V G R 2002

La prevenzione e la protezione da atti esterni (terrorismo, sabotaggio, dolosità) nelle attività a rischio di incidente rilevante.

C. Aprile – D. Barone – M. Messina

1. Premessa

Recenti atti terroristici ad installazioni civili (New York 12.09.2001) e minacce di sabotaggio ad altre attività industriali e/o commerciali hanno riproposto la tematica della prevenzione e protezione, da atti esterni, degli impianti a rischio di incidente rilevante.

2. Incidenti rilevanti a seguito di sabotaggio

- Deposito costiero SIOT (Trieste – 4.8.1972) Un attentato dinamitardo alle ore 3,15 coinvolge contemporaneamente 3 serbatoi di petrolio grezzo (n° 1 da 50.000 m^3 e n° 2 da 80.000 m^3).Una quarta carica di esplosivo in corrispondenza di un quarto serbatoio da 80.000 m^3 non ha alcun effetto. La tecnica utilizzata dagli attentatori è stata quella di sistemare le cariche esplosive sull'unica tubazione di carico e scarico tra il mantello dei serbatoi e la valvola di intercettazione. Il grezzo fuoriuscito prende immediatamente fuoco e si riversa nei bacini di contenimento. Un quarto serbatoio da 80.000 m^3 limitrofo prende, per effetto domino dovuto all'irraggiamento, anch'esso fuoco.

- Deposito di GPL (Piemonte – anni 80?) Una carica di tritolo posta nella parte inferiore di una sfera di GPL provoca uno squarcio con fuoriuscita ed incendio. Non viene registrata alcuna esplosione del GPL né effetto domino alle sfere limitrofe.

3. Sistemi di sorveglianza (Security)

Statistiche recenti evidenziano un preoccupante aumento del numero di casi di incendio doloso o presunto tale sia in Italia (mediamente il 40%) che negli altri paesi occidentali, con enormi danni che non gravano soltanto sulle attività colpite dal

sinistro ma sull'intera collettività, se si considera il principio di mutualità che sta alla base dell'attività assicurativa. Tutto ciò dovrebbe far riflettere sull'esigenza di elevare il livello di protezione degli insediamenti industriali anche contro le azioni criminose quali appunto gli incendi dolosi e gli attentati con fini distruttivi. Dovrebbe rappresentare, inoltre, un ulteriore elemento di spinta verso lo sviluppo di una cultura nuova della sicurezza, che porti all'applicazione di un approccio metodologico sistematico basato su criteri di valutazione dei rischi più scientifici e moderni. L'adozione di idonee misure antintrusione opportunamente integrate con quelle di prevenzione degli incendi, può consentire di ottenere i risultati sperati.

In tali attività, oltre a prendere in considerazione i rischi intrinseci legati al processo produttivo, che possono essere causa di incidente, occorre valutare anche quelli di origine esogena criminosa quali l'incendio doloso e l'attentato, e che possono causare danni assai più gravi sia in termini di vite umane sia ambientali e patrimoniali.

I vari aspetti della sicurezza dovranno quindi essere analizzati sia separatamente che in relazione reciproca, in modo da adattare le scelte alle esigenze complessive di protezione di quel determinato sito.

Alla base di questa impostazione devono essere poste l'esperienza e le singole professionalità degli specialisti della prevenzione, meglio se operanti in team, che devono intervenire sia a livello ispettivo che progettuale.

Un altro aspetto che meriterebbe di essere preso in attenta considerazione è quello della creazione di specialisti nell'investigazione degli incendi, indispensabili per poterne stabilire, con maggiore esattezza, le cause. A tale scopo, presso il Ministero dell'Interno, è stato creato, in seno al Comitato Centrale Tecnico Scientifico per la prevenzione degli incendi, istituito con il DPR 577 del 1984, un Osservatorio permanente sulla ricerca delle cause d'incendio.

3.1 La sicurezza integrata

Per raggiungere il miglior grado di difesa degli insediamenti industriali, compresi nel campo dei rischi rilevanti, contro ogni possibile tentativo di illecita intrusione avente lo scopo di causare il blocco degli impianti, la distruzione parziale o totale di essi o un disastro ecologico avente finalità terroristiche, è indispensabile adottare idonei sistemi

di sicurezza contro i rischi criminosi, che interagiscano, in modo perfetto, con le misure di prevenzione e protezione contro l'incendio e le esplosioni, tradizionalmente adottati per proteggere questi insediamenti. Tali sistemi sono costituiti, fondamentalmente, da più tipologie di impianti elettronici di prevenzione: i primi hanno la funzione principale di rilevare e segnalare immediatamente qualsiasi tentativo di superamento delle difese passive o meccaniche poste a protezione degli impianti di processo/produzione e delle aree di stoccaggio delle sostanze (ad esempio, recinzioni perimetrali, muri di contenimento, pareti di serbatoi, fabbricati, magazzini ecc.); i secondi che consentono di tenere sotto costante controllo visivo, da postazioni operative di emergenza o da centrali di telesorveglianza, ubicate anche a notevoli distanze, le zone critiche dei suindicati insediamenti industriali.

3.2 Caratteristiche principali degli impianti elettronici di allarme antintrusione

Questi impianti sono costituiti da speciali rivelatori che vengono, di regola, installati direttamente sulle recinzioni fisiche e/o negli spazi aperti circostanti i fabbricati e gli impianti dell'insediamento industriale. Tali rivelatori, grazie al loro principio fisico di funzionamento, rilevano con estrema rapidità ogni tentativo di superamento delle suddette difese.

Tra i più comuni rivelatori utilizzati negli impianti di allarme antintrusione per esterni, vi sono: il cavo microfonico, in grado di rilevare le vibrazioni generate dagli utensili da taglio nelle strutture di metallo di una recinzione; i sensori sismici che captano le frequenze tipiche di attacco prodotte nelle strutture di muratura e di cemento armato dagli utensili meccanici ed elettromeccanici di perforazione, foratura e scasso; i rivelatori che generano fasci di microonde; quelli lineari a raggi infrarossi attivi modulati e infine quelli a cavi interrati, provvisti di trasduttori a pressione, che rilevano l'illecito attraversamento degli spazi aperti circostanti i fabbricati industriali e gli impianti, da parte di persone e automezzi.

Ogni rivelatore dovrà risultare intrinsecamente protetto contro i tentativi di manomissione ed essere provvisto di propria unità di alimentazione elettrica principale (da rete) ed ausiliaria (batteria in tampone).

I cavi di interconnessione dell'impianto, sia di alimentazione sia di trasmissione del segnale, dovranno avere caratteristiche tali da non permettere la propagazione dell'incendio, non subire alcuna interferenza indotta generata dalla presenza di

eventuali campi elettromagnetici esterni, avere adeguata sezione e grado di isolamento elettrico.

Le caratteristiche dei blocchi funzionali della centralina sono indicate di seguito.

- Per i circuiti di ricezione dei segnali provenienti dai rilevatori è richiesto che il trasferimento dei dati da queste all'unità centrale di elaborazione avvenga in forma sicura, cioè adottando una modalità di colloquio dello stesso livello di quello impiegato per il collegamento tra i sensori e la centralina stessa.

- Lo stato di allarme e quello di manomissione proveniente dai rivelatori devono risultare distinti.

- I circuiti di uscita hanno la funzione di pilotare, mediante i segnali di allarme elaborati dalla centralina, i dispositivi di allarme.

  I circuiti di uscita destinati a pilotare gli avvisatori acustici esterni devono prevedere una temporizzazione regolabile da 3 a 10 minuti.

Le segnalazioni di allarme e di manomissione devono essere fornite su circuiti differenziati.

- L'organo di programmazione deve essere costituito almeno da una tastiera alfanumerica completa di display (monitor o display a cristalli liquidi). L'accesso per l'introduzione dei parametri di programmazione deve essere subordinato ad una password di almeno sei caratteri alfanumerici, gestibile direttamente dalla persona autorizzata.

- Le segnalazioni devono essere disponibili soltanto al personale autorizzato, fornite per mezzo di indicatori led ed inoltre essere rese disponibili per la visualizzazione su un pannello sinottico locale ed essere stampate.

  Le segnalazioni provenienti dai rivelatori devono consentire l'identificazione del singolo rivelatore. Le segnalazioni, inoltre devono essere memorizzate fino all'accettazione da parte del personale autorizzato (comando di ripristino).

- Un registratore grafico di eventi deve essere inserito all'interno dell'armadio di centrale, il cui accesso sarà disponibile alle sole persone autorizzate, e dovrà fornire, in forma chiara e codificata, le segnalazioni indicate in precedenza accompagnate dalle corrispondenti indicazioni di anno-mese-giorno-ora-minuto.

Il collegamento con la centralina deve essere a sicurezza positiva al fine di registrare eventuali guasti o interruzioni nel collegamento stesso.

La centrale locale dovrà essere posta in un ambiente, nel quale trovano sede anche i rack dell'impianto di videosorveglianza digitale (TVCC) e della unità di concentrazione dei rivelatori.

3.3 La protezione delle zone critiche interne allo stabilimento

Dovranno essere installati rivelatori di apertura magnetici, almeno a doppio bilanciamento, sui cancelli carrai presenti nella recinzione, sui portoni carrai e sulle porte di ingresso e di uscita di emergenza dei fabbricati, nonché sui lucernarii apribili presenti sulle coperture degli stessi fabbricati.

Allo scopo di rilevare eventuali intrusi negli ambienti a rischio, dovranno essere installati rivelatori volumetrici di movimento (di tipo antiaccecamento) in maniera da integrare la prevista protezione perimetrale dei fabbricati, in particolare in:

- spazi interni ai fabbricati presenti in prossimità dei portoni carrai e delle porte di accesso pedonali dei reparti di produzione e di stoccaggio;
- ambienti provvisti di finestre poste ad altezza d'uomo;
- zone in cui sono presenti impianti tecnologici;
- corridoi interni di collegamento tra i reparti;
- magazzini;
- uffici di direzione e riservati;
- centri elaborazione dati.

3.4 Apparati di segnalazione

Per la segnalazione locale dell'allarme, dovranno essere previsti avvisatori acustici di adeguata potenza autoprotetti ed elettricamente autoalimentati, provvisti di lampeggiante di colore giallo-arancio posti all'esterno dell'edificio, in modo da risultare facilmente udibili e visibili, dalle strade esterne presenti in prossimità dello stabilimento.

All'interno dei locali è opportuno prevedere avvisatori acustici di adeguata intensità sonora (almeno 80 dBA), tale da creare disturbo in chi stia tentando una illecita intrusione.

Devono essere previsti inoltre dispositivi fissi di segnalazione silente di aggressione del tipo a pulsante o a pedale, opportunamente installati nelle zone più esposte a tali rischi. Ad alcuni degli addetti ai reparti, dovrebbero essere forniti pulsanti tascabili di segnalazione di allarme ad onde radioelettriche.

3.5 Gestione allarmi ed eventi

In linea di massima tutti gli allarmi o gli eventi dovranno poter essere gestiti da centrale remota di telesorveglianza.

La presentazione grafica sulla schermo dovrà consentire, in condizioni di presenza di più allarmi contemporanei, di evidenziare la natura, l'entità e l'urgenza degli allarmi in coda, per consentire all'operatore di gestirli secondo la sequenza più appropriata, non necessariamente coincidente con la sequenza temporale di arrivo.

La gestione degli allarmi dovrà essere logicamente concatenata con la gestione dei telecomandi, per consentire una sovrapposizione senza interferenze.

Dovrà esser prevista la gestione dello stato operativo "inserito" della centrale che preveda, nel caso siano esclusi gli apparati di allarme, l'inibizione della manovra di inserimento.

3.6 L'impianto di videosorveglianza digitale

Gli impianti di videosorveglianza, da alcuni anni, sono parte integrante di un buon sistema di sicurezza anticrimine. Hanno la duplice funzione di far giungere, in tempo reale, alle centrali di telesorveglianza, un segnale di allarme intrusione associato alle immagini dell'evento criminoso, riprese dalle telecamere installate nei siti protetti con tali impianti.

La tecnica digitale per la trasmissione dei segnali video ha praticamente soppiantato quella analogica; tra i numerosi vantaggi offerti da questa innovativa tecnologia vi sono:

- l'elevata immunità ai disturbi del mezzo trasmissivo;
- migliori risoluzione e definizione delle immagini;
- la possibilità di trasferire soltanto le variazioni che intervengono nell'immagine base;
- l'interfacciamento, mediante apparecchiature adatte, dei terminali a qualsiasi tipologia
  di rete di comunicazione.

Un altro punto di forza della TVCC digitale è rappresentato dalla facilità di adeguamento di una data realizzazione ad eventuali future modifiche del supporto trasmissivo, volte a migliorarne la velocità e l'efficacia.
La registrazione/archiviazione delle immagini riprese e la loro trasmissione avvengono tramite algoritmi di compressione della quantità dei dati che consentono di ottimizzare l'occupazione del disco magnetico e dei mezzi di comunicazione.
La registrazione delle immagini inviate contemporaneamente da più telecamere (multitasking) avviene in modo sincronizzato. Il reperimento delle immagini è praticamente immediato, eliminando così i tempi di scorrimento del nastro e le ricerche per approssimazione successiva.
E' anche possibile l'asportabilità delle immagini riprese dalle telecamere in formato standard, tramite unità a dischetti. E' infine possibile attuare la criptografia dei dati trasmessi, nonché configurare, in linea, la base dati e la telediagnostica sugli stati di funzionamento delle apparecchiature del sistema.

4. Sistemi di sicurezza (Safety)

I sistemi di sicurezza adottabili/adottati negli impianti a rischio di incidente rilevante possono essere del tipo passivo e/o del tipo attivo come di seguito descritto.

4.1 Sistemi di sicurezza passiva

- Localizzazione decentrata e/o lontana dai perimetri esterni degli stoccaggi di sostanze pericolose. In tal modo si ha una intrinseca difficoltà al raggiungimento degli stoccaggi.

- Doppio contenimento degli stoccaggi di sostanze pericolose quali ad esempio:
  - Bacino di contenimento concentrico in cemento armato (o acciaio) per gli stoccaggi di idrocarburi liquidi a pressione atmosferica
  - Bacino di contenimento concentrico in cemento armato per gli stoccaggi di sostanze pericolose griogeniche (ammoniaca, GPL, ecc.).

  Con il doppio contenimento concentrico avente un'altezza pari a quella del serbatoio principale si ha sia a difficoltà di accesso sia una protezione fisica esterna dello stesso.

- Serbatoi interrati o tumulati

  Con questa soluzione attuata ad esempio per il GPL, oltre la difficoltà di accesso allo stoccaggio, si ha una protezione fisica esterna dello stesso.

- Sale controllo a prova di esplosione esterna.

  Queste sale controllo sono adottate negli impianti petrolchimici e/o di raffineria ove il rischio di esplosione, di nubi di vapori infiammabili non è trascurabile. Tali sale controllo bunkerizzate proteggono gli operatori presenti da eventuali esplosioni esterne dovute a sabotaggio e permettono di mettere in sicurezza gli impianti con le valvole telecomandate di sezionamento.

4.2 Sistemi di sicurezza attiva

Tali sistemi consentono di limitare le conseguenze a seguito di incidenti causati da sabotaggio.

- Valvole telecomandate di sezionamento delle grosse capacità e/o dei serbatoi di stoccaggio di sostanze pericolose. Tali valvole collegate il più vicino possibile alla apparecchiatura o all'interno della stessa consentono di intercettare il prodotto fuoriuscito a seguito della rottura delle tubazioni di collegamento.

- Impianti automatici (o telecomandati) di raffreddamento delle apparecchiature azionati da rilevatori di incendio.

- Impianti automatici (o telecomandati) di versamento della schiuma nei bacini di contenimento o nelle aree di impianto azionati da rilevatori di incendio.

- Impianti automatici per l’aspirazione e l’abbattimento dei gas tossici emessi nel doppio contenimento dell’impianto o dello stoccaggio considerato.

5. Conclusione

I sistemi di sorveglianza impediscono o limitano la possibilità di intrusione di persone non autorizzate negli impianti o stoccaggi a rischio di incidente rilevante.
I sistemi di sicurezza passiva non consentono o limitano la possibilità di sabotaggio delle apparecchiature o stoccaggio di sostanze pericolose.
I sistemi di sicurezza attiva limitano le conseguenze qualora l’attività di sabotaggio o dolosa venga attuata.