SISTEMI DI GESTIONE DELLA SECURITY IN AMBITO PORTUALE

Fabio Garzia
Ingegneria della Sicurezza – Dipartimento ICMMPM
Università degli Studi di Roma "La Sapienza"
Via Eudossiana, 18 - 00184 Roma
Email fabio.garzia@uniroma1.it
Sito web: w3.uniroma1.it/sicurezza

1 INTRODUZIONE

Alla luce dei tragici fatti dell'11 Settembre 2001 tutta la comunità internazionale si è resa conto che la sicurezza di infrastrutture e edifici è indispensabile per garantire un livello di salvaguardia soddisfacente dei beni materiali e, ben più importante, delle vite umane.
Mai come prima d'ora la sicurezza è diventata una necessità; basti ricordare con che drammatica frequenza si sono succeduti i più gravi attacchi terroristici dopo quello alle "due Torri": Istanbul - 15 Novembre 2003; Madrid - 11 Marzo 2004; Londra - 07 Luglio 2005 e 21 luglio 2005.
Stazioni ferroviarie, metropolitane, aeroporti e porti, ovvero luoghi oggetto di passaggio di grandi masse sono diventati oggi più che mai a rischio per eclatanti attentati di matrice terroristica. E' quindi indispensabile, per la salvaguardia della vita umana, dotare questi siti di efficienti sistemi di gestione della sicurezza.
Si è presa coscienza quindi della necessità immediata di costruire o, nella maggioranza dei casi, migliorare e perfezionare i sistemi di sicurezza, laddove la sicurezza viene intesa soprattutto come *security*, ovvero protezione di persone e beni immateriali e materiali, edifici e infrastrutture da attacchi volontari e premeditati.
E' proprio la globalizzazione dei flussi sia commerciali sia turistici oggi esistenti, con spostamento continuo di grandi masse, che comporta l'esigenza di una sicurezza di tipo non invasivo, efficace nei controlli e non limitativa dei movimenti necessari allo sviluppo economico e produttivo della collettività.
Proprio per tali ragioni la sicurezza viene considerata attualmente come un valore aggiunto all'interno dei servizi che deve fornire una grande infrastruttura sia pubblica che privata, per valorizzare l'affidabilità dell'uso della stessa da parte dei traffici sia commerciali che turistici. La qualità del livello di security messo a disposizione permette di elevare in modo significativo il valore economico sul mercato dell'infrastruttura offerta.
Scopo del presente lavoro è quello di illustrare un sistema di gestione della security in ambito portuale, partendo dalle disposizioni normative vigenti che stabiliscono i compiti di una Autorità Portuale (legge n° 84 del 28 Gennaio 1994) e istruiscono sulle disposizioni da attuare e sulle procedure d'emergenza (SOLAS, ISPS code).
Si partirà da una metodologia di analisi delle vulnerabilità e del calcolo del danno provocato nel caso di vari scenari minacciosi ipotizzati. Successivamente, si analizzeranno gli scenari di pericolo creando procedure organiche da eseguire sia in condizioni ordinarie di lavoro sia straordinarie in caso d'emergenza.
Di seguito si stabiliranno l'architettura e le peculiarità di un sistema di sicurezza integrato che dovrà essere perfettamente funzionante per costituire uno strumento efficace a disposizione della security. Si terrà conto, inoltre, dell'evoluzione della tecnologia in questo campo e di tutti gli enti che devono essere informati e che, in caso di pericolo, devono intervenire per garantire la migliore gestione dell'emergenza.
Infine, un ruolo rilevante nell'esecuzione delle procedure d'emergenza è rappresentato dalla rete di comunicazione, dalla centrale operativa, dagli addetti alla vigilanza e alla sicurezza, dagli enti e dalle Forze dell'Ordine che devono eventualmente intervenire. Un fattore fondamentale per assicurare la massima efficienza delle comunicazioni è rappresentato dall'utilizzo di una rete di trasmissione dedicata e protetta per evitare interferenze, attacchi e danneggiamenti dall'esterno,

garantendo l'indipendenza da tutte le convenzionali reti di comunicazione impiegate in condizioni normali.

2 RIFERIMENTI NORMATIVI

Nel presente paragrafo si illustreranno i provvedimenti di carattere legislativo che hanno permesso e permettono, con continui aggiornamenti, di migliorare la security in ambito portuale.

2.1 L'Organizzazione Marittima Internazionale – IMO

Sin dai primi decenni del secolo scorso un gran numero di Paesi propose di costituire un'organizzazione permanente che avesse lo scopo di promuovere la sicurezza marittima e della navigazione. Questo proposito tuttavia non si realizzò se non in concomitanza con la costituzione delle Nazioni Unite.
Nel 1948 il Consiglio economico e sociale delle Nazioni Unite promosse la nascita di un'organizzazione permanente per la sicurezza in mare, ma la convenzione che creò l'I.M.C.O. (Organizzazione Consultiva Marittima Intergovernativa) fu ratificata solo dopo dieci anni. L'organizzazione aveva lo scopo di favorire la cooperazione fra governi nel campo delle regolamentazioni governative e delle pratiche relative alle questioni tecniche di tutti i tipi, riguardanti i mercantili impegnati nel commercio internazionale e di incoraggiare l'adozione delle misure più efficaci per assicurare la sicurezza marittima e l'efficienza della navigazione.
L'IMCO nel 1982 cambiò nome in IMO (*International Marittime Organization*), pur rimanendo un organo consultivo. L'IMO è attivo soprattutto nei settori della sicurezza e dell'inquinamento ed è suddiviso in comitati. Questa organizzazione ha però dei limiti nella sua attività in quanto molti paesi in via di sviluppo non dispongono di infrastrutture per applicare o accettare la regolamentazione internazionale. Inoltre, talvolta, alcuni stati favoriscono il fenomeno delle "bandiere di comodo" e si alleano con compagnie di navigazione private, nel tentativo di eludere l'applicazione di normative che potrebbero avere, come effetto indiretto, quello di abbassare il livello del profitto a fronte di un aumento del livello di sicurezza.
Il primo compito della Organizzazione era quello di adottare una nuova versione della Convenzione SOLAS (*International convention on the Safety Of Life At Sea*), il trattato più importante che si occupa di sicurezza marittima.
La nuova versione della SOLAS fu pronta nel 1960 ed in seguito l'Organizzazione volse la sua attenzione a problemi come la *facilitation* dei traffici marittimi internazionali, le linee di carico ed il trasporto di merci pericolose.
Col passare del tempo, tuttavia, sebbene il problema della sicurezza sia rimasto il primo obiettivo della IMO, la sua attenzione ed i suoi interessi si sono ampliati. In particolare negli anni settanta, col crescere dei traffici marittimi di greggio e derivati e delle dimensioni delle navi adibite al trasporto di tali prodotti, l'attenzione si è rivolta anche al problema dell'inquinamento da greggio.
La IMO ha svolto e continua a svolgere il suo lavoro non solo tramite Convenzioni ma anche pubblicando una serie di Risoluzioni, Raccomandazioni e Codici, incluse linee guida.

2.2 Convenzione SOLAS 74

La convenzione SOLAS è la più importante tra tutti gli strumenti concernenti la sicurezza marittima. La prima versione, anche se mai applicata, risale al 1914 e fu diretta conseguenza del disastro del Titanic. Da quella data la Convenzione ha subito varie modifiche e versioni. A partire dal 1914, infatti, si sono avute altre quattro convenzioni SOLAS: la seconda fu adottata nel 1929 e divenne attiva nel 1933; la terza venne adottata nel 1948 ed entrò in forza nel 1952; la quarta infine, fu adottata nel 1960, sotto gli auspici dell'IMO e divenne operativa nel 1965.

In questo momento vige la Convenzione adottata nel 1974 ed entrata in forza nel 1980; per questo l'attuale convenzione è conosciuta come SOLAS 74 "*International convention on the Safety Of Life At Sea*".
Le convenzioni hanno affrontato molti diversi aspetti della sicurezza in mare. La versione del 1914, per esempio, si occupava di sicurezza della navigazione, costruzione apparecchi radiotelegrafici, dispositivi per la sicurezza e la salvaguardia delle persone, misure antincendio. La prima versione si occupava in modo particolare della salvaguardia della vita umana in mare anche se indirizzava la sua attenzione anche alle navi mercantili.
La Convenzione SOLAS 74 venne stipulata a Londra da 71 paesi. La Convenzione del 1974 è quella attualmente in vigore e difficilmente sarà sostituita in quanto in essa è presente la regola del *tacit acceptance* contenuta nell'art. VII. La regola in questione è tale per cui gli eventuali emendamenti alla convenzione entrano in vigore dopo tempi ben precisi a prescindere dal numero di paesi che a quella data li hanno già adottati. Dal momento che la Convenzione è attualmente in vigore si riportano, con maggiore dettaglio, le fasi e la struttura che, per altro, ricalcano in pieno la struttura delle versioni precedenti.
La convenzione consta di otto articoli che fissano le principali regole che rappresentano i principi di base della convenzione e di altrettanti allegati che si individuano come Capitoli. All'interno degli allegati vengono riportate le raccomandazioni, le disposizioni ed i requisiti tecnici che devono essere rispettati in fase di progettazione, equipaggiamento e costruzione di una nave e di comportamento nella navigazione.
Le caratteristiche principali dei diversi capitoli sono:

- Disposizioni generali (Capitolo I)
  Le disposizioni principali riguardano i tipi di ispezioni ed il tipo di documentazioni che una nave deve possedere in modo da dimostrare di rispettare le disposizioni previste dalla Organizzazione.
- Sicurezza antincendio (Capitolo II)
  Il capitolo, a sua volta suddiviso in CAP II-1 e CAP II-2, contiene importanti cambiamenti in materia di sicurezza antincendio rispetto alla convenzione del 1960.
- Costruzione–suddivisione e stabilità, macchine e istallazioni elettriche(Capitolo II-1)
  Le disposizioni sono in particolare rivolte alle navi passeggeri.
- Costruzione – protezione, individuazione e estinzione incendi (Capitolo II-2)
  Lo scopo del capitolo è quello di migliorare l'equipaggiamento di protezione prevenzione ed estinzione incendi. Il capitolo non si occupa soltanto di navi passeggeri ma anche delle navi trasportanti merci pericolose infiammabili in particolare dei tankers, per i quali si prevede un sistema di gas inerte. Altre disposizioni sono di carattere costruttivo, come, per esempio, l'utilizzo di barriere strutturali con caratteristiche antincendio.
- Dispositivi di salvataggio (Capitolo III)
  Il capitolo è suddiviso in tre parti: A, B, C.
  La parte A si occupa dei dispositivi che devono trovarsi su ogni tipo di nave a prescindere dalla tipologia, dal tipo di carico e dalle dimensioni. La parte B, contiene disposizioni che si applicano alle navi passeggeri mentre la Parte C si occupa dei dispositivi di cui deve essere dotata una nave da carico.
- Radiotelegrafia e radiotelefonia (Capitolo IV)
  Il capitolo suddiviso in quattro parti si occupa di apparecchiature radio e di telecomunicazione in genere che devono trovarsi a bordo di una nave. Il capitolo è strettamente correlato con la *Radio Regulations* della *International Telecomunication Union*.
- Sicurezza della navigazione (Capitolo V)
  Le disposizioni che si trovano nel capitolo si applicano alle navi di qualunque stazza, cosa questa non comune al resto della convenzione che in genere si applica a navi oltre una determinata stazza (in genere a navi di 500 GT). Il capitolo tratta tutti i maggiori aspetti della sicurezza della navigazione.
- Trasporto di granaglie (Capitolo VI)
- Trasporto di merci pericolose (Capitolo VIII)

Il capitolo si occupa della classificazione, dell'imballaggio, dell'identificazione e dello stivaggio di merci pericolose trasportate in colli (non si applicano al trasporto di merci pericolose alla rinfusa). Al fine di fornire dettagliate regole al riguardo, l'Organizzazione adottò il codice IMDG che, fin dalla prima edizione, venne costantemente aggiornato.

- o Navi a propulsione nucleare (Capitolo VIII)
  Vennero forniti soltanto requisiti base che erano integrati da varie raccomandazioni contenute in un allegato. Oggi queste raccomandazioni sono state superate dal codice per le navi mercantili a propulsione nucleare e dalle raccomandazioni per le navi a propulsione nucleare che entrano nei porti.

Come noto, la SOLAS prevede la creazione di tre distinti livelli di sicurezza (MARSEC):

MARSEC 1: rappresenta il livello più basso di sicurezza, ovvero il normale livello di minaccia generica contro le infrastrutture del Porto. Gli impianti dovrebbero effettuare le seguenti attività per evitare o tenere sotto controllo incidenti dovuti al trasporto o alla movimentazione di merci o persone:

- o assegnare risorse sufficienti per realizzare le funzioni prescritte di sicurezza;
- o controllare le *restricted areas* per accertarsi che soltanto le persone autorizzate abbiano accesso;
- o controllare l'accesso all'impianto;
- o controllare e vigilare la *port facility* in questione, comprese le aree operative;
- o sorvegliare la sicurezza dei depositi della nave e del carico;
- o accertarsi che le comunicazioni di sicurezza siano prontamente disponibili.

MARSEC 2: oltre alle misure previste dal MARSEC livello 1, vanno adottate ulteriori misure indicate negli allegati A e B dell'ISPS Code, che sono:

- o assegnare personale aggiuntivo alle operazioni di controllo e sorveglianza delle zone perimetrali del Porto;
- o autorizzare preventivamente, verificandone le necessità, l'accesso delle persone all'interno dell'infrastruttura;
- o Incrementare il controllo lungo la banchina, dove è ormeggiata la nave, in accordo con lo *Ship Security Officer*;
- o limitare l'accesso a specifiche aree dell'Autorità Portuale (APO) alle sole persone che hanno una reale e comprovata necessità ad accedervi;
- o incrementare il controllo delle merci caricate a bordo delle navi;
- o aumentare la sorveglianza per individuare eventuali attività che si configurino come sospette;
- o incrementare il numero di containers controllati.

MARSEC 3: rappresenta il massimo livello di sicurezza ed indica che una nave specifica od una infrastruttura del Porto sono state identificate come obiettivi e che la minaccia è altamente probabile od imminente.

A questo livello di sicurezza vanno adottate le seguenti ulteriori misure:

- o massimizzare l'uso dei dispositivi di sorveglianza e sicurezza;
- o proibire l'accesso al Porto;
- o mettere in sicurezza tutti gli accessi del Porto;
- o considerare la possibilità di interrompere le operazioni di carico e scarico delle merci;
- o eseguire tutte le disposizioni dell'Autorità Marittima, delle Forze dell'Ordine e della Direzione per quanto riguarda specifiche attività;
- o sospendere gli arrivi delle navi fino a quando il livello di sicurezza sarà riportato a MARSEC 2;
- o assicurarsi che tutte le navi ormeggiate siano informate del livello di MARSEC in atto;
- o attivare la sorveglianza lato mare;
- o prepararsi ad evacuare totalmente o parzialmente il Porto.

2.3 La convenzione di Roma 10 Marzo 1988

Tra i problemi inerenti la sicurezza marittima, un'importanza fondamentale è stata assunta dal tema della "security" così come elaborato in relazione al dilagare del fenomeno terroristico.
La convenzione di Roma del 10 marzo 1988 per la repressione dei reati contro la sicurezza della navigazione marittima considera inoltre come azione di terrorismo marittimo atti di violenza o di depredazione compiuti ai danni di una nave o del suo carico o dei suoi passeggeri per finalità politiche e/o terroristiche.
La Convenzione in esame mira a completare le lacune della normativa internazionale in materia di pirateria che erano state messe in evidenza dal caso della nave da crociera italiana Achille Lauro, dirottata da un gruppo di guerriglieri del Fronte per la liberazione della Palestina. In pari data è stato concluso un protocollo aggiuntivo sulla repressione degli atti illeciti condotti a danno della sicurezza delle installazioni situate sulla piattaforma continentale. L'art. 10, par. 1 della Convenzione adotta il principio "aut dedere aut punire", in virtù del quale ogni Stato contraente in cui si trovi l'autore dell'atto terroristico ha l'obbligo di punirlo ovvero di estradarlo verso altri Stati.
Inoltre, è sancito l'obbligo di prendere tutte le misure necessarie per impedire la preparazione di attacchi terroristici.
La convenzione del 1988 non dà una definizione di "terrorismo marittimo" ma in sostanza, nell'art. 3, si ritiene che la navigazione possa essere messa in pericolo dal verificarsi delle seguenti ipotesi:

1. commissione di atti di violenza o minaccia allo scopo di impadronirsi di una nave o arrecare danno ad una persona ivi imbarcata in maniera tale da compromettere la sicurezza della navigazione;
2. distruzione di una nave o danneggiamento grave del carico o delle installazioni di bordo o dei servizi relativi alla navigazione marittima;
3. comunicazione dolosa di informazioni marittime false così da mettere in pericolo la sicurezza della navigazione marittima;
4. uccisione o ferimento di una persona in connessione con uno dei fatti criminali di cui sopra.

Pur essendo la Convenzione di Roma uno strumento importante per la sicurezza dei traffici marittimi, essa si limita, per così dire, all'aspetto repressivo dei fatti terroristici, mentre i terribili eventi dell'11 settembre 2001 hanno portato all'introduzione di misure antiterrorismo per i mari che hanno finalità preventive. Non v'è dubbio che tali misure siano applicabili anche ai pirati o alla folle impresa di qualche squilibrato, ma la finalità principale è quella di combattere quella enorme insidia che mina le basi dell'economia e della civile convivenza e che è rappresentata dal terrorismo.
All'indomani degli attentati alle "due torri" si è verificato uno stato di quasi-paralisi dei traffici aerei, ma non v'è dubbio che gli eventi di cui sopra abbiano influenzato negativamente anche le altre forme di trasporto. L'economia ha risentito assai pesantemente dei tragici fatti e specialmente il mondo occidentale ha vissuto l'incubo di una regressione fatta di isolamento e paura. Ci si è resi conto drammaticamente di quanto siano importanti i collegamenti nel mondo odierno e come dilaghi la psicosi dell'isolamento e l'incubo del terrore, anche a causa della enfatizzazione dei mass media. Il problema di prevenire, per quanto possibile, gli attacchi terroristici non poteva non riguardare anche la navigazione marittima, anche perché le navi, per lo più isolate nell'ambiente in cui si muovono, possono costituire un ottimo bersaglio per azioni terroristiche.
Il pensiero corre soprattutto alle navi da crociera, dove centinaia di passeggeri possono divenire ostaggi di terroristi alla ricerca di azioni clamorose e che abbiano un forte impatto sull'opinione pubblica. Anche navi con caratteristiche tecnologiche altamente sofisticate o a propulsione nucleare o, per esempio, terminali galleggianti off-shore per l'estrazione del gas o del petrolio potrebbero costituire un obiettivo appetibile per le varie organizzazioni terroristiche presenti ovunque nel mondo e non legate necessariamente al fondamentalismo islamico.

2.4 ISPS code

Questa situazione ha fatto sì che nel corso della conferenza dell'IMO, tenutasi nel Dicembre 2002 a Londra, siano state adottate una serie di misure, procedure operative e piani per prevenire il terrorismo nei mari. La Conferenza ha adottato una serie di emendamenti alla *Safety Of Life At Sea convention* (SOLAS 74) del 1974, che hanno comportato alcune modifiche:

- la rinumerazione del Cap. XI nei Cap. XI-1;

- le previsioni dell'installazioni a bordo dei sistemi di identificazione automatica (AIS);
- la prescrizione di installare a bordo un registratore sinottico continuo per la registrazione della storia della nave;
- la previsione dell'apposizione del numero di identificazione IMO regola XI-1/3, oltre che all'interno, anche all'esterno della nave, in maniera visibile, sullo scafo o sulla sovrastruttura.

E' stato inoltre aggiunto il Capitolo XI-2 "*Special measures to enhance marittime security*", che rappresenta l'*International Ship and Port facility Security code – ISPS code*.
Le modifiche, compreso il Codice ISPS, si considerano accettate il 1° Gennaio 2004 e sono entrate in vigore il 1°Luglio 2004 .
Il nuovo Capitolo della SOLAS (13 regole) contiene prescrizioni obbligatorie per le navi, per le compagnie, per le aree portuali e per i governi contraenti.
Nella regola 1 sono contenute alcune definizioni fondamentali per la comprensione dell'ISPS code, tra cui ricordiamo:

- *ship/port interface*: che identifica le interazioni che si manifestano quando una nave è direttamente e immediatamente condizionata da azioni che coinvolgono movimento di persone, merci o da forniture di servizi portuali;
- *port facility*: che identifica l'area in cui avvengono per l'appunto *ship/port interface*;
- *ship to ship activity*: che identifica l'operazione di trasbordo o allibo tra due navi che non avviene in una *port facility*;
- *designed Authority*: identifica l'organizzazione o amministrazione, all'interno del governo contraente, responsabile di assicurare l'implementazione delle regole del capitolo riguardanti le port facility e le *ship/port interface*;
- *security incident*: identifica ogni atto o circostanza sospetta che minaccia la sicurezza di una nave, comprese le unità mobile di perforazione e le unità veloce o un'area portuale attrezzata (*port facility*);
- *security level*: identifica il grado di rischio quando viene tentata o quando si verifica un'azione di minaccia alla security;
- *declaration of security*: identifica un accordo raggiunto tra una nave e una *port facility* o un'altra nave con cui si eseguiranno operazioni, specificante le misure di sicurezza che ognuno, metterà in pratica.

Il nuovo Capitolo si applica:

- alle navi passeggeri, comprese le unità veloci da passeggeri impegnate in viaggi internazionali;
- alle navi da carico, comprese quelle veloci uguali o superiori alle 500 TSL, impegnate in viaggi internazionali;
- alle unità mobili di perforazione off-shore, alle aree portuali di servizio e navi che compiono viaggi internazionali (regola 2).

I governi degli Stati contraenti (regola 3) hanno l'obbligo di disciplinare i livelli di sicurezza e fornire le opportune relative informazioni di sicurezza:

- alle navi battenti la loro bandiera;
- alle *port facilities* all'interno del loro territorio;
- alle navi che si trovano nel mare territoriale;
- alle navi che stanno per entrare in un porto del loro territorio;
- alle navi che sono all'interno di un porto nel loro territorio.

Quando si verifica un allarme proveniente da una nave che non batte la propria bandiera, il governo interessato (regola 6), deve informare subito l'amministrazione competente ed eventualmente lo Stato nella cui adiacenza sta navigando la nave.
I governi contraenti devono stabilire un punto di contatto (regola 7) per mezzo del quale le navi possono chiedere consiglio e/o assistenza ed attraverso il quale possono segnalare ogni evento riguardante la sicurezza delle navi o dei traffici. Nel caso di individuazione di un rischio di attacco, il governo interessato avviserà le navi oggetto e le amministrazioni della possibile aggressione. La comunicazione in oggetto riguarderà il livello di sicurezza, le misure di sicurezza che dovranno essere applicate in accordo con le previsioni della parte A dell'ISPS e quelle che lo Stato costiero ha deciso di porre in essere.

Ai governi contraenti spetta infine l'approvazione dei piani di sicurezza delle navi (*ship security plan* - SSP), la valutazione della sicurezza di ogni *port facility* e l'approvazione dei relativi piani di sicurezza (*Port Facility Security Plan*).
Le compagnie di navigazione e le loro navi dovranno avere i requisiti previsti dal capitolo suddetto ed alla parte A dell'ISPS Code, mentre le indicazioni della parte B possono considerarsi facoltative.
Le compagnie devono preoccuparsi del fatto che il comandante abbia disponibili a bordo, in qualsiasi momento, le informazioni attraverso le quali gli ufficiali debitamente autorizzati dal governo interessato (PSCO) possono stabilire (regola 5) chi sia il responsabile della scelta dei membri dell'equipaggio o delle altre persone impiegate a bordo in vari ruoli o servizi di una nave, chi sia il responsabile circa la decisione sull'impiego della nave e chi siano i noleggiatori, nell'ipotesi di stipula di un contratto di noleggio della nave.
Tutte le navi dovranno essere provviste di un sistema di sicurezza d'allarme come segue:

- navi passeggeri, incluse le unità veloci, costruite prima del 1° Luglio 2004, non più tardi della prima visita alle installazioni radio dopo il 1° Luglio 2004;
- petroliere, chimichiere, gasiere, portarinfuse in genere e navi da carico veloci di stazza uguale o superiore alle 500 TSL costruite prima del 1° Luglio 2004, non più tardi della prima visita alle installazioni radio dopo il 1° Luglio 2 004;
- tutte le altre navi da carico uguali o superiori alle 500 TSL e le unità di perforazione mobile costruite prima del 1° Luglio 2004, non più tardi d ella prima visita alle installazioni radio dopo il 1° Luglio 2006.

Il sistema di allarme di sicurezza della nave, una volta attivato, deve iniziare a trasmettere un segnale d'allarme ad un soggetto competente designato dall'amministrazione che può essere anche la Compagnia della nave. Il segnale deve identificare la nave, la relativa posizione ed indicare che la sicurezza della nave è stata minacciata o si è compromessa (regola 6). Il segnale di allarme non deve essere trasmesso ad altre navi, non deve provocare nessun segnale o allerta a bordo e deve continuare ad essere trasmesso fino a quando non viene disattivato o ripristinato il sistema. Il sistema di allarme della nave deve poter essere attivato dal ponte di navigazione ed in almeno un'altra posizione. I punti di attivazione del sistema di allarme di sicurezza della nave saranno progettati in modo da impedire attivazioni casuali.
Ogni nave a cui si applica la parte A dell'ISPS Code dovrà sottostare a:

1. visita iniziale prima che la nave inizi a navigare o anteriormente al rilascio del primo international security certificate. Tale visita riguarda i sistemi e gli equipaggiamenti di sicurezza in virtù delle disposizioni del cap. XI-2, della parte A dell'ISPS Code e dal piano di sicurezza della nave (SSP);
2. visita di rinnovo ad intervalli determinati dall'amministrazione ma non superiori ai 5 anni;
3. visita intermedia da effettuarsi tra la seconda e la terza data di scadenza del certificato;
4. visite addizionali determinate dall'amministrazione.

Dopo la visita viene rilasciato l'*international security certificate* dall'amministrazione o da una organizzazione abilitata per la security (durata massima 5 anni). E' previsto anche, in determinate ipotesi, il rilascio di un certificato di sicurezza ad interim (temporaneo, valido per massimo 6 mesi).
E' da ritenere che il rilascio di detti certificati integri una presunzione "iuris tantum" di conformità ai requisiti di security, la cui valenza probatoria può essere impugnata con qualsivoglia mezzo di prova.
Ai predetti certificati si aggiunge la *declaration of security*, richiesta ai fini della valutazione del rischio che una *port facility* od una *ship to ship activity* persenta per le persone, i beni e l'ambiente.
La dichiarazione è compilata da parte del comandante della nave o dal *ship security officer* (SSO): per le infrastrutture portuali si tratterà del *port security officer* o da altro ente responsabile della sicurezza determinato dall'amministrazione.
Per le aree e le infrastrutture portuali è prevista dalla parte B del Code uno *statement of compliance of a port facility* (dichiarazione di conformità).
Il codice ISPS precede i requisiti di sicurezza per le navi e le infrastrutture portuali. Ogni governo deve procedere ad una verifica sulla sicurezza delle infrastrutture portuali, individuando innanzi tutto le strutture o le aree che, se danneggiate, possono comportare rilevanti perdite di vite umane, di natura economica o ambientale e successivamente i pericoli cui possono andare soggette. Infine, devono essere presi in considerazione i probabili obiettivi di una possibile aggressione, i sistemi di comunicazione, le carenze dei sistemi di sicurezza portuale. Compiute tutte queste

verifiche si valuterà il rischio. Il codice fa riferimento ad una serie di requisiti minimi di sicurezza sia per le navi che per le aree portuali.
Per le navi e le Compagnie di navigazione è prevista l'adozione di un piano di security (SSP), il compimento di valutazione di security (S.S.A.), la designazione di uno o due responsabili a bordo dei sistemi di security (S.S.O., *ship security officer*), la designazione di un ufficiale responsabile per la compagnia dei sistemi di sicurezza (C.S.O. – *company security officer*), l'installazione di un allarme di sicurezza a bordo, lo svolgimento di una attività formazione ed esercitazione riguardo alla security.
In particolare la S.S.O. ha tra i suoi compiti, fra l'altro, quello di compiere regolari ispezioni a bordo al fine di controllare che siano mantenute convenienti misure di sicurezza, controllare che sia applicato ed implementato, ove occorra, il *security plan*, coordinare gli aspetti di sicurezza connessi alla movimentazione del carico, fare rapporto al C.S.O. riguardo a tutte le carenze e non conformità riguardanti la sicurezza, accertate durante le verifiche e le ispezioni, assicurare l'appropriato addestramento del personale, fare rapporto circa gli incidenti accaduti, controllare l'efficienza degli apparati di bordo, coordinarsi con il C.S.O. e gli ufficiali addetti alla sicurezza del porto.
Non vi è dubbio che la figura del S.S.O. sollevi più di un problema, soprattutto riguardo al suo rapporto con il comandante della nave. Ci si è posti soprattutto il problema se una decisione "finale" in tema di security spetti al S.S.O. oppure al *master of the ship*.
Non dimentichiamoci che il comandante della nave è titolare anche di importanti funzioni di polizia (polizia di sicurezza, sanitaria, doganale, etc.) e che egli rimane il primo responsabile a bordo, per cui, pur essendo evidente che ci dovrà essere una continua collaborazione tra i due soggetti, qualora si tratti di prendere una decisione operativa immediata in tema di sicurezza, si ritiene che l'ultima parola spetti al comandante della nave, quale responsabile primo della spedizione. Un altro problema che riguarda l'ufficiale addetto alla sicurezza (anche della compagnia) è la peculiare competenza che tali soggetti dovranno possedere, il che rende sicuramente problematico il loro addestramento ed il loro inserimento nell'organizzazione della nave o dell'impresa armatoriale.
Visto che si tratta di sistemi di allarme, di possibile contatto con materie esplosive e di possibili bersagli di attacchi terroristici, si potrebbe pensare che tali soggetti debbano avere competenze in campo elettrico, elettronico, di armi e munizioni, di congegni esplosivi, il che, ovviamente, non è facile e immediato da ottenere.
Per quanto concerne le infrastrutture portuali, è il *port facility security assessment* che è parte integrante del *port facility security plan*. Tale *assessment* comprende i seguenti elementi:

- identificazione e valutazione delle strutture ed infrastrutture che abbisognano di protezione;
- identificazione delle possibili minacce alle infrastrutture;
- scelta e graduazione delle contromisure;
- identificazione delle carenze sia a livello di infrastrutture che di elemento umano.

Dovrà poi essere redatto un piano di sicurezza per ogni specifica *port facility* e per ognuna delle infrastrutture portuali verrà designato un *port facility security officer* (PFSO).
Sia per le navi che per le infrastrutture portuali sono previsti:

- il monitoraggio ed il controllo degli accessi,
- il monitoraggio ed il controllo delle attività delle persone e della caricazione,
- la disponibilità in tempi brevi di informazioni sulla security.

Il codice regola la sicurezza a tre livelli:

- Livello I: situazione normale di minaccia;
- Livello II: situazione media di minaccia;
- Livello III: situazione elevata di minaccia.

Un accenno deve essere fatto alle prescrizioni inerenti l'entrata delle navi in un porto dello Stato contraente. Prima di tale entrata gli Ufficiali, debitamente autorizzati, possono richiedere informazioni circa:

- il possesso di un certificato internazionale di sicurezza valido;
- il livello di sicurezza della nave;
- il livello di sicurezza a cui la nave ha funzionato nel porto precedente e durante le ultime dieci soste;

- le procedure di sicurezza della nave applicate durante le operazioni di allibo o trasbordo, se avvenute, durante le ultime dieci soste.

Un eventuale rifiuto di notizie potrà condurre al divieto di accesso al porto. Il divieto in questione o l'espulsione dal porto presuppongono che gli ufficiali del porto abbiano fondato motivo di credere che la nave presenti una immediata minaccia per la sicurezza e la protezione delle persone, o delle navi o d'altri beni e non vi siano alternative per rimuovere la minaccia. Ci si dovrà adoperare per evitare di ritardare o detenere la nave oltre quanto strettamente necessario.
L'ISPS Code crea una situazione completamente nuova, imposta, per così dire, dai recenti eventi internazionali e pone esigenze di cui occorrerà tener conto. Il meccanismo messo in moto appare, per certi versi, importante, anche se può sorgere qualche dubbio sulla sua pratica attuazione.
In linea generale, però, il terrorismo è un fenomeno con cui doverci misurare attualmente, anche se ciò comporta ritardi e controlli. I collegamenti nazionali e soprattutto internazionali sono vitali per le nostre economie e specialmente per il mondo occidentale, per cui ben si può comprendere la necessità di adottare misure antiterrorismo, anche se esse comportano una serie non trascurabile di problemi. La security, quindi, è diventata una necessità imposta dal comportamento di persone che hanno per finalità distruzione e morte e mirano sistematicamente a minare le basi dell'economia e la stabilità sociale dei paesi civili.

3. STRUMENTI OPERATIVI PER LA VALUTAZIONE DEL RISCHIO

Per garantire accettabili livelli di sicurezza in infrastrutture così rilevanti come i porti è necessaria un'attenta analisi degli scenari incidentali.
Per quanto riguarda le infrastrutture portuali, sussistono elevati livelli di pericolosità dovuti sia a fattori di rischio specifici dell'ambiente, legati al trasferimento di merci e persone, sia alla reale possibilità di essere uno scenario ideale per attacchi terroristici.
Il raggiungimento di un elevato livello di sicurezza è la conseguenza dell'applicazione di una metodologia sistematica assolutamente necessaria durante la fase preliminare di progettazione. Le linee guida di origine statunitense e anglosassone fissano molti standards e sono prese in considerazione per definire una completa analisi, utilizzando un approccio strutturato che mira a uno "screening iniziale" di localizzazione delle infrastrutture.
Gli standards presi come riferimento sono essenzialmente quelli della *Federal Emergency Management Agency* (FEMA) e del *National Institute of Standards and Technology* (NIST).
Il FEMA recentemente ha prodotto una serie di pubblicazioni dirette a fornire delle linee guida per mitigare il rischio terrorismo. Lo scopo del "*Risk Management Series*" è di ridurre il danno fisico della componente strutturale e non strutturale della costruzione e delle relative infrastrutture, provvedendo, con i mezzi correntemente a disposizione dell'architettura e dell'ingegneria, a ridurre il danno fisico, causato da un attacco terroristico, alle persone e alle relative infrastrutture.
Il NIST suggerisce l'uso di una analisi metodologica proposta dalla FEMA per valutare la vulnerabilità delle strutture e integrarle con metodi e modelli per la seguente analisi costi/benefici eseguita per scegliere le tecniche e/o le contromisure procedurali per stilare un ordine per ridurre il rischio residuo ad un livello ritenuto accettabile.
In accordo con la divisione comunemente accettata, il processo di analisi del rischio terrorismo si sviluppa in 3 fasi distinte:

1. *Treath Assessment* (TA), valutazione della minaccia;
2. *Vulnerability Assessment* (VA), valutazione della vulnerabilità;
3. *Risk Assessment* (RA), valutazione del rischio.

Lo scopo del *Treath Assessment* è identificare e studiare le possibili condizioni di pericolo in termini di potenziale aggressione (Threat: minaccia) e modalità d'attacco (Hazard: rischio). Nel processo di analisi proposto, il TA è diviso in due distinte fasi: una fase di identificazione del rischio, che precede la fase di valutazione della vulnerabilità di una struttura e definisce le modalità d'attacco da analizzare, e una seguente fase di analisi del rischio nella quale sono valutate le potenziali conseguenze sulla base dei risultati ottenuti. La lista delle modalità d'attacco presa come un riferimento è definita dalla FEMA.

Le conseguenze collegate ad un attacco terroristico sono valutate con riferimento ai seguenti elementi considerati significativi:

- perdita di vite umane;
- danno materiale;
- interruzione degli affari e conseguenze astratte (in termini di “immagine” e impatto sull’opinione pubblica).

Il proposito della fase di *Vulnerability Assessmen*t è valutare la debolezza della struttura, così come le caratteristiche specifiche o le carenze di un sistema di sicurezza esistente. L’analisi è formata dall’applicazione della check list definita nella FEMA riguardante gli aspetti di potenziale vulnerabilità di una costruzione.

Possiamo definire quattro categorie per classificare la vulnerabilità di una struttura:

1. la disponibilità: ovvero l’evidenza che ha la struttura e la propria attitudine ad essere oggetto di un piano d’attacco;
2. l’accessibilità: ovvero la facoltà d’accesso alla struttura nello scenario di attacco. Si riferisce a barriere fisiche e geografiche che scoraggiano la minaccia senza prendere in considerazione la sicurezza organica;
3. la sicurezza organica: ovvero la capacità del personale addetto alla sicurezza di scoraggiare l’attacco. Include i piani di sicurezza, la capacità di comunicazione, il personale di sorveglianza, i sistemi di rilevamento delle intrusioni e la tempestività delle forze di polizia nel prevenire l’attacco;
4. resistenza della struttura: ovvero la capacità della struttura di resistere ad uno specifico attacco basata sulla complessità del progetto del porto e delle relative caratteristiche dei materiali di costruzione utilizzati.

Lo scopo della fase di RA è riassumere, sia analiticamente che numericamente, i risultati ottenuti dall’analisi di ogni modalità d’attacco in termini di vulnerabilità delle strutture e possibili conseguenze.

La fase della valutazione della vulnerabilità ha lo scopo di identificare le “vulnerabilità”, cioè che gli aspetti specifici o la parte fisica della struttura che in presenza di uno o più attacchi può comportare scenari di danno considerevole.

Una fase preliminare di familiarizzazione con le strutture da analizzare ha lo scopo di raccogliere le informazioni tecniche e di gestione che possono essere importanti nella seguente valutazione. Il primo passo è quindi identificare le attività e le operazioni critiche per una struttura portuale. Le varie missioni che possono essere riferite a ogni struttura sono così elencate:

- Salute pubblica;
- Commercio;
- Sicurezza / difesa;
- Trasporti;
- Comunicazioni.

L’analisi del rischio ha lo scopo di valutare le potenziali conseguenze ad ogni modalità d’attacco. In una fase di analisi preliminare si collega la totalità dell’indice dei danni a ogni modalità d’attacco, con riferimento al più grave scenario di danno tra quelli ipotizzabili.

La totalità dell’indice di danno include differenti aspetti (*damage feature*) considerati importanti per la totale valutazione delle conseguenze d’attacco: perdita di vite umane, danni materiali, non disponibilità/interruzione degli affari e conseguenze astratte (in termini di “immagine” e impatto sull’opinione pubblica).

L’indice del danno è definito in accordo al sistema contenuto nella tabella 1.

	INDICE DEL DANNO (DI)
0	Nessun danno
1	Danno minore
2	Danno significativo
3	Danno maggiore

Tabella 1: Damage Index (DI)

Come caratteristica della infrastruttura considerata, è definito un peso per ognuno degli aspetti sopra menzionati e la loro relativa importanza nella totalità della valutazione delle conseguenze di ogni metodo d'attacco. Un esempio di pesi caratterizzanti la struttura di analisi è illustrato nella tabella 2.
Per ogni modalità d'attacco, la totalità dell'indice di danno è calcolato come la media di indici di danno assegnati ad ogni aspetto dannoso, basato su coefficienti (normalizzati) caratterizzanti la struttura.

Damage feature	**Human Life**	**Material Damage**	**Mission unavailability/ Business interruption**	**Untouchable Consequence: Image**	**Untouchable Consequence: Public opinion**
Damage weight	0,4	0,1	0,2	0,1	0,2

Tabella 2: Esempio di Damage Weight

Le misure sopra menzionate sono assegnate sulla base delle seguenti considerazioni qualitative:

- la perdita di vite umane indubbiamente rappresenta l'aspetto più critico da considerare quando si valuta il danno prodotto da un evento terroristico;
- in caso di non disponibilità della struttura, l'interruzione del servizio causa al soggetto (pubblico) che utilizza la struttura un danno più grande del danno materiale considerato (quindi economico).
- come loro intangibili conseguenze, l'impatto degli eventi sull'opinione pubblica è considerato molto più critico rispetto ad un danno d'immagine subito da un soggetto (pubblico) che utilizza la struttura in oggetto.

Quando si crea un'analisi dettagliata, che in generale fa riferimento a un limitato numero di modalità degli attacchi, l'analisi del rischio (HA) può:

- identificare e formalizzare il possibile scenario di danno collegato a ogni modalità d'attacco e analizza la possibile evoluzione;
- prendeRE in considerazione gli attacchi diversi (contro differenti strutture) e situazioni d'emergenza causate da eventi esterni, sempre se non internazionali;
- identificaRE sistematicamente gli scenari conseguenti al fallimento di ogni misura tecnica predisposta;
- analizzaRE le misure stabilite dalla gestione dell'emergenza con l'integrazione di indici definiti in base all'effettività e tempestività. Per questo scopo è raccomandato il modello definito dalla FERC (*Federal Energy Regulatory Commission*).
- assegnaRE un indice di danno a ogni scenario di danno analizzato.

Continuando l'applicazione della metodologia dell'analisi del rischio, possiamo classificare la capacità delle strutture inizialmente perse in base alla loro capacità di recuperare l'efficienza dopo un evento dannoso:

- Eccellente;
- Buona;
- Discreta;
- Povera;
- Nulla.

Il livello di rischio viene stimato secondo la scala di seguito illustrata:

- Critico: gli elementi critici supportano molteplici aree di missione, hanno diversi effetti di conseguenze e sono difficili o impossibili da ricostruire in tempi brevi;
- Moderato: gli elementi moderati possono supportare una/due aree di missione, incidono su una/due livelli di conseguenze e possono essere ricostituiti in tempi ragionevoli;

- Marginale: targets che possono anche non supportare nessuna area di missione, possono avere effetti minimi di distruzione e possono avere sistemi di back-up che minimizzano i tempi di recupero.

4 OBIETTIVI E PECULIARITA' DI UN SISTEMA INTEGRATO DI SICUREZZA

Nel presente paragrafo si illustreranno, sinteticamente, le funzionalità di un sistema integrato di sicurezza e le tecnologie da utilizzare per realizzarlo.
Tale sistema integrato rappresenta la sicurezza tecnologica, che è uno dei 3 elementi fondamentali per la realizzazione di un efficiente sistema di gestione della sicurezza. Gli altri 2 elementi sono rappresentati dalla sicurezza fisica (barriere, recinzioni, ecc.) e dalla sicurezza procedurale (risorse umane, procedure, ecc.).
La progettazione e la realizzazione di un sistema integrato di sicurezza deve garantire un soddisfacente livello di sicurezza e di gestione delle emergenze, evitando di cadere nell'errore di dividere l'impianto in settori non integrabili e interagenti reciprocamente.
Un altro importante aspetto che un sistema security deve soddisfare è rappresentato dalla semplicità gestionale. Infatti l'operatore della sicurezza deve riuscire a gestire il sistema in maniera efficiente ed efficace, specialmente in condizione d'emergenza, senza inutili difficoltà che possano creare uno stress infruttuoso ed inutile.
Un ruolo rilevante è rappresentato dalla gestione dell'informazione all'interno del sistema integrato di sicurezza. Il flusso informativo, talora particolarmente elevato, deve essere incanalato ed eventualmente memorizzato per evitare sovraccarichi sui canali di trasmissione.
Il flusso informativo nei confronti degli operatori deve essere il minimo indispensabile, destinato ovviamente ad aumentare in condizioni d'emergenza. Questo per porre l'operatore nelle migliori condizioni di lavoro e garantire la possibilità di mantenere elevato il livello d'attenzione.
Una peculiarità del sistema, che gli permettere di rispondere in modo efficiente alla protezione del territorio, è rappresentata dall'utilizzo e dallo sviluppo di tecnologie capaci di automatizzare il flusso delle informazioni in base al verificarsi degli eventi o all'analisi dei dati acquisiti, consentendo all'operatore di gestire in maniera dedicata solo le situazioni che richiedono una sua reale attenzione. Rimane comunque un elemento fondamentale il poter disporre di figure professionali qualificate, capaci di analizzare e studiare in maniera efficace il problema della sicurezza e progettare una risposta estremamente funzionale attraverso la perfetta integrazione dei sistemi.
Le tecnologie impiegate devono rispondere ad elevati standard di efficienza, di affidabilità nel tempo e di capacità di integrazione reciproca durante le procedure di gestione in situazioni convenzionali e in special modo in scenari emergenziali.
Un'attenzione particolare deve essere rivolta alla manutenzione dell'impianto di sicurezza soprattutto dove sono impiegate tecnologie integrate poiché si deve far fronte ad un degrado nel tempo sia per quanto riguarda l'impiantistica che l'efficienza strutturale.
E' quindi necessario impiegare tecnologie affidabili ma con costi di manutenzione contenuti e formare al meglio personale capace di valutare l'efficienza del sistema nel tempo e in grado di fronteggiare eventuali guasti, per avere in ogni momento un impianto caratterizzato da uno standard elevato, sia sul piano tecnico che operativo.

5 ARCHITETTURA GENERALE DEL SISTEMA INTEGRATO DI SICUREZZA

Un sistema integrato di sicurezza è composto da una serie di elementi che vengono illustrati nel seguito.

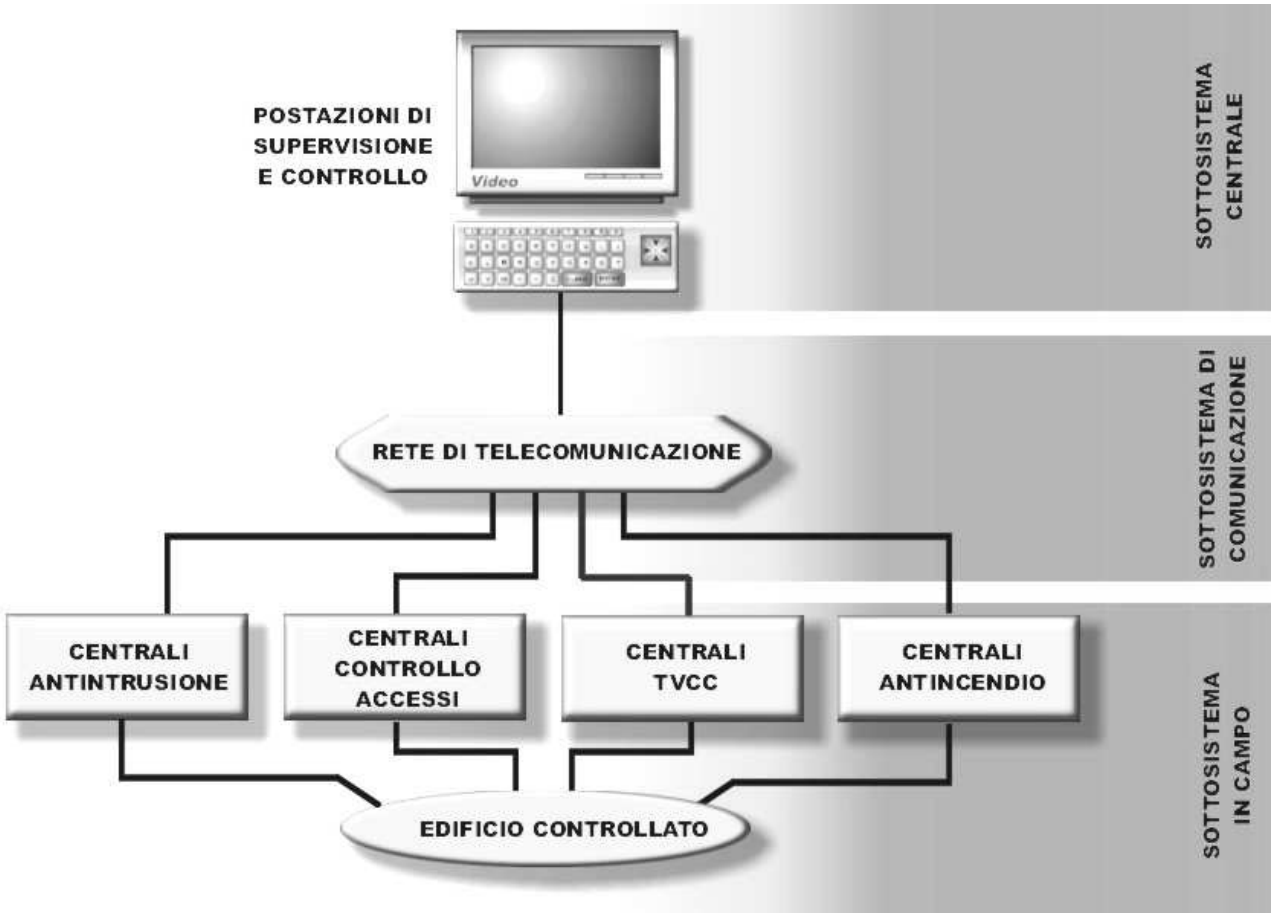

Fig.1 Architettura di un sistema integrato di sicurezza

5.1 Rete cablata

Il primo passo fondamentale nell'organizzazione di un sistema di sicurezza è la definizione della tipologia che dovrà assumere l'infrastruttura cablata in modo da integrarsi perfettamente con le tecnologie che dovrà gestire.
Questa infrastruttura deve rimanere stabile nel tempo. Le informazioni che vengono trasmesse attraverso una rete cablata necessitano di un sito centrale dove dovranno essere concentrate e rese disponibili.

5.2 Sala di controllo e gestione

Le informazioni che vengono trasmesse attraverso una rete cablata necessitano di un sito centrale dove dovranno essere concentrate e rese disponibili.
La sala di controllo e gestione (SCG) svolge tali funzioni e permette allo stesso tempo agli operatori di visualizzare e gestire le informazioni. Essa è senza alcun dubbio il fulcro della gestione del lavoro ordinario ed è fondamentale nelle emergenze.

5.3 Impianto di sorveglianza

Il sistema di sorveglianza di un'area ben definita deve essere realizzato per mezzo di un impianto TVCC (TV a circuito chiuso) che non rappresenta solo un semplice sistema di visione e videoregistrazione ma un sistema attivo in grado di reagire alle situazioni d'allarme.
Un sistema TVCC di nuova generazione deve consentire all'operatore di verificare in tempo reale gli eventi permettendo la gestione e l'immediato collegamento con i diversi servizi interessati.

Inoltre, indispensabile per il sistema di sorveglianza, è la necessità di integrarsi alle tecnologie e ai software capaci di elaborare, in tempo reale, le immagini video e trasformarle in dati significativi.
Fondamentale è l'affiancamento, ai sistemi TVCC, di impianti di controllo accessi e gestione allarmi che abbiano la capacità di lavorare in rete in remoto ma con un controllo centralizzato delle informazioni in maniera tale da permettere all'operatore di effettuare interventi mirati.
Le reti centrali di gestione allarme devono essere in grado di interagire in modo dinamico con i sistemi TVCC così da visualizzare su opportuni schermi la situazione reale dell'area interessata all'allarme.

5.4 Reti di comunicazione radio

È fondamentale poter disporre, per la gestione di un sistema integrato di sicurezza, di una rete di telecomunicazione radio dedicata di tipo evoluto per essere nelle migliori condizioni di gestione e coordinazione degli interventi.
Le tecnologie di nuova generazione superano il problema di avere una sola frequenza per ogni servizio permettendo una nuova tipologia operativa. Sono i cosiddetti "Sistemi TRUNKING" che possono utilizzare sia la tecnologia analogica che quella digitale.
La tecnologia analogica, considerando le caratteristiche tecniche ed economiche, è indicata per trasmissioni in piccole aree locali mentre la tecnologia digitale è applicabile per aree più vaste, regionali o nazionali.
L'interconnessione tra gli impianti di videosorveglianza e quelli radio, controllati da una centrale operativa, permette oggi una notevole interazione fra servizi di sicurezza di natura diversa per l'impiego efficace nel territorio da proteggere.

6 STRUMENTI PER ATTUARE UNA PROCEDURA D'EMERGENZA

Per far fronte in maniera funzionale ed efficace ai diversi scenari pericolosi che possono presentarsi in ambito portuale è dunque necessario individuare delle corrette procedure. In tal senso si deve organizzare una risposta funzionale del sistema gestione della sicurezza del porto per poter avere a disposizione uno strumento realmente utilizzabile per gestire un'emergenza.
È indispensabile una perfetta organizzazione per gestire, al meglio, le emergenze senza disperdere energie e personale in azioni inutili e indirizzarle da subito ove sia necessario.
È fondamentale disporre di un programma di addestramento di tutto il personale (incluso quello di sicurezza), corredato di aggiornamenti periodici ed esercitazioni. L'addestramento ideale deve essere continuativo ed efficace e deve essere mirato a rafforzare la capacità di garantire la sicurezza delle persone.
Il programma di addestramento e di esercitazione è promosso dal *Port Facility Security Officer* che ne è anche il coordinatore. Esso deve avere lo scopo di assegnare ad ogni persona il ruolo specifico nel programma della sicurezza.

6.1 Misure per il controllo accessi

Il controllo degli accessi è il primo controllo fisico da attuare per garantire un buon livello di sicurezza nel Porto. Alla luce dei recenti attentati terroristici, si devono attuare misure che non permettano alle persone di accedere e circolare in maniera incontrollata nell'area portuale. Le disposizioni da seguire richiedono che:

- il personale della sicurezza sia sempre presente nell'area dell'APO;
- tutto il personale ed i visitatori debbano portare badge numerati, colorati in modo da evidenziare la mansione del possessore all'interno della struttura portuale e dotati di sistemi RFID o SIM, quindi rilevabili da lettori di prossimità o lettori di dati;
- si utilizzino obbligatoriamente tecnologie per la lettura dei badge e sistemi di lettura targhe per la registrazione dell'ingresso e dell'uscita sia del personale che dei visitatori dai varchi;

- sia operativo un sistema informatico centralizzato per la sicurezza, con database specifici per l'acquisizione delle informazioni, capace di fornire agli operatori della sicurezza informazioni in tempo reale, in modo particolare per le autorizzazioni di accesso;
- le aree riservate siano ben chiuse;
- le disposizioni per l'accesso all'area portuale siano coordinate con il personale delle navi ormeggiate;
- esista un efficace sistema di illuminazione specifico per la sicurezza che sia mantenuto attivo durante le ore notturne;
- siano operativi sistemi di comunicazioni dedicati, basati su tecnologie di tipo trunking analogico o digitale, per permettere un collegamento costante ed affidabile tra i varchi e la Sala di Controllo.

Durante tutti i livelli di MARSEC il personale addetto alla sorveglianza degli accessi e del traffico mantiene costantemente il controllo su tutta la superficie e il perimetro dell'area portuale. Inoltre esso ha il compito di segnalare avarie del sistema d'illuminazione, dell'impianto di sorveglianza e di tutti gli incidenti della sicurezza.

6.2 Tecnologie impiegate

Oltre ai dispositivi e agli strumenti debitamente illustrati precedentemente, è possibile utilizzare ulteriori tecnologie di ultima generazione che rendono ancora più elevato lo standard di sicurezza sia per quanto riguarda la sorveglianza nell'area portuale che per il monitoraggio lato mare. Essi sono rappresentati da:

1. Termocamere per il controllo accessi lato mare: sono telecamere particolari che permettono la visione in condizioni sfavorevoli di scarsa o nulla visibilità. Vengono utilizzate di notte o in caso di nebbia per monitorare l'ingresso del porto e l'area dove attraccano le navi da crociera. Analogamente al sistema TVCC, i segnali delle termocamere vengono raccolti e remotizzati nei centri di controllo dell'Autorità Marittima.
2. Sistemi radiogeni per il controllo bagagli: sono apparecchi mobili che permettono lo screening del bagaglio.
3. Metal detector: sistemi per la rivelazione di armi. I modelli fissi devono essere installati in tutte le zone dove se ne ritiene opportuno l'uso, terminal passeggeri, aree doganali. I modelli mobili (hand held) possono essere usati nelle aree sopraelencate e in situazioni d'emergenza.
4. Incremento dell'illuminazione delle aree: è uno dei sistemi di deterrenza più efficaci contro le intrusioni e atti criminali.
5. Sistemi d'illuminazione mobili.
6. Rilevatori portatili di esplosivo/droga e rilevatori doppi fondi.
7. Pattugliamento a mare con motovedette armate: da applicare solo nei momenti di massima allerta.
8. Punto unico di accesso e punto unico di uscita per il terminal passeggeri: consente un'efficace ispezione e sorveglianza delle persone in transito.
9. Sistemi mobili anti – inquinamento: riescono in tempi brevi a circoscrivere eventuali fuoriuscite di prodotti petroliferi e chimici.

7. GESTIONE DELL'EMERGENZA

Per ottenere la migliore risposta di fronte alle minacce è quindi necessario avvalersi delle migliori tecnologie, che fanno riferimento ad una o più Sale di Controllo equipaggiate con software di gestione avanzato e sistema di sicurezza all'avanguardia, sempre efficiente e funzionante.
La sequenza di azioni da gestire si può riassumere in tre passi:

1. rilevazione dello stato d'emergenza;
2. comunicazione allarme alla SCG;
3. attuazione delle misure.

La rilevazione dello stato d'emergenza sarà eseguita direttamente dalle persone che si trovano nella zona dell'allarme o dagli operatori addetti alla sicurezza, oppure dagli operatori della SCG attraverso la segnalazione in arrivo dai sensori del sistema integrato di sicurezza.
Come già illustrato in precedenza, le comunicazioni dell'emergenza avvengono attraverso una avanzata rete di telecomunicazione e giungono ai terminali della Sala di Controllo e di Gestione.
A questo punto è necessario che il software di gestione della Sala di Controllo e Gestione disponga di una programmazione puntuale che permetta all'utilizzatore di esplicitare nei dettagli la sequenza delle azioni da intraprendere. Quando un segnale d'allarme giunge nella SCG si aziona il display d'allarme, che mostra immediatamente la posizione del sensore interessato all'evento. Le funzioni correnti del programma vengono sospese dando priorità alla gestione dell'emergenza.
Una volta individuata la natura della minaccia in atto, l'operatore dovrà procedere all'attuazione delle misure di sicurezza avviando la corrispondente procedura già programmata nel software di gestione.
Per fare ciò è necessario che la SCG trasferisca l'allarme agli enti interessati. Il software di gestione deve essere impostato per attuare, una volta rilevata la tipologia dell'emergenza, le chiamate necessarie.
Queste comunicazioni viaggiano su reti realizzate ad hoc, più veloci e affidabili di quelle ordinarie, protette da interferenze, sabotaggi e intasamenti.
Gli enti da contattare per fronteggiare un'emergenza sono:

- Autorità Portuale;
- *Port Facility Security Officer* dell'Autorità Portuale;
- Presidente dell'Autorità Portuale;
- Polizia o Commissariato del Porto;
- Capitaneria di Porto;
- Dogana;
- Guardia di Finanza;
- Vigili del Fuoco;
- Carabinieri;
- Emergenza Medica;
- Piloti;
- Ormeggiatori.

7.1 Procedura in caso di rivelazione di ordigno esplosivo con relativo rischio di danneggiamento/distruzione

Nel presente paragrafo si vuole illustrare, come esempio, la procedura relativa alla rivelazione di un ordigno esplosivo con il relativo rischio di danneggiamento/distruzione.
Si illustrerà, dunque, uno degli scenari più importanti, considerando anche la situazione internazionale attuale. Altre minacce quali presa in ostaggio di persone, contrabbando di armi e droga, traffico di clandestini, presentano, in linea generale, le stesse procedure di gestione, in quanto cambiano solo alcuni enti da contattare e alcune misure di sicurezza
Nel caso venga rinvenuto un pacco sospetto o si abbia la certezza di trovarsi di fronte ad un ordigno che potrebbe esplodere, in nessun caso esso deve esser toccato o rimosso.
Chi ha effettuato la scoperta deve immediatamente comunicare l'evento agli addetti alla sicurezza nelle vicinanze. Essi devono prontamente comunicare quanto rilevato alla SCG.
Dalla SCG gli operatori della sicurezza sono in grado di rilevare la zona interessata tramite i monitor a cui arriva il segnale delle telecamere; essi, grazie agli strumenti ausiliari come brandeggi e zoom, riescono a fornire numerose informazioni utili.
Nel momento in cui il segnale d'allarme giunge nella SCG, il software di gestione sospende automaticamente l'attività ordinaria per procedere con le direttive specifiche degli eventi straordinari.
A questo punto viene informato il PFSO e scattano le prime disposizioni di sicurezza: sia quelle che effettuate materialmente dal personale (sgombero e evacuazione) sia quelle effettuate dal software

di gestione della SCG (chiamate agli enti principali e disposizioni per blocco accessi) sono quasi contemporanee.
È obbligatorio lo sgombero della zona con immediato allontanamento delle persone presenti. L'evacuazione parziale o totale dell'area portuale deve avvenire in tempi rapidi e usando solo percorsi principali. Solo se questi ultimi non sono utilizzabili, si può passare attraverso accessi secondari.
La zona interessata dall'allarme deve essere delimitata in maniera fisica e ben visibile, e deve permettere l'accesso esclusivamente alle persone autorizzate.
Possono essere rese necessarie operazioni di controllo e perquisizione delle persone e dei veicoli che lasciano l'area portuale; tale misura di sicurezza è a discrezione del PFSO.
Il software di gestione della SCG deve essere in grado di effettuare chiamate agli enti da coinvolgere:

- Autorità Marittima;
- Autorità Portuale;
- Polmare;
- Artificieri.

E' necessaria, come ulteriore misura di prevenzione, far pervenire sul posto un'unità di primo soccorso.
Informate queste istituzioni, si attueranno contemporaneamente gli interventi relativi all'area dove è stato individuato l'ordigno e relativi alla sicurezza di tutto il porto.
Nel luogo interessato, debitamente messo in sicurezza e isolato, con arrivo delle Forze dell'Ordine, dei primi soccorritori, e del personale dei servizi d'emergenza, gli artificieri provvederanno a far detonare il dispositivo.
La procedura deve includere l'eventualità dello scoppio della bomba, sia essa collocata in una macchina in prossimità di un obiettivo o all'interno dell'obiettivo stesso.
La presenza delle istituzioni preposte garantisce il rapido soccorso alle eventuali persone ferite o vittime.
Le Autorità Marittime hanno il compito di innalzare, se necessario, il livello di MARSEC.
Il livello normale di lavoro si svolge con MARSEC 1.
In questo il MARSEC sarà innalzato a livello 3, cioè il più elevato. In particolare, si dovranno attuare le misure in grado di mettere in sicurezza l'area portuale.
A questo livello di sicurezza vanno adottate le seguenti ulteriori misure oltre a quelle indicate per i livelli MARSEC 1 e MARSEC 2 (come dagli allegati A e B dell'ISPS code):

- massimizzare l'uso dei dispositivi di sorveglianza e sicurezza;
- proibire l'accesso al Porto;
- mettere in sicurezza tutti gli accessi del Porto;
- considerare la possibilità di interrompere le operazioni di carico e scarico delle merci;
- eseguire tutte le disposizioni dell'Autorità Marittima, delle Forze dell'Ordine e della Direzione per quanto riguarda specifiche attività;
- sospendere gli arrivi delle navi fino a quando il livello di sicurezza sarà riportato MARSEC 2;
- assicurarsi che tutte le navi ormeggiate siano informate del livello di MARSEC in atto;
- attivare la sorveglianza lato mare;
- prepararsi ad evacuare totalmente o parzialmente il Porto.

Queste disposizioni dovranno valere fino a quando il livello MARSEC verrà riportato a quello ordinario, con doverosa e immediata comunicazione a tutti gli enti coinvolti.

8. CONCLUSIONI

Quanto illustrato sinora dimostra come sia importante affrontare le gestione della security con la dovuta competenza e preparazione, prestando particolare attenzione a tutti quei fattori che costituiscono il sistema integrato di gestione o interagiscono con esso, ricordando che anche la

trascuratezza di un dettaglio ritenuto di secondaria importanza può inficiare l'efficienza dell'intero sistema.

9. BIBLIOGRAFIA

1. F. Garzia ,"Impianti e sistemi di sicurezza", Carocci Editore, 2001.
2. F. Garzia, T.Bucciarelli, R. Cusani, G.M. Poscetti, "Sicurezza delle comunicazioni", ILSOLE 24 ORE, (in pubblicazione).
3. F. Garzia (editore), "Il progetto della sicurezza", numero speciale luglio/agosto 2005 della rivista MODULO, BE-MA editrice, Milano, 2005.
4. Garzia, F., Sammarco, E., "The integrated security system of the Vatican City State", SAFE 2005, WIT Press, Southampton (UK), pp. 391-403, 2005.
5. Garzia, F., "The integrated supervision and control system of the Gran Sasso mountain", SAFE 2005, WIT Press, Southampton (UK), pp. 699-711, 2005.
6. Garzia, F., Sammarco, E., De Lucia, M., "The security telecommunication system of the Vatican City State", Risk Analysis IV, WIT Press, Southampton (UK), pp.773-782, 2004.
7. Garzia, F., "The integrated safety/security system of the Accademia Nazionale dei Lincei at Corsini Palace in Rome", Proc. of International Conference on Integrating Historic Preservation with Security, Fire Protection, Life Safety and Building Management Systems, Rome (Italy), pp.77-99, 2003.
8. Garzia, F., Cusani, R. "Wireless LAN optimal design in the underground Gran Sasso mountain national laboratories of Italian Institute of Nuclear Physics", Proc. of Energy, Environment and Technological Innovation, Rio de Janiero (Brazil), 2004.
9. Garzia, F., Veca, G. M., "Integrated security systems for hazard prevention, management and control in the Italian high speed train line", Risk Analysis III, WIT Press, Southampton (UK), pp.287-293, 2002.
10. Antonucci, E., Garzia, F., Veca, G.M., "The automatic vehicles access control system of the historic al centre of Rome", Sustainable City II, WIT Press, Southampton (UK), pp.853-861, 2002.
11. Monica Riannetti, Leonardo Vanni, "Norme e Organizzazione del Trasporto Navale di Merci Pericolose",studi e ricerche STIMA,Sicurezza dei Trasporti in mAre, volume n°1; 2004
12. Pamela Giacchini, Leonardo Pasquali, Barbara Pecchia, "Evoluzione della normativa internazionale ed europea in materia di sicurezza del trasporto in mare" studi e ricerche STIMA,Sicurezza dei Trasporti In Mare, volume n°7; 2004
13. Bardazza, M. M., Vestrucci, B., Zappellini, G., Adinolfi, P., Buldrini, M., La Rovere, S., Vercilli, C., "Application of a Systematic Methodology to Terrorism Risk Management", SAFE 2005, WIT Press, Southampton (UK), 2005.
14. Waltz, E., "Information Warfare – Principles and operations", Artech House Publisher, Boston (USA),1998.
15. Denning, D. E., "Information Warfare and Security", Addison-Wesley, Boston (USA), 1999.
16. Nichols, R.K. & Lekkas, P.C., "Wireless Security: Models, Threats, and Solutions", McGraw-Hill", New York (USA), 2002.
17. AUTORI VARI, CCTV for public safety:1997-98 report, Security Industry Association, New York (USA), 1999.
18. AUTORI VARI, Emergency planning, BOMA Building Owner and Manager Association International, Washington DC (USA), 2000.
19. AUTORI VARI, Mastering security using technology, Security Management Reprint Series, American Society for Industrial Security, Alexandria (Virginia, USA), 1996.
20. AUTORI VARI, National study of false alarms, consumer and business, Security Industry Association, New York (USA), 1999.
21. AUTORI VARI, Physical security, Security Management Reprint Series, American Society for Industrial Security, Alexandria (Virginia, USA), 1997.
22. AUTORI VARI, Security and privacy, IEEE Institute of Electrical and Electronics Engineers, Piscataway (NJ, USA), 2000.

23. AUTORI VARI, Security planning guidebook. Safeguarding your tenant and property, BOMA Building Owner and Manager Association International, Washington DC (USA), 2000.