso esteso fino alle pratiche di management.

Alcune possibili categorie di beni dell'azienda che possono essere target di attacco sono riassunte di seguito:

- Personale;
- Sostanze chimiche utilizzate o prodotte;
- Informazioni;
- Impianti e componenti;
- Attività;
- Operazioni.

Esistono due tipi di approccio per valutare e testare la vulnerabilità della Security:

- Approccio per scenario: si tratta di immaginare, guidati da check list, alcune possibilità di attacco su determinati target e andare ad analizzare quali possono essere le conseguenze;
- Approccio per selezione successiva dei target di interesse.

Alla base di qualsiasi approccio c'è la valutazione appetibilità del target: è necessario valutare il valore reale e quello percepito in termini di attrattiva.

Alcuni possibili fattori o classi di appetibilità del target di seguito elencati:

- Potenzialità di determinare un ingente numero di morti e feriti;
- Potenzialità di determinare danni estesi alla proprietà;
- Vicinanza a beni strategici dello Stato;
- Potenzialità di compromettere l'efficienza di infrastrutture e servizi di interesse nazionale;
- Facilità di accesso al target;
- Alta risonanza sui mezzi di comunicazione;
- Reputazione e visibilità dell'azienda;
- Target simbolo per la collettività (monumenti, chiese, …).

Un altro parametro da valutare è la probabilità di successo di un avversario in caso di attacco, grandezza complementare all'efficacia delle misure di protezione. Le contromisure, o misure di protezione, sono tutte quelle azioni atte a ridurre o eliminare una o più vulnerabilità per la Security.

I costi per le misure di sicurezza possono essere finanziari ma anche non finanziari, per esempio un costo può essere la perdita di efficienza operazionale, una certa pubblicità negativa, condizioni di lavoro non favorevoli. Spesso le conseguenze di alcune contromisure hanno ricadute politiche.

Le tipiche contromisure già intraprese o da intraprendere nell'industria di processo:

- Accesso ristretto e controllato agli impianti;

- Confinamento degli impianti e in particolare delle unità critiche in modo da renderle lontane e difficilmente raggiungibili tramite azioni penetrative via terra;
- Prevenzione e sconfinamento delle perdite;
- Controllo avanzato dell'inventario delle merci pericolose in entrata e in uscita;
- Incremento di sicurezza nelle sale controllo (DCS, PLC, sistemi di ultima generazione);
- Creazione di un'unità di crisi e di risposta all'emergenza anche in caso di attentato;
- Politiche e procedure specifiche per la Security;
- Cyber Security.

Le strategie per la mitigazione del rischio in termini di Security devono seguire un approccio detto "DDD" (Deter, Detect, Delay) che prevede l'installazione di una serie di barriere fisiche e no [2], nel dettaglio:

- Creazione di deterrenti in grado di scoraggiare eventuali attacchi. Classici e validi esempi sono le barriere fisiche di sicurezza come segnali, luci, guardie di sicurezza, telecamere, recinzioni multilivello, impedimenti per i veicoli, restrizione accessi anche per il personale dipendente;
- Rilevazione in tempo reale e preventiva per l'identificazione degli avversari e delle azioni di attacco;
- Ritardare tramite barriere indipendenti in serie l'accesso agli elementi critici.

Il concetto di porre delle barriere in serie per scongiurare la possibilità, abbattendone radicalmente la frequenza attesa di accadimento, vale anche per la Safety. Di seguito è proposto uno schema delle varie barriere a protezione del processo.

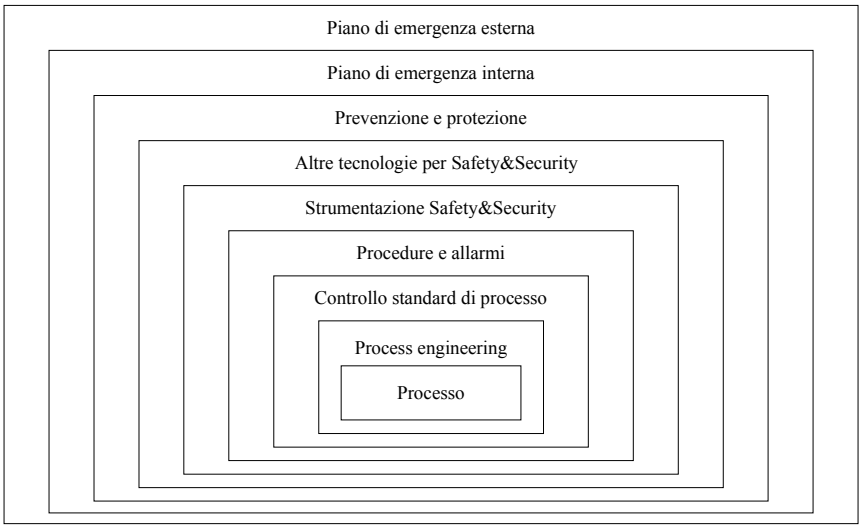

Figura 1. La stratificazione delle barriere di protezione e prevenzione

Va evidenziato che l'efficacia delle barriere è legata pure alla loro indipendenza: le barriere, infatti, non dovrebbero presentare cause di "rottura" in comune.

2.0 GENERALIZZAZIONE DEL CONCETTO DI INCIDENTE E CRITERI PER LA PREVISIONE DELLE CONSEGUENZE

La progettazione di un SGSS implica una riflessione preliminare sul concetto di incidente, sulle cause che lo determinano e sulle conseguenze. L'incidente, a livello di manifestazione degli effetti, può essere identificato con il rilascio di sostanze pericolose ma questa schematizzazione non deve distogliere l'attenzione sugli eventi iniziatori. È possibile individuare diversi criteri in base ai quali è possibile classificare eventi calamitosi come gli incidenti industriali:

1. Grado di previsione;
2. Grado di evitabilità;
3. Grado di allarme;
4. Durata del fenomeno;
5. Grado di volontarietà con cui l'incidente o più in generale il rischio è subito.

Il secondo e il quinto criterio sono stati scarsamente indagati nelle analisi di rischio tradizionali. Solo negli studi comparati di percezione del rischio si è cercato di analizzare complessi parametri come il grado di

evitabilità e quanto la popolazione sia disposta a convivere con un determinato rischio secondo un rapporto costi-benefici.
La direttiva Seveso II nel suo recepimento italiano attraverso il D.Lgs. 334/99 sembra aver voluto cogliere un po' tutti questi aspetti, infatti la definizione di incidente rilevante recita: "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 di cui all'articolo 2, comma 1, e che dia luogo a 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".
Nell'allegato VI del suddetto decreto legislativo si precisa ancora i criteri per riconoscere un incidente rilevante:

- Conseguenze per persone o beni:
  - Un morto;
  - Sei persone ferite all'interno dello stabilimento e ricoverate in ospedale per almeno 24 ore;
  - Una persona situata all'esterno dello stabilimento ricoverata in ospedale per almeno 24 ore;
  - Abitazione/i all'esterno dello stabilimento danneggiata o resa inagibile;
  - Evacuazione o sconfinamento di persone per oltre 500 ore-uomo;
  - Interruzione dei servizi di acqua potabile, elettricità, gas, telefono per oltre 1000 ore-uomo.
- Conseguenze immediate per l'ambiente:
  - Danni a 0.5 ha o più di un habitat importante dal punto di vista dell'ambiente o della conservazione e protetto dalla legislazione;
  - Danni a 0 ha o più di un habitat più esteso, compresi terreni agricoli;
  - Danni rilevanti causati a 10 km o più di un fiume o di un canale;
  - Danni rilevanti causati a 1 ha o più di un lago o stagno;
  - Danni rilevanti causati a 2 ha o più di un delta;
  - Danni rilevanti causati a 2 ha o più di una costiera o di mare;
  - Danni causati a una falda o acque sotterranee per 1 ha o più;
  - Danni materiali;
  - Danni materiali nello stabilimento per più di 2 milioni di €;
  - Danni materiali all'esterno dello stabilimento a partire da 0.5 milioni di €.

Per quanto riguarda i fattori che determinano la scala del pericolo vanno menzionati:

- La sostanza coinvolta, modalità di confinamento, grado di dispersione, eccetera;
- Fattore energetico: quantità di energia sprigionata nell'unità di tempo;
- Fattore tempo: durata del fenomeno;
- Relazione *intensità-distanza*;
- Fattore di esposizione (dose);
- Relazioni tra *intensità-danno* ad ambiente, uomo e strutture antropiche.

3.0 LA NECESSITÀ DI SECURITY INDUSTRIALE

Gli attacchi terroristici dell'11 settembre 2001, pur non essendo stati direttamente concentrati contro l'industria di processo, hanno indubbiamente cambiato il modo di concepire la sicurezza in tutte quelle situazioni dove di per sé è presente un potenziale di generare un danno che possa avere un grosso impatto verso l'esterno in termini di perdita di vite umane, di danno economico, ambientale e di sconvolgimento delle coscienze collettive. L'industria si deve ora e sempre di più confrontare con la necessità di valutare se le attuali misure di sicurezza sono sufficienti a scongiurare e a prevenire possibili attentati ed eventualmente prendere tutte le misure correttive per incrementare al massimo il livello di sicurezza per i lavoratori all'interno dell'impianto, per la popolazione, per l'ambiente e le infrastrutture. Queste misure di sicurezza sono necessarie in special modo per tutti quegli impianti che, per importanza strategica, economica, visibilità, per il grado di conseguenze che un attacco può generare risultano essere più appetibili nei confronti di eventuali azioni terroristiche. Lo stesso recente incidente accaduto all'impianto di Tolosa nel 2002, le cui cause non sono ancora chiare e soprattutto tali da non poter escludere la matrice volontaria, ha aumentato il grado di attenzione e di consapevolezza che porta necessariamente a ripensare l'impostazione stessa dell'analisi del rischio. È necessario, d'ora in poi, identificare ogni indicazione, circostanza, evento che ha la potenzialità di determinare una perdita di contenimento o una minaccia per i beni (tecnologici, ambientali, …). In questo lavoro si vuole sostenere che la valutazione della vulnerabilità della sicurezza, nel senso di Security, di un bene diventa un aspetto critico del processo di analisi del rischio. È necessario pertanto nel processo di estensione del rapporto di sicurezza per i nuovi impianti o di revisione per quelli esistenti

introdurre una valutazione dei rischi di Security per l'impianto e delle contromisure adottate o adottabili per ridurre il rischio di un rilascio intenzionale a un livello accettabile con investimenti anch'essi accettabili.

3.1 Analisi della vulnerabilità in termini di Security, differenze e complementarietà tra Safety and Security

L'analisi della vulnerabilità in termini di Security è un processo per determinare la probabilità in termini di possibilità di un avversario di causare una situazione di potenziale danneggiamento per determinati target. Questo tipo di analisi non produce risultati quantitativi nello stesso senso dell'analisi di rischio tradizionale, piuttosto si integra nell'intero processo di valutazione della vulnerabilità dando luogo a risultati qualitativi che costituiscono la base per stabilire delle priorità nell'applicazione di contromisure.
Il rischio nella classica prospettiva della sicurezza industriale viene definito come la potenzialità di un evento che coinvolge sostanze pericolose di generare delle conseguenze indesiderate per l'uomo, per l'ambiente, per le infrastrutture e per le proprietà. Dal punto di vista dell'analisi della vulnerabilità in termini di Security il rischio può essere definito come la probabilità che un'azione intenzionale violi la vulnerabilità generando un rilascio non desiderato. La Safety si concentra sulle cause accidentali, sul complesso processo di concatenazione di eventi che porta al rilascio di sostanze pericolose e alle successive conseguenze agendo attraverso la definizione e l'attuazione di misure preventive e protettive (tabella 1). La Security si concentra sulla causa che genera il rilascio, sull'intenzionalità di un'azione (tabella 2), sabotaggio o attentato, che porta alla perdita di contenimento delegando sempre alla Safety il compito di analizzare le conseguenze (tabella 1). Bisogna, però, precisare che le conseguenze a seguito di un rilascio intenzionale sono in generale diverse di quelle studiate nella normale analisi di rischio. L'intenzione di chi compie un attentato è generalmente quella di causare il più grande danno possibile e non solo in termini di perdita di vite umane, quindi ci avviciniamo a una logica worst-case scenario talvolta perpetrata nelle analisi di rischio di tipo speditivi [1].
Esempi di possibili conseguenze a seguito a un'azione terroristica possono essere:

- Morti e feriti nella popolazione;
- Morti e feriti nello staff dell'impianto;
- Distruzione dell'impianto;
- Distruzione di infrastrutture;
- Problemi per l'economia nazionale;
- Inquinamento ambientale su larga scala;
- Perdite finanziarie su larga scala;
- Perdita di reputazione, di competitività e di business;
- Perdita di dati critici.

Da quanto detto risulta evidente che i due approcci sono perfettamente e doverosamente integrabili.

3.2 Similitudini e differenze tra Safety e Security

Il rischio in termini di Security può essere definito come la probabilità che una definita minaccia sia in grado di sfruttare una determinata vulnerabilità di un target particolarmente appetibile e di dare delle conseguenze fissate.

Tabella 1. Requisiti di Safety e Security

Security	Safety
Valutazione della vulnerabilità e delle minacce	Valutazione della Safety operativa
Valutazione del rischio	Valutazione del rischio
Requisiti in termini di Security	Requisiti in termini di Safety
Test di penetrabilità delle barriere di Security	Test basato sui requisiti normativi

La tabella 2 invece mostra le principali differenze e campi di applicazione di Safety e Security. È importante evidenziare i diversi presupposti di partenza degli studi, cioè la probabilità di successo di un attacco intenzionale da una parte e la probabilità di accadimento di un evento accidentale dall'altra e poi la differenza tra gli scenari di riferimento: nel primo caso si devono ipotizzare scenari di tipo catastrofico mentre nel caso dell'analisi di rischio tradizionale allo scenario catastrofico competono bassissime probabilità di accadimento.

Tabella 2. Accidentale vs intenzionale

Il rischio di rilascio dovuto ad azioni intenzionali: Probabilità di successo dell'attacco; Severità delle conseguenze	**Il rischio di rilascio accidentale è funzione di:** Probabilità del verificarsi dell'evento accidentale Severità delle conseguenze
La probabilità dipende da: Attrattività dei beni; Grado di minaccia; Grado di vulnerabilità	La probabilità dipende da: Dalla possibilità che un evento possa innescare una catena incidentale

3.3 Valutazione della Security

La valutazione della vulnerabilità della Security è un processo composto da cinque stadi distinti:

1. Pianificazione del progetto di valutazione: identificazione dei criteri e delle modalità da utilizzare nell'analisi dei pericoli per la Security, le minacce, le vulnerabilità di un'azienda che in cui sono stoccate e processate sostanze pericolose. Bisogna anche evidenziare le contromisure per la protezione del personale dell'impianto, la popolazione, l'ambiente, le infrastrutture. Per ottenere questo scopo è necessario creare un team o integrare le competenze nel gruppo che si occupa della Safety esistente, così:
    a. Formazione del team;
    b. Definizione dello scopo;
    c. Definizione degli obiettivi.
2. Analisi delle caratteristiche del sito: identificazione delle criticità del sito cioè dei target appetibili;
    a. Valutazione dei beni e dei target critici;
    b. Identificazione dei pericoli;
    c. Analisi delle conseguenze;
    d. Valutazione della appetibilità dei target;
    e. Revisione dei livelli di protezione;
    f. Lista dei target critici che necessitano un ulteriore approfondimento.
3. Identificazione delle minacce;
    a. Identificazione degli avversari;
    b. Caratterizzazione degli avversari.
4. Analisi delle vulnerabilità: il team deve elaborare una serie di scenari di attacco da parte degli avversari e valutare le possibili conseguenze;
    a. Sviluppo di una matrice degli accoppiamenti minacce e dei target;
    b. Analisi delle vulnerabilità della Security;
        i. Approccio basato sulla classificazione dei target;
        ii. Approccio basato sugli scenari.
    c. Analisi dei rischi per la sicurezza e ranking degli stessi.
5. Valutazione e predisposizione delle contromisure.
    a. Analisi delle contromisure in un'analisi basata sulla classificazione dei target;
        i. Assegnazione di standard di performance;
        ii. Identificazione delle raccomandazioni;
        iii. Revisione.
    b. Analisi delle contromisure in un'analisi basata sugli scenari;
        i. Identificazione dei punti di debolezza;
        ii. Identificazione delle raccomandazioni;
        iii. Rivalutazione del rischio.
    c. Prioritizzazione delle contromisure, definizione degli obiettivi e del programma di implementazione.

La valutazione della vulnerabilità della Security può essere fatta secondo due livelli distinti:

· Attraverso il percorso suggerito da una linea guida e da alcune check list di riferimento. Questo primo livello è da consigliarsi ai management degli impianti che intendono estendere le funzioni del proprio sistema di gestione della sicurezza introducendo anche la Security. In questo caso si viene a costituire un SGSS, sistema di gestione della sicurezza e della Security. Le procedure ai sensi del DM 9.8.2000 e delle

UNI EN ISO 16016, 16017 e 16072 possono essere integrate con adempimenti e altre procedure derivate dai princìpi finora descritti. La revisione del sistema andrebbe condotta con frequenza annuale;

· Valutazione speditiva attraverso delle tabelle di riferimento. Questa metodologia permette di ottenere in pochi semplici passaggi, a patto di conoscere i risultati dell'analisi del rischio, che deve essere stata condotta secondo criteri avanzati, e una conoscenza del layout dell'impianto, un risultato numerico che esprime proprio la vulnerabilità dell'impianto o parti di esso a eventuali minacce e attacchi di avversari. La valutazione speditiva può essere utilizzata nell'ambito dell'SGSS come calcolo preliminare.

3.4 Calcolo speditivo della vulnerabilità della Security

Per il calcolo speditivo della vulnerabilità della Security si procede come segue: per ogni apparecchiatura o stoccaggio in cui sono detenute sostanze pericolose in grado di recare offesa all'uomo, all'ambiente o alla proprietà va fatta una valutazione del fattore di severità dell'attacco e poi in cascata altri due indici per mezzo di tabelle. I valori ottenuti saranno combinati con la relazione (1). Per la selezione delle installazioni da analizzare ci si può riferire all'applicazione del metodo a indici selezionando tutte le unità che hanno ottenuto un indice di rischio generale compensato *G'* (così come definito dal DPCM 31.3.1989 e poi con maggiore specializzazione nel DM 15.05.1996 per il GPL e nel DM 20.10.1998 per i depositi di liquidi facilmente infiammabili e/o tosici) maggiore di 390 o *T'*>11, oppure ci si può servire del giudizio esperto selezionando attraverso un audit in campo e documentale tutte le situazioni impiantistiche da sottoporre all'analisi di Security. Il fattore di severità dell'attacco (*SA*) è desumibile dalla seguente tabella.

Tabella 3. Fattore severità dell'attacco

Fattore	**Scenario rilascio tossico (numero di persone coinvolte)**	**Scenario irraggiamento o onda d'urto (numero di persone coinvolte)**
1	0-10	0-10
2	10-50	10-20
3	50-100	20-50
4	100-1000	50-100
5	1000-10000	100-1000
6	10000-100000	1000-10000
7	>100000	>10000

Il fattore di intensificazione della severità dell'attacco (*FIA*) è desumibile dalla seguente tabella. I valori di soglia utilizzati sono quelli del DM 9.5.2001 con questa precisazione: si attribuisce il valore del fattore di intensificazione considerato in corrispondenza del valore di soglia con cui il fenomeno pericoloso raggiunge una distanza fissata che dipende dal tipo di fenomeno e dalle condizioni con cui si estrinseca. Per il rilascio tossico questo valore è pari a 500 m. Per rilascio di energia termica e onda d'urto è pari a 200 m.

Tabella 4. Fattore di intensificazione della severità dell'attacco

fattore di intensificazione della severità dell'attacco	**Rilascio tossico a 500 m (ppm)**	**Rilascio energia radiante a 200 m (kW/m^2)**	**Rilascio onda d'urto a 200 m (bar)**
0.5	TWA	3	0.01
0.75	ERPG-2	5	0.03
1.0	IDLH	7	0.1
1.25	LC_{50}	12.5	0.3

La seguente tabella permette il calcolo del fattore difficoltà dell'attacco (*DA*):

Tabella 5. Fattore difficoltà dell'attacco

Fattore *DA*	**Descrizione e fattori che influenzano la probabilità di successo dell'attacco**	**Esempi**
1	Lo scenario in esame può originarsi da un attacco che richiede una ben coordinata e pianificata serie di azioni che coinvolge parecchie persone con competenze avanzate e richiede la violazione di vari livelli di sicurezza e il superamento di diverse barriere	Dirottamento di un aereo commerciale, azione paramilitare organizzata contro l'impianto
2	Lo scenario in esame può originarsi da un attacco che impegna un piccolo gruppo di persone anche con competenze avanzate e richiede l'accesso ad aree ristrette dell'impianto	Uso di esplosivi all'interno dell'impianto, uso del sistema di controllo per scavalcare le barriere protettive
3	Lo scenario in esame può originarsi da un attacco che impegna un piccolo gruppo di persone con materiali e mezzi normalmente a disposizione dei gruppi terroristici e non richiede l'accesso ad aree ristrette dell'impianto	Uso di esplosivi dall'esterno dell'impianto (per esempio macchine cariche di tritolo)
4	Lo scenario in esame può originarsi da un attacco portato avanti da un singolo individuo dotato di materiali e mezzi di facile reperibilità	Generazione di reazioni indesiderate con acqua, spari di pistola o fucile contro apparecchiature e stoccaggi

La tabella 6 permette di valutare il fattore di appetibilità del target (*AT*):

Tabella 6. Fattore appetibilità dell'attacco

Fattore *AT*	**Descrizione e fattori che influenzano l'appetibilità del target per un avversario**
1	È improbabile che un attacco che abbia successo causi dei problemi all'economia o alle infrastrutture locali. L'attacco non ha una grande risonanza sui mezzi di comunicazione
2	Un attacco di successo può portare a un'evacuazione di una parte della popolazione, problemi all'economia locale, e danneggiamento delle infrastrutture locali. L'attacco ha una rilevante attenzione sui media locali
3	Un attacco di successo può portare a un impatto significativo sull'economia regionale, sulle infrastrutture, o può causare un consistente danno alla proprietà. L'attacco ha una certa attenzione sui media nazionali
4	L'impianto si trova nelle vicinanze di un altro obiettivo strategico (ministero, ambasciata, monumento, …). Un attacco di successo può essere di impatto negativo sull'economia nazionale, può inficiare la distribuzione di servizi critici come quelli energetici, può distruggere delle infrastrutture di interesse nazionale

3.5 Indice di valutazione della Security

Una volta che sono stati determinati i quattro fattori (severità, intensificazione della severità, difficoltà, appetibilità del target) essi devono essere combinati insieme per ottenere l'indice complessivo di valutazione della Security (OSI, *Overall Security Index*) con la relazione (1). Il valore dell'OSI ottenuto permette di valutare il grado di prioritizzazione dell'intervento e di calcolare il fattore di aggravio dell'indice di rischio globale compensato così come definito dal DPCM 31.3.1989.

$$OSI = SA \cdot FIA + DA + AT \qquad (1)$$

Tabella 7. Determinazione della prioritizzazione dell'intervento

Intervallo	**Livello di prioritizzazione dell'intervento**	**Fattore d'aggravio dell'indice di rischio compensato** ***far***	
		Relativo a *G'*	Relativo a *T'*
<3	Non c'è necessità di intervento	1	1
3<*OSI*<6	Lieve necessità intervento	1.1	1.1
6<*OSI*<9	L'intervento è necessario	1.2	
9<*OSI*<12	L'intervento è necessario e comporta una spesa ingente	1.7	1.25
12<*OSI*<15	Intervento critico, devono essere allocate delle risorse per provvedere nel più breve tempo possibile a innalzare il livello di sicurezza	3.5	
>15	Intervento ultracritico	10.5	1.4

Il nuovo indice di rischio G'^{*} è dato dalla (2) o dalla (3):

$$G'^{*} = G' \cdot far \quad (2)$$

$$T'^{*} = T' \cdot far \quad (3)$$

4.0 ELEMEMENTI DEL SISTEMA DI GESITIONE DELLA SAFETY E DELLA SECURITY

In questo paragrafo verrà mostrato come è possibile integrare i concetti relativi alla Security finora esposti nel SGS organizzato secondo il DM 9.8.2000. Il primo passo da compiere è quello di individuare delle aree comuni. Nella figura 2 è evidenziato come Safety e Security possono essere integrate a partire da una comune politica di sistema e da una comune valutazione del rischio. Il passo successivo è quello più oneroso perché presuppone anche un cambiamento di mentalità: il modo più efficace per compierlo è organizzare le procedure secondo i princìpi della norma UNI 16017 e della OHSAS 18001, il cui indice opportunamente modificato è stato riportato in basso.

1 Requisiti generali
2 Politica per la Safety e la Security
3 Pianificazione
- 3.1 Identificazione dei pericoli, valutazione dei rischi, controllo dei rischi
- 3.2 Prescrizioni legali e altre
- 3.3 Obiettivi di S&S
- 3.4 Programma di gestione S&S

4 Attuazione e funzionamento
- 4.1 Struttura e responsabilità
- 4.2 Formazione, sensibilizzazione, competenze
- 4.3 Consultazione, comunicazione
- 4.4 Documentazione
- 4.5 Controllo della documentazione
- 4.6 Controllo operativo
- 4.7 Preparazione alle emergenze e risposta

5 Controlli e azioni correttive
- 5.1 Sorveglianza e monitoraggio della performance
- 5.2 Incidenti, mancati incidenti, non conformità, azioni correttive e preventive
- 5.3 Registrazioni e gestione delle registrazioni
- 5.4 Audit

6 Riesame della direzione

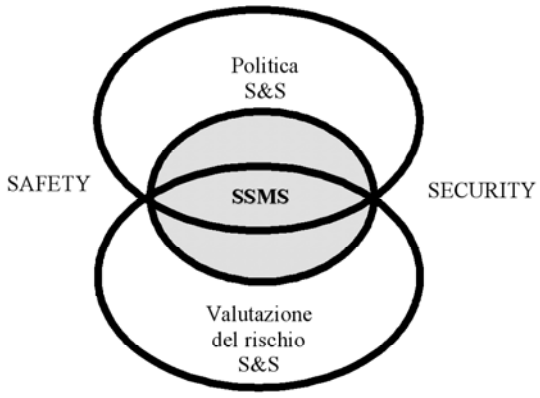

Figura 2. Integrazione tra Safety e Security in un sistema di gestione

Nella figura 3 è stato sviluppato graficamente l'assetto del sistema integrato evidenziando in parallelo tutti gli step da compiere. Si vede che anche nell'analisi dei pericoli molte procedure sono speculari e possono essere condotte in maniera integrata.

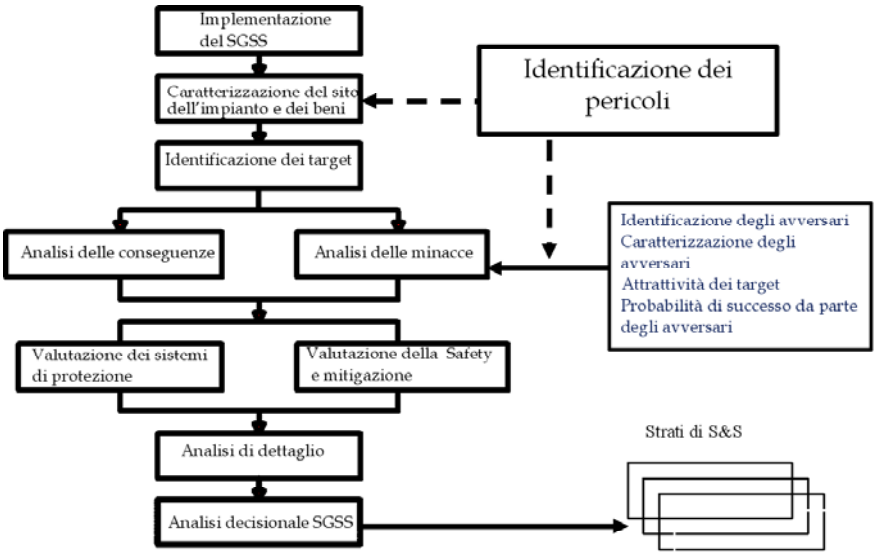

Figura 3. Assetto del SGSS

La completa integrazione secondo la logica PDCA può essere raggiunta con un ulteriore passaggio che evidenzia i vantaggi dell'implementazione del sistema stimolatore della crescita di una cultura SGSS a tutti i livelli aziendali.

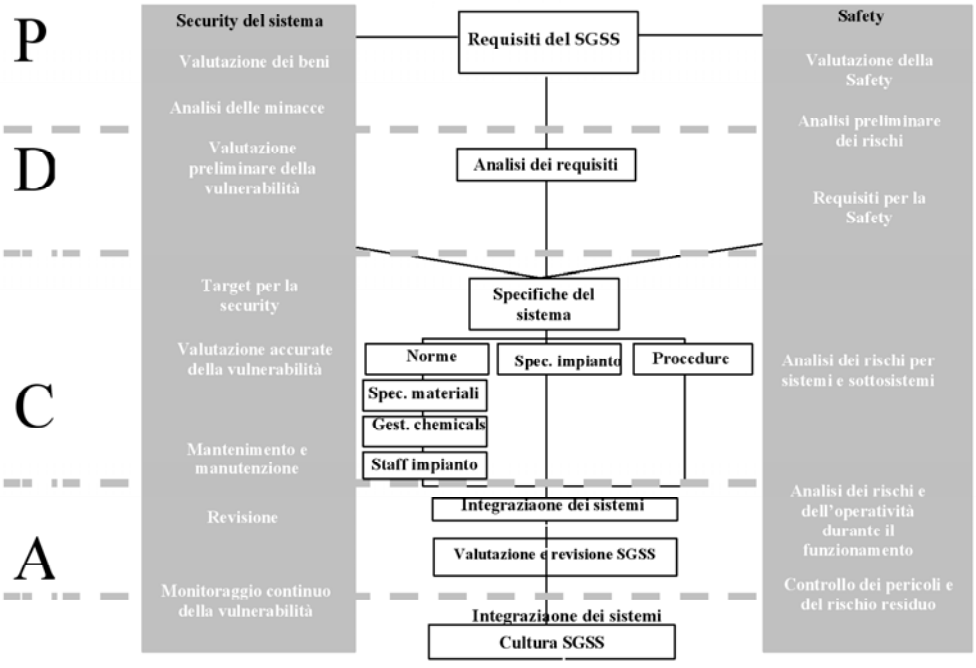

Figura 4. Schema concettuale del sistema SGSS costruito con logica PDCA

4.1 Sistema di gestione della Safety e della Security e organizzazione dei processi

Vengono di seguito analizzati per punti i processi di riferimento che articolano il SGSS in accordo con il ciclo PDCA e tenendo conto della struttura della ISO 16017.

Politica S&S

La politica è un documento strategico che da una visione di insieme su come il gestore dell'impianto intenda assicurare un alto livello di protezione per l'uomo, l'ambiente e le infrastrutture.

Il gestore si impegna ad assicurare un alto livello di Safety e di Security per l'impianto e una adeguata protezione per la popolazione, per lo staff dello stabilimento nel mantenimento della continuità della produzione grazie al sistema di gestione dei rischi in termini di Safety e Security.

Identificazione dei pericoli S&S

- Salute umana e impatti sulla popolazione;
- Identificazione dei pericoli di tipo chimico connessi ai processi, alle operazioni, al personale o ad altri beni;
- Lista dei chemicals presenti nello stabilimento e analisi della pericolosità intrinseca degli stessi. Scenari legati al rilascio.
- Impatti psicologici;
- Impatti strategici e sull'economia (per esempio, in caso di ripristino, rimborso dei costi di impatti ambientali, eccetera)
- Impatti sulla sicurezza nazionale.

Identificazione dei target di Safety e Security

- L'identificazione dei pericoli chimici deve essere effettuata a partire da queste considerazioni**:**
  - Possibilità di effetti oltre il confine di proprietà con scenari worst-case;
  - Analisi dei processi e delle lavorazioni che possono facilmente dare luogo a effetti domino;
  - Possibilità di manomissioni ed effetti di queste;
  - Identificazione degli eventi indesiderati e dei possibili obiettivi degli avversari;
  - Identificazione dei possibili target e la loro posizione;
  - Prioritizzazione della protezione dei target;
  - Livelli di sicurezza esterna: area controllata dal gestore, punti di accesso controllati, area protetta da doppia recinzione, affidabilità del personale, programmi di osservazione del comportamento.
- Definizione dei ruoli e delle responsabilità del personale coinvolto nella gestione SGSS a tutti i livelli dell'organizzazione;
- Identificazione delle necessità in termini di formazione a tutti i livelli dell'organizzazione comprese le ditte esterne;
- La definizione dei ruoli e delle responsabilità deve essere effettiva e formalizzata di un organigramma; Le mansioni critiche devono essere ben descritte e comprese;
- Il sistema di gestione SGSS deve essere implementato in modo che sia possibile a vari livelli di disporre di risorse proporzionate al livello di responsabilità e al grado di attuazione del programma di miglioramento previsto;
- Il gestore deve sviluppare e implementare delle procedure per identificare sistematicamente e valutare i pericoli S&S che possono nascere dalle lavorazioni, dalle sostanze presenti, da errori del personale e da azioni intenzionali di avversari. Le procedure utilizzate per l'identificazione e la valutazione dei pericoli devono essere semplici, sistematiche e riviste con una periodicità fissata. Deve essere, altresì, predisposta una procedura che identifichi le misure per la prevenzione degli incidenti e la mitigazione delle conseguenze. Tale procedura deve includere le azioni intenzionali.

Controllo operativo

Il gestore deve preparare e mantenere aggiornate tutte le informazioni sui pericoli di processo, sui limiti operazionali, sulle lacune di progettazione e sui sistemi di controllo che possono derivare dalla identificazione dei pericoli in termini di Safety e Security. Da queste risultanze devono essere preparate e implementate delle procedure che assicurino una progettazione e una operatività in sicurezza. Particolare attenzione deve essere rivolta agli stoccaggi. Tali procedure devono necessariamente includere:

- Analisi delle barriere, analisi delle minacce, pericoli durante gli start-up, manutenzioni e ispezioni, operazioni periodiche e speciali, sorveglianza in condizioni di fermo impianto o manutenzione, operazioni di emergenza, decommissioning.

Gestione delle modifiche

- Nessuna modifica dovrebbe in qualche modo inficiare la Safety e la Security;

- Il gestore deve adottare e implementare procedure di gestione per la pianificazione e il controllo di tutte le modifiche, specialmente quelle critiche, a livello di organizzazione del personale, processo e variabili di processo, sostanze, apparecchiature, software di gestione, trasporto di merci pericolose, fornitori e tutte quelle circostanze che possono avere effetto sul controllo degli incidenti rilevanti.

Pianificazione delle emergenze

- Il gestore deve sviluppare un adeguato piano di emergenza interno ai sensi della normativa Seveso;
- Il gestore in collaborazione con il prefetto e gli altri enti preposti deve sviluppare un piano di emergenza esterno che deve poi essere adottato, implementato, revisionato e testato mediante esercitazioni. L'operatore deve inoltre provvedere a creare dei team di lavoro che interagiscano direttamente con la squadra di emergenza in modo da diffondere la cultura dell'emergenza a tutto il personale. Deve essere inoltre prevista, e coordinata con le istituzioni, un'adeguata campagna di formazione e informazione della popolazione, che deve essere coinvolta anche nelle esercitazioni;
- Il gestore deve sviluppare e mantenere delle procedure per l'identificazione e l'analisi sistematica delle catene incidentali o dei singoli eventi, compresi quelli intenzionali, che potrebbero portare a situazioni di emergenza. Tale analisi deve essere documentata. La pianificazione dell'emergenza e le esercitazioni e la stessa revisione dei piani dovrebbero essere condotte in base alle risultanze di suddette analisi;
- Il gestore deve sviluppare e mantenere attive delle procedure che garantiscano la comunicazione tra lo staff dell'impianto e con l'esterno in ogni circostanza. Devono essere individuate quelle tecnologie che permettano una comunicazione efficace in caso di emergenza e che rendano più agevole l'intervento.

Monitoraggio delle prestazioni

- Il gestore deve mantenere attive procedure che assicurino un alto grado di performance del sistema di gestione S&S nel rispetto degli obiettivi prefissati e del programma;
- Il gestore deve garantire un monitoraggio attivo che include una sorveglianza dei confini di stabilimento, controlli antiintrusione, ispezioni e ronde agli impianti, alle apparecchiature a alla strumentazione.
- Un sistema di monitoraggio altamente reattivo deve prevedere inoltre un efficace sistema di report degli incidenti e dei quasi incidenti che non identifichi solo le cause immediate ma che cerchi di comprendere quelle nascoste e possibili falle nelle barriere di protezione.

Audit e revisione

- Il gestore deve programmare e condurre audit periodici del SGSS, perché questi sono parte integrante dell'attività stessa. L'audit deve fornire una misura della performance complessiva del SGSS e della sua conformità alla procedure, alle norme cogenti e agli obiettivi. Le risultanze di questi audit devono essere il punto di partenza per la formulazione di nuovi obiettivi e per la revisione di quelli esistenti;
- Il gestore con l'ausilio di gruppi di lavoro allargati deve, a intervalli opportuni, revisionare la politica S&S e le strategie per il controllo degli incidenti rilevanti, tutti gli aspetti del SGSS per assicurare il rispetto degli obiettivi e degli standard preposti. La revisione deve pure costituire il punto di partenza per l'indirizzamento delle risorse per l'implementazione e il miglioramento del SGSS e di quelle risorse tecnologiche per garantire un miglioramento continuo delle prestazioni e del sistema stesso.

5.0 CONCLUSIONI

L'analisi condotta ha mostrato che l'interazione dei concetti e delle necessità industriali in termini di Security sono facilmente integrabili all'interno dei tradizionali sistemi di gestione della sicurezza. È possibile fare analisi del grado di vulnerabilità della Security a più livelli di approfondimento ma già un'analisi speditiva condotta con il metodo proposto permette perlomeno una prioritizzazione degli interventi di protezione. Il passo successivo è quello di individuare le contromisure più efficaci per limitare le conseguenze e per ridurre al massimo la possibilità di successo di azioni terroristiche.

RIFERIMENTI

1. Whiteley, J.R.R. and Mannan M.S., Initial perspectives on process threat management, J.Haz. Mat., vol. 115, 163-167 2004
2. American Petroleum Institute, Security Guidelines for the Petroleum Industry, 2003.