Titolo del progetto di ricerca

L'impatto di nuove tecnologie sulla security del trasporto marittimo quale elemento della catena logistica integrata

Responsabile: Prof. Giuseppe Sciutto – Dipartimento di Ingegneria Elettrica

1. Obiettivi del progetto

Obiettivo del progetto è lo studio degli impatti legati all'impiego delle nuove tecnologie sulla security del trasporto marittimo nell'ambito della catena logistica integrata.
Lo studio prevede nella prima fase la definizione di un approccio metodologico basato su tecniche di analisi del rischio al fine di identificare i possibili azzardi derivanti da azioni dolose o terroristiche perpetrate nell'ambito della realtà portuale ai danni delle infrastrutture o delle merci nel nodo di scambio modale gomma-ferro-nave, sulle banchine o nei piazzali, valutarne la probabilità di occorrenza e le conseguenze sull'incolumità delle persone e sull'integrità dei beni, tenendo in debito conto tutte le azioni mitigatrici poste in essere. Mediante tale approccio sarà possibile classificare il rischio connesso con ciascun azzardo sulla base del binomio gravità delle conseguenze – frequenza dell'evento e valutare come lo stesso risulti influenzato dall'adozione di tecnologie a supporto della security. Nella seconda fase del progetto, a valle dell'identificazione delle menzionate tecnologie, la metodologia individuata sarà applicata sia a ipotetici scenari operativi che ad un case study reale, onde validarne generalità funzionale ed applicabilità operativa.
Il progetto di ricerca proposto trova naturale collocazione nell'ambito della Linea 3 – *Logistica e sicurezza*, fermo restando che durante lo sviluppo delle attività potranno rendersi necessarie sinergie con i ricercatori della Linea 4 – *Il porto come nodo logistico*.

2. La security in campo marittimo

A valle dell'attacco terroristico dell'11 settembre 2001 alle Twin Towers di New York è cresciuta in tutto il mondo l'attenzione a prevenire eventuali azioni terroristiche o comunque a limitarne i danni. Il problema è evidentemente complesso poiché nella società occidentale sono svariati i siti ove un'azione terroristica può avere luogo (obiettivi sensibili), come diverse sono le tecniche terroristiche che possono essere attuate. La rete dei trasporti risulta facilmente esposta a minacce terroristiche, che possono essere messe in atto con alta efficacia dal punto di vista dei danni economici arrecati. E' stato stimato che un attacco in un opportuno punto della catena logistica, quale un porto, con armi di distruzione di massa o esplosivo contenuto in un container potrebbe facilmente comportare un impatto economico superiore a un miliardo di dollari.
I timori relativi ai porti sono di varia natura: si può andare dalla gasiera fatta esplodere all'interno del porto, al container carico di esplosivo o contenente un'arma nucleare.
Gli USA hanno ritenuto i traffici marittimi, e le infrastrutture a loro connessi, estremamente vulnerabili e contemporaneamente strategici per l'economia poiché i 361 porti dell'Unione movimentano il 95% delle merci trasportate in import/export e 7500 navi commerciali ogni anno originano circa 51.000 movimenti.
Di conseguenza gli USA si sono dotati di strumenti legislativi, organizzativi e tecnologici tesi a limitare il rischio di atti terroristici.
L' Amministrazione Doganale Americana ha avviato le seguenti principali iniziative:

- il C-TPAT (Custom - Trade Partnership Against Terrorism) che prevede che gli operatori internazionali del trasporto operino per valutare, sviluppare e comunicare nuove procedure tese a aumentare il livello di sicurezza operando sull'intera catena logistica. In cambio viene loro garantita una maggiore velocità nell'inoltro delle merci all'interno degli USA;
- la CSI (Custom Security Initiative) che prevede la realizzazione di accordi bilaterali con i Governi stranieri al fine di effettuare lo screening e l'ispezione di container a potenziale rischio attraverso procedure, scambi di informazioni e tecnologie idonee. La priorità di attuazione riguarda i 20 più grandi porti nel mondo che coprono il 68% dei sedici milioni di container destinati agli Stati Uniti ogni anno. Le dogane italiane hanno aderito alla CSI nel novembre 2002. Nell'ambito della CSI è operativa dal

febbraio 2003 la cosiddetta regola delle 24 ore, che prevede la comunicazione del manifesto di carico alle autorità USA 24 ore prima che le merci siano caricate in una nave con destinazione USA.

Il Congresso Americano ha inoltre istituito il DHS, Department of Homeland Security, ed adottato il MTSA (Maritime Security Act) operativo già dal luglio 2003 mediante le "Interim Final Rules".
Sulla scia di queste iniziative, caratterizzate spesso dall'essere fortemente unilaterali, si è reso ben presto evidente che anche gli altri paesi interessati all'interscambio con gli USA avrebbero dovuto organizzarsi con strumenti analoghi per addivenire ad una forma di governo della sicurezza globale per il mondo dello shipping.
In tal senso l'IMO (International Maritime Organization) ha elaborato una serie di emendamenti al SOLAS (Safety Of Life At Sea Convention) del 1974, il più ampio dei quali incorpora il nuovo codice ISPS (International Ship and Port Facility Security Code). Gli emendamenti al SOLAS e l'ISPS code sono stati recepiti nella conferenza IMO del dicembre 2002 a Londra.
A livello europeo, recependo per lo più quanto elaborato dall'IMO, la Commissione dell'Unione Europea ha presentato nel maggio 2003 al Consiglio e al Parlamento Europeo una proposta di regolamento Europeo relativo al miglioramento della security delle navi e degli impianti portuali, approvato nel marzo 2004. La necessità di tale regolamento nasce dalla volontà di creare un contesto comunitario uniforme ed evitare che l'applicazione delle disposizioni contenute negli emendamenti della convenzione SOLAS e delle disposizioni del Codice ISPS possano portare distorsioni di concorrenza tra gli Stati membri. Il regolamento ha quindi il compito di armonizzare a livello di Comunità la normativa sulla security. Si tratta di disposizioni che riguardano i piani e la valutazione di sicurezza delle navi e degli impianti portuali, talune competenze dei governi contraenti in materia di sicurezza, nonché l'obbligo per la società di navigazione di fornire al comandante informazioni concernenti gli operatori della nave nelle realtà portuali europee.
Ad oggi gli emendamenti alla convenzione SOLAS e il menzionato regolamento della UE costituiscono i documenti cui è necessario riferirsi per lo sviluppo della security, nell'attesa di due direttive comunitarie nel settore.
La prima direttiva sulla port security dovrebbe estendere all'intera area portuale i principi del codice ISPS che, al momento, riguarda solo le cosiddette aree di interfaccia nave-porto. A tal fine nel porto potranno essere distinte sotto-aree con diversi requisiti in merito alla security.
La seconda direttiva allo studio riguarda la security del trasporto intermodale. Essa trae origine dalla consapevolezza che le problematiche di security nel caso delle merci non possono essere affrontate efficacemente ed efficientemente considerando un solo nodo, per quanto importante come il porto, di tutta la catena del trasporto. Dovrebbe quindi realizzarsi un approccio alla sicurezza comune per tutti i modi di trasporto pur tenendo conto delle peculiarità di ciascuno di questi. L'adeguamento alle norme attuali e future implicherà, come altresì auspicato dalla Commissione europea, un utilizzo diffuso di moderne tecnologie per lo scambio e registrazione delle informazioni in modo elettronico e sicuro, per il controllo dei carichi e delle aree, per l'identificazione e controllo delle persone, per l'attivazione delle misure di emergenza.
È in un tale contesto internazionale che si colloca l'attività di ricerca proposta, il cui obiettivo finale sarà la definizione e l'applicazione di un rigoroso approccio metodologico per la valutazione dei vantaggi ottenibili dall'introduzione di nuove tecnologie a supporto della security nell'ambito del trasporto marittimo, inteso come anello della catena logistica integrata.

3. Approccio metodologico

La prima fase del progetto, a valle di una approfondita analisi bibliografica, rivolta anche ad applicazioni nel campo nucleare e avionico, riguarderà la definizione della metodologia e dei relativi strumenti operativi per la stima dell'impatto di nuove tecnologie sulla security del trasporto marittimo, che ad oggi si ipotizza sarà effettuata mediante un approccio basato sull'analisi del rischio, ossia su tecniche di *Risk analysis* e *Risk assessment*, attraverso i passi procedurali di seguito descritti.

- **Analizzare la struttura organizzativa e individuare le persone e i beni a rischio**
  A valle di un'analisi della struttura organizzativa, sarà necessario individuare tutte le persone considerate a rischio, ossia quelle coinvolte, direttamente o indirettamente, con le operazioni portuali, nonché i possibili beni soggetti ad attacchi, quali container, silos o infrastrutture (incluse quelle di scambio dati e i dati stessi).

- **Specificare gli azzardi che si possono verificare**
  L'identificazione degli azzardi che si possono verificare sarà eseguita sulla base di incidenti o eventi già accaduti, sulla base di eventi verificatisi in luoghi simili oppure sull'eventualità che gli stessi possano accadere per la presenza di un determinato tipo di commercio o per la conformazione geologica del luogo.

- **Stimare la probabilità di occorrenza degli azzardi**
  Contrariamente all'approccio utilizzato nel campo della safety, laddove la probabilità di occorrenza dell'azzardo è spesso legata ai guasti degli impianti tecnologici, nel campo della security tale probabilità dovrà essere opportunamente stimata introducendo i concetti di vulnerabilità e minaccia. Per minaccia si intende la presenza di condizioni che possono influenzare la probabilità che uno specifico attacco sia condotto contro un determinato obiettivo. Tali condizioni possono essere valutate considerando aspetti quali le caratteristiche fisiche e ambientali, il contesto sociale e politico, le procedure e i processi, le capacità offensive della criminalità. L'analisi di vulnerabilità dovrà individuare i punti di debolezza derivanti dalla mancanza di protezioni o da misure di sicurezza non adeguate. In base alle informazioni raccolte sarà quindi assegnato un valore sia al parametro "minaccia" che al parametro "vulnerabilità" e la probabilità di occorrenza dell'azzardo stimata in modo quantitativo o qualitativo.

- **Determinare le conseguenze degli azzardi**
  Per ogni azzardo sarà necessario valutare le possibili conseguenze finali, ossia le perdite in termini economici e di vite umane, considerando gli eventuali contributi derivanti dalle esistenti procedure di mitigazione. In questa valutazione si dovranno considerare sia le perdite dirette sia quelle indirette, ossia tutte le possibili ripercussioni economiche immediate e future.

- **Classificare il rischio**
  La classificazione sarà effettuata sulla base del binomio probabilità di occorrenza/gravità delle conseguenze dei singoli azzardi. Tale classificazione consentirà di individuare tutte le zone laddove risulta mandatorio un intervento per la riduzione del rischio.

- **Formulare eventuali alternative atte a ridurre il rischio**
  Le misure che potranno essere prese in considerazione includeranno nuove infrastrutture e sistemi, così come nuove procedure. A valle della formulazione, sarà necessario effettuare uno studio di fattibilità e un'analisi costi/benefici delle contromisure ideate, onde verificarne l'effettiva realizzabilità e la compatibilità con le attività commerciali, al fine di trovare un equilibrio tra security del sistema ed esigenze operative della catena logistica.

4. L'impatto delle tecnologie

Nella seconda fase del progetto saranno identificate e analizzate le tecnologie utilizzabili nell'ambito del trasporto marittimo ai fini della security e il loro impatto valutato mediante la metodologia individuata nella prima fase. Tale metodologia sarà applicata dapprima ipotizzando differenti possibili scenari operativi (onde verificarne le caratteristiche *general purpose*) e quindi a un *case study* reale (al fine di validarne l'effettiva applicabilità sul campo). Nel seguito vengono fornite a titolo di esempio alcune indicazioni di carattere generale sui sistemi di ausilio all'implementazione e gestione della security che saranno, in tutto o in parte, oggetto dell'analisi.

Protezione perimetrale
Dovrà essere affidata a sistemi di anti-intrusione che permettano di segnalare tentativi di scavalcamento delle recinzioni, sollevamento delle stesse o accesso indebito. Tra le principali tecnologie disponibili si ricordano i sensori con struttura autoportante (sistemi a barriera ad infrarossi o a microonde), i sensori associati alle recinzioni **(**cavo microfonico, cavi in fibra ottica, sistemi a filo sensibile) e i sensori interrati **(**sistemi a misura di pressione con circuito idraulico, rilevatori di dispersione elettromagnetica).

Illuminazione
Tutte le aree individuate come critiche dal punto di vista della security dovranno essere sufficientemente illuminate tramite l'installazione di torri faro, con monitoraggio dello stato operativo effettuato da un sistema

di controllo centralizzato. Le torri faro dovranno essere opportunamente dimensionate sia come potere illuminante sia come disponibilità del servizio (tramite opportune ridondanze).

Videosorveglianza

L'impianto di videosorveglianza dovrà consentire di visionare nella sala operativa le immagini riprese da telecamere opportunamente ubicate, permettendo di svolgere il monitoraggio in tempo reale delle aree sorvegliate e la registrazione automatica delle immagini per un intervallo di tempo prefissato. Il sistema DVS (videosorveglianza digitale) rappresenta l'attuale stato dell'arte dei sistemi di video sorveglianza: esso combina le principali caratteristiche dei tradizionali sistemi televisivi a circuito chiuso (TVCC) con le ultime tecnologie per la video registrazione digitale (DVR).

Rete di comunicazione

Per effettuare un controllo centralizzato delle informazioni relative alla security e per poter implementare dei servizi efficaci ed efficienti di scambio informativo tra i vari enti presenti all'interno dell'ambito portuale sarà necessaria la realizzazione di una rete di comunicazione, scomponibile in livello fisico (costituito dai collegamenti fisici tra gli elementi che devono comunicare tra loro), livello di trasporto (costituito dal protocollo di comunicazione che tramite il livello fisico veicola le informazioni tra le applicazioni), livello di applicazione (costituito da tutte le applicazioni che tramite il livello di trasporto si appoggiano alla rete per comunicare e scambiare informazioni). La scelta di quale tecnologia implementare ai vari livelli dovrà essere effettuata valutando unitamente agli aspetti di sicurezza intrinseca anche ulteriori criticità, quali quelle legate all'implementazione, manutenibilità, scalabilità e prestazioni del sistema.

Controllo accessi

Per ogni varco di ingresso all'ambito portuale e per ogni zona interna caratterizzata da particolari restrizioni, si dovranno implementare sistemi di controllo degli accessi per il riconoscimento dei mezzi e delle persone che accedono alle aree interessate.
Ad oggi molti terminal nel mondo impiegano sistemi per il riconoscimento ottico dei codici identificativi dei container o delle targhe degli automezzi che li trasportano: la maggior parte dei porti del Nord America sono dotati oggi di OCR (Optical Character Recognition), che consentono di effettuare le operazioni di controllo con elevata affidabilità, ma l'attuale tecnologia rende oggi disponibili sistemi "multi-aspect", ovvero con più videocamere che aumentano le prestazioni del sistema OCR garantendo la visione dell'oggetto in esame da diverse angolazioni. In condizioni di elevata vulnerabilità, i dispositivi per il controllo degli accessi basati sull'identificazione del container trasportato potranno essere integrati da sistemi per il riconoscimento delle persone autorizzate all'ingresso nei terminal, quali ad esempio i sistemi biometrici (controllo delle impronte digitali, riconoscimento delle caratteristiche facciali, scansione dell'iride, controllo dell'impronta della mano).

Controllo Merci

Il problema dell'individuazione di materiale potenzialmente pericoloso (ordigni esplosivi, materiale tossico, materiale radioattivo) potrebbe essere risolto con un capillare servizio di ispezione dei container e della merce in transito, ma ciò provocherebbe un rallentamento inaccettabile nelle operazioni portuali. Ne consegue quindi che il controllo dovrebbe avvalersi di dispositivi tecnologici (scanner e contatori geiger) e di una logistica in grado di effettuare un'analisi del contenuto dei container e della merce in transito in tempi ragionevolmente brevi. I veicoli o i container da sottoporre a scansione o a procedura di rilevamento radiazioni dovranno essere in questo caso selezionati sulla base della valutazione del rischio e della merce trasportata.

5. Evoluzione temporale delle attività

	Anno 1												Anno 2											
Attività	**1**	**2**	**3**	**4**	**5**	**6**	**7**	**8**	**9**	**10**	**11**	**12**	**1**	**2**	**3**	**4**	**5**	**6**	**7**	**8**	**9**	**10**	**11**	**12**
State of the art																								
Procedura di analisi del rischio																								
Definizione delle tecnologie																								
Definizione degli scenari																								
Risk analysis “as is”																								
Impatto azioni mitigatrici																								
Cost-benefit analysis																								
Case study reale																								
Risk analysis “as is”																								
Impatto azioni mitigatrici																								
Cost-benefit analysis																								