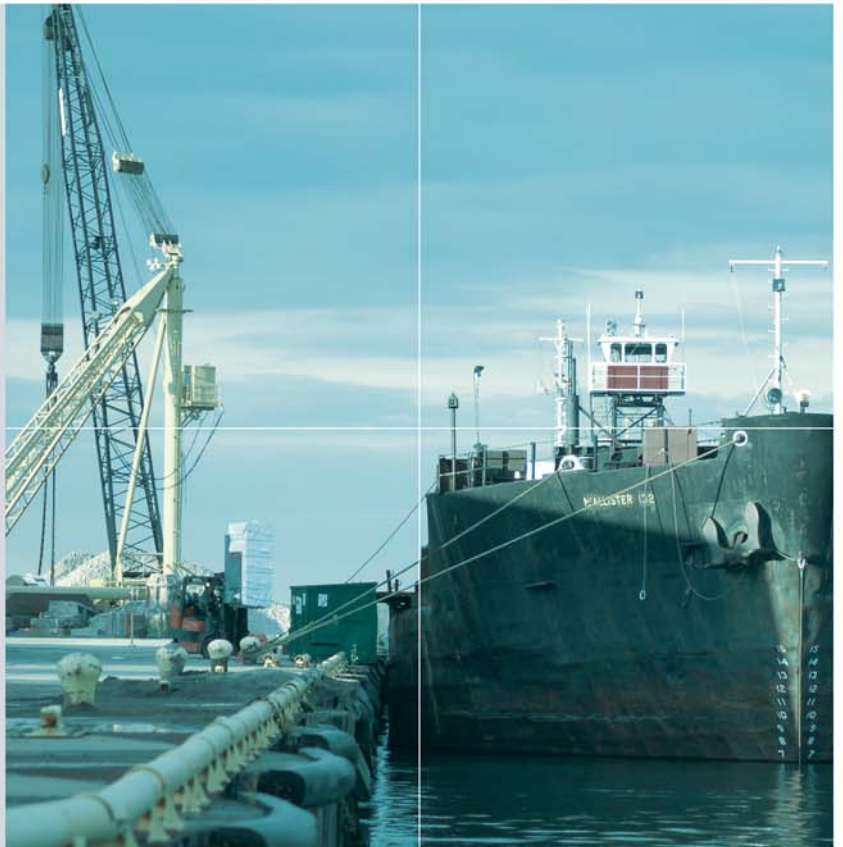




# La Sicurezza in Porto

Come proteggere le aree portuali ed assicurare un efficace sistema di sicurezza per il traffico merci e passeggeri





## Scenario di riferimento

I porti, spesso situati in prossimità di città, assumono un ruolo essenziale del sistema logistico di trasporto, in quanto consentono il collegamento fra le rotte marittime e terrestri del commercio e del traffico passeggeri.

L'impatto delle minacce ordinarie o straordinarie per la sicurezza portuale è dunque particolarmente rilevante ed appare in tutta la sua evidenza se si considera che:

- » il 90% dei commerci esterni della UE avviene via mare
- » il 40% dei commerci interni della UE avviene via mare
- » il 20% delle navi che battono bandiera europea è vittima di pirateria

S'impone allora l'esigenza di salvaguardare, da un lato, le vie dei rifornimenti e dei commerci e, dall'altro, la fiducia degli utenti nella sicurezza della navigazione.

Un fattore importante per potenziare l'economia del paese è legato alla capacità di incrementare i volumi di merci e passeggeri trasportati via mare e ciò può avvenire solo consolidando il binomio "trasporto e sicurezza" e cercando di sfruttare le potenzialità derivanti dal contesto organizzativo, normativo e tecnologico.



## Il contesto organizzativo

Per organizzare un sistema di sicurezza efficace è necessario partire dalla definizione di un programma che tenga conto di vari aspetti.

E' fondamentale partire dall'Analisi del Rischio che, una volta individuato l'ambiente sul quale intervenire, prevede:

- » l'individuazione delle minacce e vulnerabilità
- » l'analisi dei controlli già in essere
- » la valutazione delle probabilità degli eventi dannosi
- » la valutazione dell'impatto come stima delle potenziali perdite
- » la determinazione del livello di rischio
- » l'identificazione delle contromisure idonee ad abbattere il livello di rischio stesso
- » la fase operativa realizzando sia le contromisure opportune sia il monitoraggio per attuare azioni correttive

Il programma, specializzato per l'analisi dei rischi, la pianificazione, l'attuazione ed il controllo delle misure di sicurezza, si sviluppa principalmente nelle quattro fasi del "Ciclo di Deming" (**PDCA**):

- » Pianificazione (Plan)
- » Realizzazione (Do)
- » Controllo (Check)
- » Correzione (Act)

Tale ciclo è molto utile per assicurare un progressivo miglioramento della qualità, richiesto dagli attuali standard, attraverso l'applicazione di un metodo ordinato ed efficace nella gestione dei processi dinamici come quelli che si presentano nei contesti portuali.



## La situazione normativa

### L'impianto normativo

L'impianto normativo sulla sicurezza portuale considera molti aspetti:

- » l'elevato traffico dei beni, mezzi ed individui coinvolti nella filiera marittima; basti pensare all'elevato numero di "container" che vengono quotidianamente lavorati nei porti commerciali ed industriali o l'elevato numero di passeggeri che transitano con i loro mezzi nei porti turistici nel periodo estivo;
- » le diverse modalità di trasporto internazionale dei beni da sorgente a destinazione con interoperabilità normativa articolata a seconda che sia su rotaia, gomma, via fiume, via mare, via aereo;
- » potenziali conflitti di competenza giurisdizionale dovuti alla presenza nell'area portuale di rappresentanti istituzionali e non dediti alla sicurezza pubblica quali: la Capitaneria di Porto, la Guardia di Finanza, la Polizia di Frontiera, la Polizia di Stato, la Dogana, i Vigili del Fuoco, eventuali Istituti di Vigilanza Privati;
- » il numero elevato di attori che operano nell'area portuale: società di trasporto su gomme, compagnie navali, aziende di logistica, società che lavorano per la sicurezza degli impianti portuali, i turisti;
- » il coinvolgimento di attori pubblici e privati che sostengono il peso economico di un progetto di sicurezza portuale.

A livello europeo la normativa di riferimento è la direttiva UE 725/2004 che si rifà a quella internazionale, ovvero al capitolo XI-2 della convenzione **SOLAS** (International Convention for Safety of life at Sea) e all'**ISP Code** (International Ship and Port Facility Security Code).

In Italia, la Sicurezza Portuale si basa sulle funzioni governative del **CISM** (Comitato Internazionale per la Sicurezza Marittima e dei Porti), che ha il compito di elaborare un programma nazionale contro atti terroristici rivolti al settore marittimo e di stabilire il livello di sicurezza secondo quanto fissato dall'**IMO** (International Maritime Organization).



## L'International Maritime Organization

Nel Dicembre 2002, a poco più di un anno dell'attentato di New York, viene emanato dall'IMO a Londra, sotto una fortissima spinta degli Stati Uniti, l'**ISPS Code**.

Le nuove disposizioni di natura obbligatoria definiscono un complesso di norme indispensabili per rafforzare la protezione del trasporto marittimo, prevedendo un insieme di misure di sicurezza attive e passive articolate su tre livelli (normale, rafforzato, elevato) la cui attuazione concreta è correlata all'analisi dei rischi (**Risk Assessment**).

In particolare, il nuovo ordinamento dei trasporti navali rende obbligatoria la designazione dei **soggetti responsabili** dell'applicazione delle misure di sicurezza (agenti di sicurezza della nave, della società e dell'impianto portuale) e la definizione di un **Piano di Security** (preparato dalla Compagnia per le navi e dal terminalista per le Port Facility) che tenga conto dell'analisi dei rischi sia della nave che dell'impianto portuale.

Viene, inoltre, previsto il rilascio di un **certificato internazionale di sicurezza della nave**.

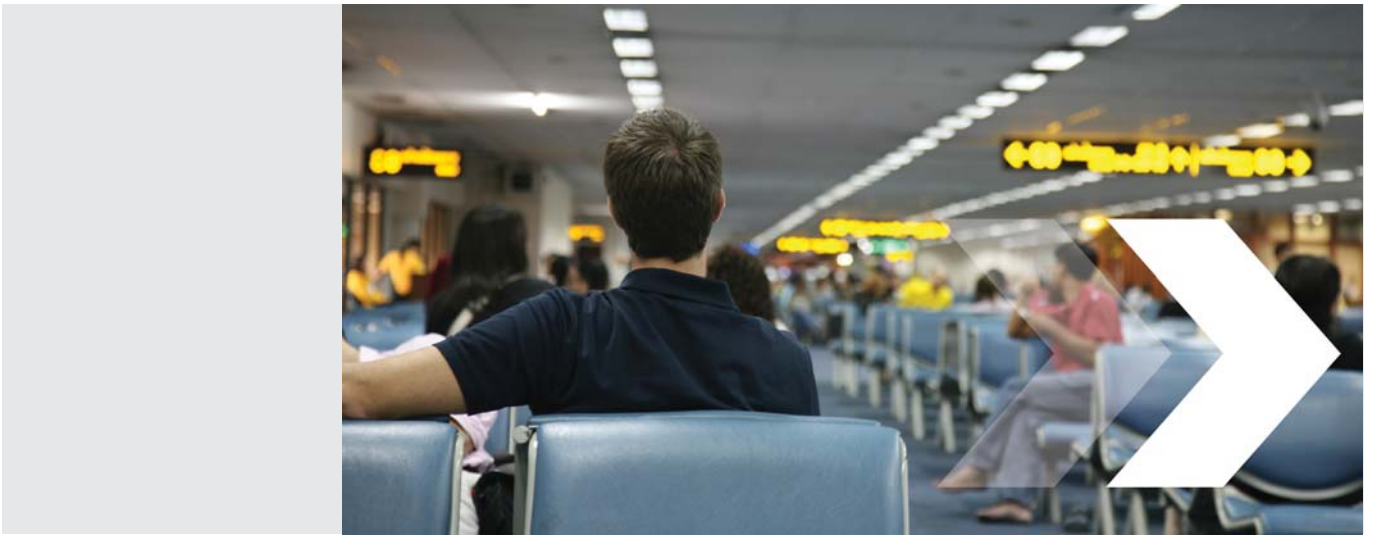


## La Direttiva Europea

La Direttiva dell'Unione Europea 2005/65, unitamente al D.Lgs 203/2007, ha contribuito ad ampliare i concetti di security portuale, prevedendo una serie di prescrizioni che coinvolgono l'intero sistema di approdo e scarico di persone e merci provenienti dal mare.

Tali procedure presuppongono l'applicazione degli strumenti di valutazione del rischio e di pianificazione ed implementazione dei piani security in un'area molto estesa e complessa, caratterizzata da spazi comuni, aree di transito e viabilità, magazzini, depositi di container vuoti, parcheggi per autoveicoli, strettamente connessa al trasporto marittimo, anche se distante dall'interfaccia nave/porto.

Sulla base della normativa internazionale, integrata dalla normativa e dalle linee guida nazionali, tutto il settore marittimo è stato così coinvolto in un vasto piano di adeguamento del proprio sistema di security.



## La Security Portuale

### Port Facility Security Assessment (PFSA)

L'Autorità Portuale (ove costituita, altrimenti l'Autorità Marittima) ha la responsabilità di effettuare la valutazione del rischio degli impianti portuali e delle parti comuni.

Al fine di corrispondere al meglio a questo delicato compito può ricorrere, qualora non disponga di skill professionali al proprio interno, alla consulenza di società specializzate.

In Italia, a differenza di molti altri paesi, non sono state individuate le Recognised Security Organization (RSO) che, in base all'ISPS Code, possono svolgere le attività di pianificazione e gestione del sistema di sicurezza portuale al posto dell'Autorità Designata.

Sulla base delle linee guida emanate dal CISM, la valutazione del rischio avviene secondo il seguente schema:

**Valutazione scenari ed individuazione dei possibili obiettivi:** vanno debitamente considerati scenari di rischio connessi ad attentati terroristici, attività di taccheggio (o tampering), traffico di esseri umani;

**Individuazione dei punti di debolezza e valutazione del rischio:** vengono ipotizzati eventi anche molto improbabili, ma con alto potenziale di impatto in termini di perdite umane e di danno all'infrastruttura portuale;

**Indicazione delle misure di mitigazione:** il PFSA deve contenere un'indicazione circa le possibili misure di mitigazione, sia di tipo organizzativo che infrastrutturale, nella prospettiva di ridurre la probabilità e l'incidenza dell'evento.



## Port Facility Security Plan (PFSP)

Il Port Facility Security Officer (PFSO) ha la responsabilità di realizzare, sulla base delle indicazioni contenute nel PFSA e secondo le indicazioni della normativa di riferimento, il Piano di Security dell'Impianto Portuale.

In questo importante documento sono contenute tutte le indicazioni relative alle misure organizzative, tecniche ed infrastrutturali che la società terminalista deve porre in essere a difesa della propria azienda e dell'interfaccia nave/porto, con riguardo a ciascuno dei tre Livelli di Security previsti.

L'ISPS Code individua i principali contenuti del Piano di Security dell'impianto portuale:

**Accesso alla Port Facility:** e' previsto il rigoroso controllo degli accessi alle aree portuali, per garantire sia la security che la safety degli utenti di questa particolare infrastruttura.

**Zone ad accesso ristretto:** con questa espressione si fa riferimento ad aree particolarmente sensibili del terminal (depositi di carburante, centrali elettriche, telefoniche e radio, sale di comando e controllo, strutture IT), in quanto ospitano obiettivi cruciali che meritano una specifica protezione in caso di attacco dall'esterno.

**Movimentazione del carico:** il controllo all'ingresso del carico, durante il deposito ed al momento dell'imbarco, rappresenta un momento critico che va disciplinato, attraverso il PFSP, secondo puntuali protocolli di sicurezza; nel caso di traffico container, il controllo della presenza e dell'integrità del sigillo, nonché l'utilizzo quando possibile di high security seal, appare indispensabile al fine di verificare debitamente l'integrità della merce e la sicurezza dell'intera catena logistica.

**Consegne delle provviste di bordo:** l'ingresso a bordo della nave delle provviste deve avvenire solo a seguito di accurati controlli sull'identità, sulla ragione e sulla tipologia della consegna e dopo un'attenta verifica degli alimenti.



**Movimentazione di bagaglio non accompagnato:** soprattutto nel settore crocieristico, la gestione del bagaglio, in particolare quello gestito in assenza del proprietario, riveste particolare criticità; il Programma Nazionale di Sicurezza Marittima, su questo punto, indica procedure e standard minimi che devono essere tenuti in considerazione, sia per la parte organizzativa e di formazione, che per la scelta dei macchinari di controllo bagaglio.

**Sorveglianza e pattugliamento:** nell'ambito della sorveglianza della port facility, la componente umana si salda con la componente tecnologica. Il controllo del sistema portuale deve avere come oggetto sia la banchina che le aree adibite a deposito, posto che nel nostro paese la responsabilità della sorveglianza degli specchi acquei non ricada sul terminalista; normalmente si utilizza personale formato al fine di garantire il pattugliamento, spesso affiancati da sistemi di videosorveglianza più o meno sofisticati. La scelta della soluzione dipende in massima parte dal livello di rischio, accuratamente valutato in fase di risk assessment e dalla configurazione dell'infrastruttura portuale.

**Comunicazioni di security:** deve essere garantita la possibilità di effettuare comunicazioni relative agli aspetti di security (sia attraverso sistemi radio che telefonici e mediante la rete internet) fra l'interno della nave e l'esterno, in ogni momento, soprattutto in situazioni di emergenza.

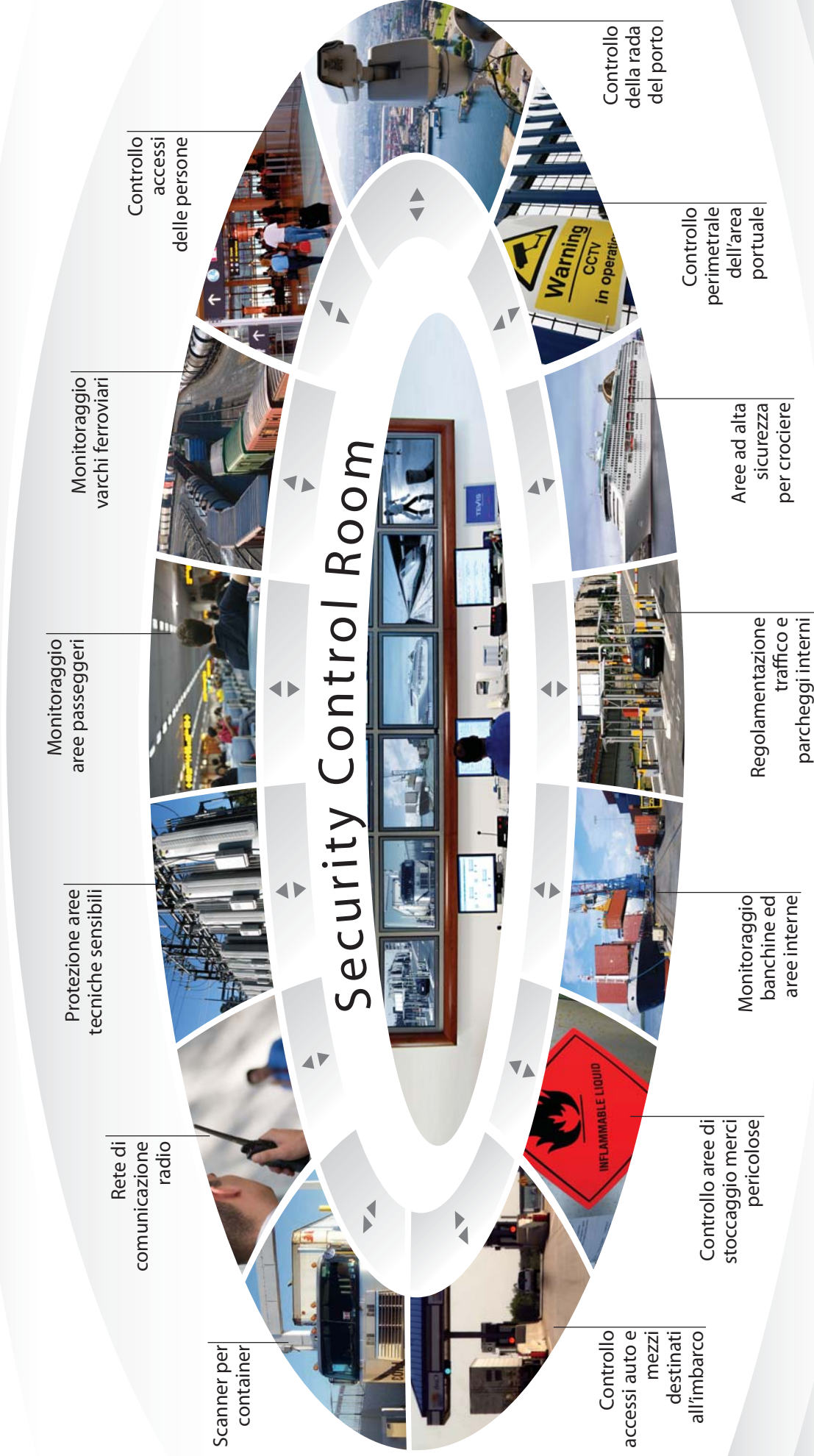
**Formazione, informazione e familiarizzazione:** l'ISPS ed il Programma Nazionale di Sicurezza Marittima prevedono percorsi formativi definiti per tutti coloro che esercitano a vario titolo compiti di security.

La formazione è destinata ai PFSO ed ai loro deputy. L'informazione al personale con compiti diretti di security ha per oggetto i contenuti del PFSP, mentre un livello minimo di familiarizzazione con i protocolli operativi di sicurezza è previsto per tutto il personale della Port Facility.

**Esercitazione ed addestramenti:** la normativa internazionale prevede un obbligo di esercitazione almeno trimestrale, da effettuare anche in collaborazione con le Forze di Polizia.

Ulteriori addestramenti possono essere pianificati dall'Autorità designata, ovvero da altri soggetti istituzionali (Polizia di Frontiera, Guardia di Finanza, ecc.).

# Sistema Integrato di Sicurezza Portuale



## Soluzione a 360°



## Un nuovo modello di sicurezza integrata

Nessun sistema di sicurezza può risultare efficace senza una profonda analisi e puntuale progettazione; pertanto è fondamentale definire un progetto che sia frutto di accurati sopralluoghi e di attenti calcoli che tengano conto delle vigenti disposizioni di legge.

Di seguito si propone un nuovo sistema integrato di sicurezza a 360°.

### **Controllo Accessi**

Il sistema di controllo accessi è realizzato mediante un insieme di accorgimenti e soluzioni, atti a verificare e controllare il personale che entra nel sedime portuale. Tali soluzioni comprendono, *badge* con diversi privilegi di accesso, *tag* per il controllo dell'accesso degli automezzi, tornelli per i pedoni, sbarre, dossi e sistemi di canalizzazione del flusso veicolare.

### **Monitoraggio delle Aree Interne, dei Varchi e degli Impianti Portuali**

Il sistema di monitoraggio è costituito da un insieme di telecamere che riprendono i punti più significativi delle aree portuali comuni, da un insieme di componenti tecnologiche in grado di acquisire i flussi video ripresi dai sistemi di videosorveglianza degli impianti portuali e da una piattaforma di controllo che ne governa il funzionamento e fornisce l'interfaccia verso gli operatori.



### **Controllo Perimetrale**

Il controllo perimetrale consiste in un sistema di rilevazione delle intrusioni, composto da un insieme di telecamere poste a controllo dei perimetri, da un sistema di antiscavalamento realizzato mediante difese passive (concertina e fili tesi) e difese attive (fibra ottica), da un cavo microfonico, da barriere IR e/o a microonde e da una piattaforma di controllo che governa il funzionamento del sottosistema e fornisce l'interfaccia verso gli operatori; il sistema di rilevazione segnala automaticamente tentativi di intrusione, attivando, nel caso, apposite registrazioni e generando allarmi per il centro di monitoraggio.

### **Controllo della Rada del Porto**

Il controllo della rada del porto è costituito da telecamere termiche e da radar in grado di rilevare intrusi con qualsiasi condizioni di tempo (nebbia, pioggia, grandine ecc.).

### **Controllo delle Targhe e dei Codici ISO dei container**

Il controllo delle targhe e dei codici ISO dei container è costituito da telecamere Megapixel e da particolari software OCR, in grado di leggere le targhe degli automezzi ed i codici dei container tramite opportuni software al fine di controllare e consentire l'accesso al porto.

### **Controllo delle Aree di Stoccaggio e delle Merci Pericolose**

Mediante protezioni perimetrali, sistemi TVCC e la regolamentazione degli accessi (come ad esempio lettori biometrici) è possibile autorizzare l'ingresso solo al personale preposto con definizione di differenti livelli di accesso ad aree sensibili.



### **Monitoraggio Varchi Ferroviari**

Il monitoraggio dei varchi ferroviari consiste in un sistema che verifica automaticamente il treno (numero dei vagoni) e il container sopra il treno (codice container), quando questo passa attraverso il *gate*.

### **Rilevazione ed abilitazione dei Transiti ai Varchi**

La rilevazione ed abilitazione dei transiti ai varchi consta di un insieme di apparati e sistemi tecnologici per la registrazione e l'abilitazione agli accessi delle persone e dei mezzi; il sistema di rilevazione e abilitazione è inoltre dotato di una piattaforma di controllo che governa il funzionamento del sottosistema e fornisce l'interfaccia verso gli operatori.

### **Rilevazione di Esplosivi e Droga all'interno dei container**

Mediante opportuni apparati che sfruttano le proprietà dei raggi gamma, si possono rilevare sostanze pericolose all'interno dei container quali esplosivi (commerciali, militari e fatti in casa) e droghe (cocaina, eroina, ecc.).

### **Integrazione con Enti esterni o Forze dell'Ordine**

L'integrazione con Enti esterni o Forze dell'Ordine è costituita da una infrastruttura e da apparati tecnologici basati su tecnologia TETRA, in grado garantire comunicazioni e trasmissioni dati sicure con tutte le Forze dell'Ordine e con i corpi speciali che devono collaborare.

### **Controllo dei Viaggiatori e dei Bagagli per la zona crociera**

Il controllo dei viaggiatori e dei bagagli per la zona crociera è costituito da un insieme di apparati necessari per il controllo delle persone che poi dovranno imbarcarsi, quali *metal detector* e di apparati per il controllo dei bagagli quali scanner a raggi X e rilevatori di esplosivi.



### **Centrale Operativa**

La centrale operativa è costituita da tutti gli apparati di centralizzazione, in cui trovano posto tutti i sistemi di archiviazione ed elaborazione delle immagini e degli allarmi che provengono dal campo. Il sistema assicura il presidio di sorveglianza presso l'Autorità Portuale ed è essenzialmente costituito da una sala di controllo dalla quale è possibile tenere costantemente sotto sorveglianza le aree portuali, i perimetri, gli specchi d'acqua ed i varchi; ciò consente la gestione dei passaggi da un livello di sicurezza a quello superiore e viceversa oltre a garantire capacità di comunicazione con la Prefettura, le Forze dell'Ordine e gli impianti portuali.

### **Integrazione dei Sistemi di Sicurezza**

Mediante una piattaforma software scalabile è possibile integrare i sistemi di sicurezza portuali; grazie, infatti, ad un'unica interfaccia, facilmente gestibile dall'operatore, è possibile far interagire tutti i sistemi con maggiore efficacia.

### **Manutenzione**

Tutti i sistemi di sicurezza, se non opportunamente mantenuti, sono destinati ad essere utilizzati non al massimo delle prestazioni diminuendo il loro ciclo di vita e non soddisfacendo pienamente le aspettative del cliente. In quest'ottica, si reputa importante la manutenzione programmata e preventiva in modo da avere un sistema che garantisca sempre il massimo delle sue prestazioni.

### **Formazione**

E' fondamentale, per ultimo, formare ed aggiornare periodicamente il personale addetto alla sicurezza secondo quanto stabilito anche dall'ISPS Code (CSO, PFSO, ecc.) e tenendo presenti le singole necessità delle realtà portuali.



## Gruppo DAB

### Polo Tecnologico Sicurezza

Il Gruppo DAB, con oltre trentacinque anni di esperienza, è tra le aziende leader in Italia nel settore Security & Safety.

Il Gruppo nasce dalla volontà di realizzare un polo tecnologico di eccellenza per la Sicurezza di beni e persone operando sia in ambito pubblico che privato, con l'obiettivo di diventare **Security Partner** di clienti esigenti che intendono sviluppare economie di scala e certificare i risultati.

La holding, con sede a Roma, è costituita da cinque aziende che lavorano sinergicamente tra loro per offrire soluzioni integrate ed innovative in diversi settori di mercato.



**Redev** (Ricerca & Sviluppo)



**Epro Engineering** (Analisi & Progettazione)



**DABsi** (Sistemi Integrati di Sicurezza)



**TraiCon** (Consulenza & Formazione)



**Tevis** (Vigilanza & Telemonitoraggio)

Il Polo si impegna a promuovere una forte "Cultura della Sicurezza", organizzando eventi ove Enti e Aziende si confrontano per trovare insieme soluzioni sempre più concrete e risolutive per la sicurezza sociale.



## La Sicurezza in Porto

Come proteggere le aree portuali ed assicurare un efficace sistema di sicurezza per il traffico merci e passeggeri



**POLO TECNOLOGICO SICUREZZA**

### **Gruppo DAB S.p.A.**

#### **Sede Legale e Direzione Generale**

Via Tiburtina 1135  
00156 Roma

Tel. +39 06.41.21.21 r.a.  
Fax +39 06.41.20.04.77

#### **Filiale Area Nord**

Viale Sarca 336/F  
20126 Milano

Tel. +39 02.89.91.97.79 r.a.  
Fax +39 02.89.91.97.89

#### **Uffici di Bologna**

Via N. Dall'Arca 58/C  
40129 Bologna

Tel. +39 051.41.52.181 r.a.  
Fax +39 051.41.52.117

[www.gruppodab.it](http://www.gruppodab.it)  
[info@gruppodab.it](mailto:info@gruppodab.it)