La security nei sistemi di trasporto a guida vincolata: analisi del rischio e strategie di protezione

Autori: F. Flammini[12], A. Gaglione[12], N. Mazzino[1], N. Mazzocca[2], C. Pragliola[1]

[1]Ansaldo STS Italia, Divisione Nuove Iniziative
Via Nuova delle Brecce, n. 260 Napoli, Italia
{flammini.francesco,mazzino.nadia,pragliola.concetta}@asf.ansaldo.it

[2]Università Federico II di Napoli, Dipartimento di Informatica e Sistemistica
Via Claudio, n. 21 Napoli, Italia
{andrea.gaglione,nicola.mazzocca}@unina.it

Sommario

I recenti attentati terroristici ai danni di sistemi ferroviari e metropolitani (Madrid 2004, 191 morti e 2057 feriti; Londra 2005, 52 morti e 700 feriti) hanno messo in luce l'estrema appetibilità e vulnerabilità di tali infrastrutture, dovute essenzialmente all'elevata frequentazione e alle limitate protezioni esistenti. Pertanto, la quasi totalità dei paesi occidentali, in particolare quelli considerati più a rischio per motivi politici, si sono movimentati per incrementare il livello di sicurezza delle infrastrutture di trasporto su ferro. Al fine di perseguire tale obiettivo, è necessario pianificare tutta una serie di attività volte ad una adeguata valutazione e gestione del rischio. In questo lavoro verrà presentata una panoramica di tali attività con riferimento all'esperienza di Ansaldo STS, che ruota attorno ad un sistema integrato di gestione della security e che si avvale di molti spunti innovativi derivanti dal contributo della ricerca accademica.

1. INTRODUZIONE

Nell'ambito del programma internazionale di protezione delle infrastrutture critiche, i sistemi di trasporto a guida vincolata rivestono un'importanza notevole, sia per le vulnerabilità intrinseche che per l'impatto di eventuali attentati, ed ancora per le dipendenze che per loro natura introducono tra le altre infrastrutture. Un sistema di trasporto è per definizione "qualcosa che mette in collegamento" altri sistemi (si pensi a tutti i casi di approvvigionamento di risorse materiali). D'altra parte, è nota la stretta dipendenza da altri sistemi quali quello elettrico e quello di telecomunicazione, quest'ultima rafforzata dai moderni sistemi di radio-segnalamento.
Per i sistemi di trasporto a guida vincolata, così come per tutte le altre infrastrutture critiche, è necessario adottare approcci sistematici, rigorosi e ben strutturati al fine di modellare fenomeni per loro natura complessi ed eterogenei. La valutazione dell'occorrenza di malfunzionamenti di origine naturale o dolosa, insieme alla stima dell'impatto di tali eventi, deve guidare la scelta ed il dimensionamento dei meccanismi di protezione. Modellare fenomeni di siffatta natura richiede spesso di prendere a prestito modelli mutuati da altre discipline, incluse quelle socio-economiche.
A titolo di esempio, si riporta in Figura 1 uno schema a blocchi dell'infrastruttura ferroviaria utilizzato per l'analisi delle interdipendenze con le altre infrastrutture, in cui si è ipotizzato che il sistema di controllo e segnalamento sia conforme allo standard Unisig ERTMS/ETCS[1] di livello 2 (utilizzato sulle nuove linee ad Alta Velocità).
In questa sede, l'enfasi maggiore sarà data all'analisi del rischio e ai meccanismi di protezione relativamente a minacce di tipo doloso, senza approfondire le interdipendenze e gli effetti a catena che possono propagarsi a livello del sistema nazione.

[1] European Railway Traffic Management System / European Train Control System.

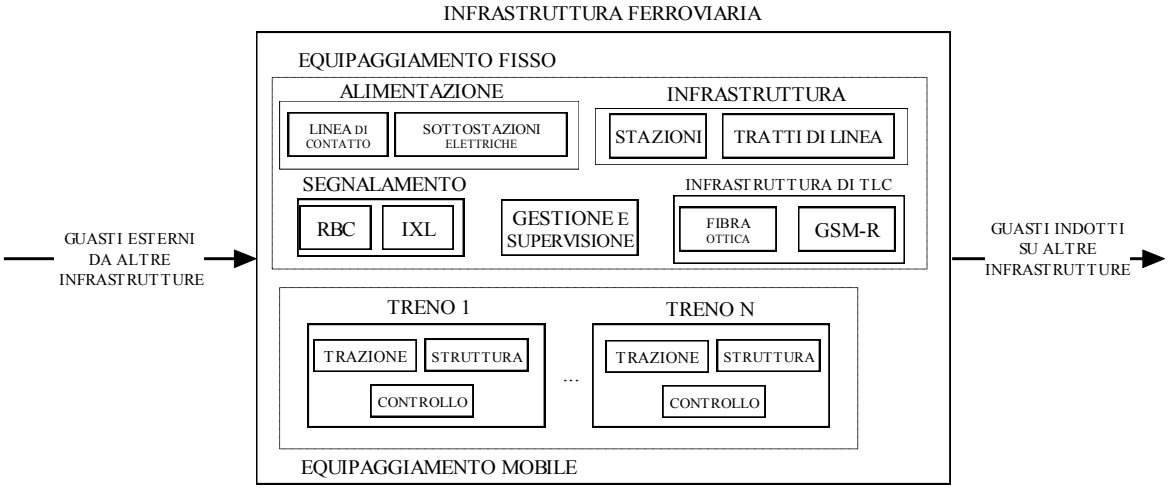

Figura 1. Schema a blocchi dell'infrastruttura ferroviaria.

2. L'ANALISI DEL RISCHIO

Per comodità di trattazione, divideremo l'analisi del rischio due grandi sottoattività: valutazione del rischio e gestione del rischio.

2.1 Valutazione del rischio

La valutazione del rischio[2] (*Risk Assessment*) ha l'obiettivo di definire le vulnerabilità dell'infrastruttura. Tale attività, da eseguire in maniera sistematica ricorrendo ad opportune metodologie, può fornire risultati di tipo sia qualitativo che quantitativi. Risultati quantitativi consentono una gestione più oculata del rischio, permettendo di valutare in maniera rigorosa l'impatto delle contromisure che si andranno ad adottare sugli indici di rischio. Ad esempio, in Italia, nell'ambito gruppo di lavoro congiunto Finmeccanica - NITEL[3] - RFI e relativamente al caso di studio Alta Velocità Roma-Napoli, si sta sviluppando una metodologia quantitativa di analisi del rischio che possa rispondere a tali requisiti di rigore e sistematicità.

Una qualsiasi metodologia di analisi del rischio per sistemi critici deve avere come dati di input: le specifiche di interesse del sistema oggetto di analisi, al fine di conoscerne in dettaglio scelte progettuali e caratteristiche strutturali; una base di dati storici relativi alle minacce a cui è stato sottoposto in passato lo stesso sistema o sistemi analoghi; informazioni derivanti dai sopralluoghi sul campo, in merito ad esempio alla morfologia del territorio circostante; il giudizio e la previsione di esperti in merito a tutti gli aspetti non direttamente quantificabili [1]. L'output consisterà in uno o più indici di rischio espressi tipicamente in €/anno, eventualmente prodotti in maniera automatica da opportuni strumenti informatici di supporto al metodo.

Nell'analisi del rischio è possibile ragionare da diversi punti di vista. Ad esempio, si può procedere in maniera top-down, partendo dagli eventi indesiderati a livello di sistema fino a giungere alle cause di origine doloso (danneggiamenti ai singoli asset[4]), oppure bottom-up, partendo cioè dalle minacce e valutando la propagazione delle conseguenze. Entrambi gli approcci presentano delle marcate analogie con le valutazioni di safety, basti citare la FMEA (*Failure Mode & Effect Analysis*, tipico approccio bottom-up) o la FTA (*Fault Tree Analysis*, tipico approccio top-down). La sostanziale differenza è che in ambito di security mancano metodologie standard, anche solo de facto. La modalità che sembra fornire una maggiore semplicità di analisi è quella legata all'elencazione delle modalità di attacco (i cosiddetti "scenari"), a cui può essere associato uno specifico indice di rischio, previa stima di relative probabilità di accadimento, vulnerabilità e conseguenze previste, anche attraverso modelli formali (es. reti bayesiane).

2.2 La gestione del rischio ed i meccanismi di protezione

Una volta individuate le criticità dell'infrastruttura sotto analisi, si deve procedere alla ricerca delle contromisure, che coincidono nella maggior parte dei casi in opportuni meccanismi di protezione passivi (es. irrobustimento di barriere nei varchi di accesso) o attivi (es. sistemi anti-intrusione perimetrali) [2]. La

[2] L'espressione matematica comunemente accettata è la seguente: RISCHIO = PROBABILITÀ DI ATTACCO * VULNERABILITÀ * DANNO, in cui la Vulnerabilità è definita come la probabilità di successo di un attacco, mentre il danno rappresenta una valutazione di carattere economico delle conseguenze dell'attacco.

[3] Consorzio interuniversitario per i trasporti e la logistica.

[4] La parola "asset" si riferisce ad un qualsiasi bene da proteggere, pertanto dotato di valore (diretto o indiretto).

selezione dei meccanismi di protezione segue essenzialmente due logiche: una funzionale, legata alla tipologia di eventi da cui è necessario proteggersi (intrusioni, aggressioni, graffitaggio, introduzione materiale esplosivo o radioattivo, ecc.); una economica, legata ai vantaggi per chi gestisce l'infrastruttura derivanti dall'adozione del meccanismo di protezione. Una terza logica può coincidere con vincoli di tipo legislativo o normativo, che possono imporre così come limitare (es. per motivi legati alla privacy) l'adozione di determinati tipi di contromisure (oltre che l'evidenza formale della conseguente e associata riduzione del rischio). E' bene sottolineare che per i meccanismi di protezione spesso all'effetto di riduzione della vulnerabilità si accompagnano anche effetti di tipo deterrente (riduzione tasso di accadimento degli attacchi) e razionalizzante (migliore gestione delle procedure di intervento grazie ad un monitoraggio più preciso della situazione).
A titolo di esempio, un moderno sistema di security impiegato in ambito metropolitano è costituito dai seguenti sottosistemi componenti:

- Anti-intrusione, costituito dalla sensoristica di rilevazione di effrazioni perimetrali (es. contatti magnetici, barriere a infrarosso, cavi microfonici) e volumetriche (es. rilevatori a microonde, infrarossi, ultrasuoni);
- Controllo accessi, che comprende l'insieme dei dispositivi (tipicamente tastierini numerici, lettori di prossimità di badge magnetici e RFID[5]) utilizzati per l'identificazione delle persone aventi diritto ad accedere all'interno dell'infrastruttura (es. locali tecnici);
- Sensoristica NBCR (Nucleare Batteriologico Chimico Radiologico), specializzata per il rilevamento di sostanze nocive immesse nel sistema, e di altri tipi (antincendio, rilevatori di esplosivo, vibrazioni, ecc.);
- Videosorveglianza intelligente, evoluzione del tradizionale sistema TVCC[6], arricchito con la videroregistrazione digitale e la rilevazione automatica di eventi anomali e potenzialmente malevoli (es. attraversamento perimetro critico, bagaglio abbandonato, ecc.) basata su algoritmi di visione artificiale;
- Rete di interconnessione ed integrazione dei diversi sottosistemi, per loro natura distribuiti ed eterogenei, tipicamente convergente in uno o più posti di controllo (periferici e/o centrali);
- Software di gestione della security (SMS, *Security Management Software*), che consente il monitoraggio ed il controllo da parte degli operatori dell'intero sistema di security, nonché il coordinamento delle procedure di emergenza.

In particolare, il SMS riveste un ruolo fondamentale nel sistema di security in quanto è il principale responsabile dell'integrazione funzionale dei diversi sottosistemi, fornendo all'utente gli strumenti per interagire con il sistema tramite un'interfaccia il più possibile coerente e user-friendly. Inoltre, esso consente una gestione e correlazione ad alto livello degli allarmi, con la possibilità di una calibrazione della probabilità di rilevamento e tasso di falsi allarmi. Ad esempio, nel caso degli imbocchi delle galleria, la combinazione degli allarmi rilevati da più barriere ad infrarossi poste ad altezze differenti con quelli provenienti da videocamere intelligenti consente di discriminare le intrusioni in galleria dai normali passaggi dei treni (vedi Figura 2).

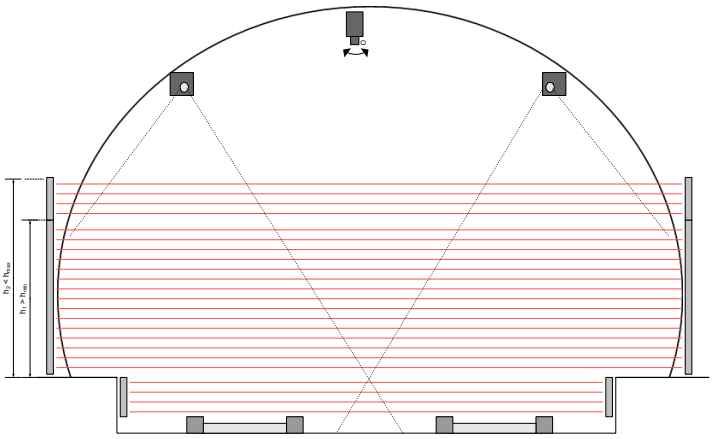

Figura 2. Sistema di protezione degli imbocchi dei tunnel.

[5] *Radio Frequency IDentifier*.
[6] TeleVisione a Circuito Chiuso.

3. SISTEMI INTEGRATI DI GESTIONE DELLA SECURITY

3.1 L'esperienza Ansaldo STS

Ansaldo STS è impegnata su diversi progetti relativi a impianti e tecnologie di security per linee ferroviarie e metropolitane. L'attività più rilevante nell'ambito security è probabilmente quella legata allo sviluppo di un software SMS proprietario AnsaldoSTS. Tale attività si avvale del supporto di consulenti dotati di elevato know-how ed esperienza nel settore della security di infrastrutture critiche. Il software ha come caratteristiche fondamentali quelle di:

- possibilità di organizzazione gerarchica dei posti di controllo e dei relativi privilegi utente;
- monitoraggio e controllo integrato di tutti i sottosistemi di security (anti-intrusione, videosorveglianza, diffusione sonora, radio-telefonia, ecc.);
- facilità d'uso, scalabilità e adattabilità a contesti diversi (interfaccia web multipiattaforma in grado di girare anche su dispositivi mobili, es. palmari);
- correlazione degli eventi a diversi livelli;
- possibilità di reporting avanzato, procedure di emergenza assistite e automazione delle contromisure.

L'architettura del sistema hardware e software nel caso metropolitano è riportata nella Figura (in cui HMI sta per *Human Machine Interface*, ovvero interfaccia uomo-macchina), mentre nella Figura è presentata un'anteprima dell'interfaccia utente (ancora in fase di sviluppo).

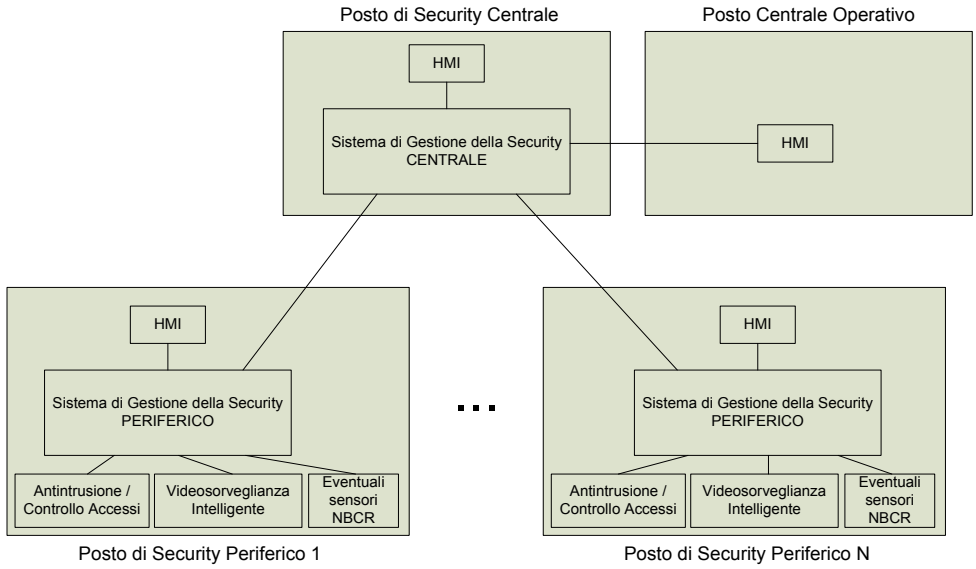

Figura 3. Architettura gerarchica del sistema di gestione della security nel caso metropolitano.

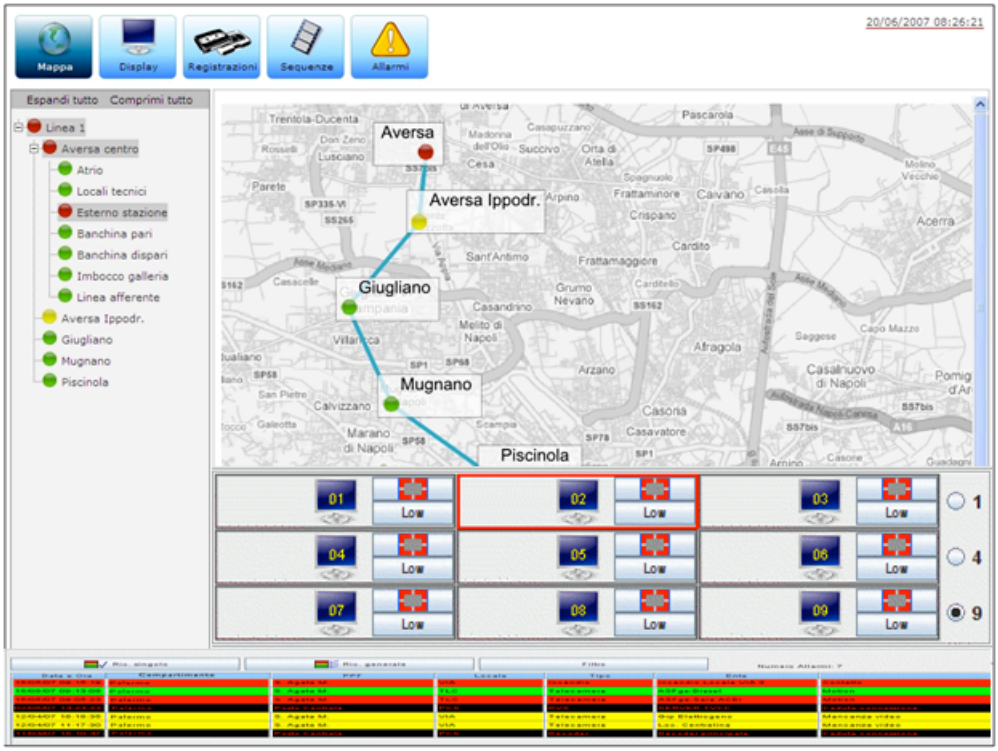

Figura 4. Anteprima dell'interfaccia utente.

3.2 Attività di ricerca

La divisione Nuove Iniziative di Ansaldo STS sta portando avanti diverse attività e progetti di ricerca in collaborazione con istituti universitari e altre aziende Finmeccanica. Di queste attività si elencano e descrivono brevemente nel seguito le più significative:

- Analisi comparativa delle prestazioni dei sistemi di videosorveglianza intelligente (stima parametri POD e FAR[7]) e dello stato dell'arte della sensoristica antintrusione e NBCR;
- Sviluppo di un'applicazione di supporto all'analisi quantitativa del rischio (Q-RA, *Quantitative Risk Analysis*);
- Modellazione delle interdipendenze tra infrastrutture critiche, con il contributo dato nell'ambito del progetto CISIA (in collaborazione con SELEX Sistemi Integrati, Università di Roma Tre e Campus Biomedico di Roma) e l'applicazione del framework multiformalismo OsMoSys (in collaborazione con l'Università di Napoli Federico II);
- Sistemi di rilevazione e acquisizione misure lungo linea;
- Progetto di ricerca europeo SAFER (Sicurezza Attiva dei sistemi di trasporto su FERro), che coinvolge numerose aziende appartenenti al gruppo Finmecccanica;
- Interconnessione ed integrazione di sorgenti di dati eterogenee tramite *Wireless Sensor Networks* [3];
- Sviluppo di un framework per il rilevamento automatico di scenari di attacco ad infrastrutture critiche attraverso l'analisi di correlazione di eventi elementari provenienti da sorgenti eterogenee (DETECT, *DEcision Triggering Event Composer & Tracker*), in collaborazione con il Dipartimento di Informatica e Sistemistica dell'Università di Napoli "Federico II".

6. CONCLUSIONI

E' ben noto agli addetti ai lavori che la protezione delle infrastrutture critiche rappresenta una problematica che travalica i domini delle singole discipline scientifiche e coinvolge numerose tecnologie. La recente esperienza di Ansaldo STS nel settore ferroviario e metropolitano testimonia questa visione, avendo potuto toccare svariati settori di ricerca, che vanno dai metodi formali all'intelligenza artificiale. Ciò richiede uno sforzo notevole nell'integrazione delle conoscenze e abilità richieste. Questo sforzo non può che essere imperniato sulla collaborazione con i centri di ricerca accademici che detengono lo stato dell'arte della conoscenza nei diversi settori applicativi e possono contribuire all'affinamento degli approcci metodologici.

[7] POD: *Probability Of Detection*; FAR: *False Alarm Rate*.

In questo lavoro, è stato presentato un rapido excursus dei progetti legati al settore della security dei sistemi di trasporto e guida vincolata, evidenziando il ruolo e l'importanza del contributo innovativo della ricerca in quest'ambito.

Ringraziamenti
Gli autori ringraziano il Prof. Roberto Setola per l'interesse manifestato nei confronti delle iniziative del gruppo di lavoro congiunto Ansaldo STS e Università di Napoli Federico II. Un ringraziamento particolare è diretto al responsabile della divisione Nuove Iniziative di Ansaldo STS, Ing. Giovanni Bocchetti, e a tutti i colleghi che collaborano alle attività menzionate, tra cui è doveroso citare Giuseppe Gotelli, Giuseppe Musella e Annarita Tedesco.

Bibliografia

[1] Ted G. Lewis: *Critical Infrastructure Protection in Homeland Security: Defending a Networked Nation*. John Wiley, New York, 2006.

[2] Mary Lynn Garcia: *The Design and Evaluation of Physical Protection Systems*. Butterworth-Heinemann, USA, 2001.

[3] F. L. Lewis: Wireless Sensor Networks. In *Smart Environments: Technologies, Protocols, and Applications*, ed. D.J. Cook and S.K. Das. John Wiley, New York, 2004.