RAILWAY INFRASTRUCTURE SECURITY

Prof. Roberto Setola

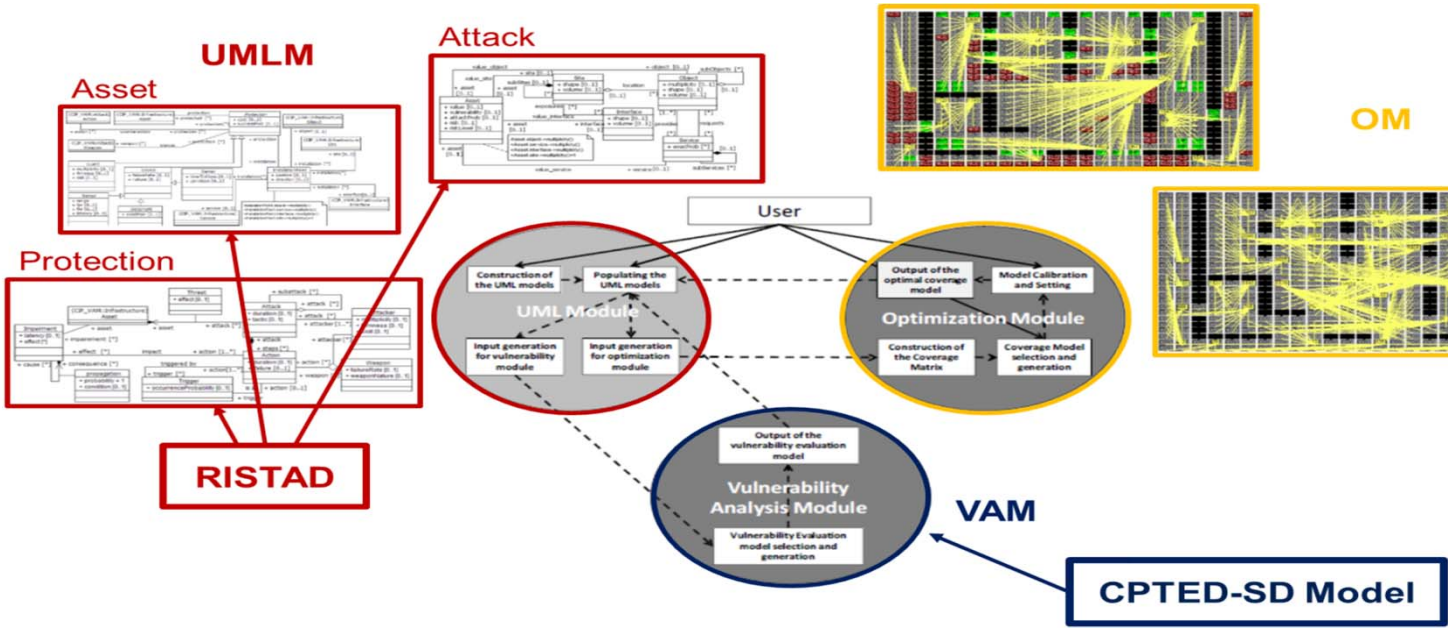
4th June 2015

Università Campus Bio-Medico di Roma - Via Álvaro del Portillo, 21 - 00128 Roma – Italia
www.unicampus.it

UNIVERSITA' CAMPUS BIO-MEDICO DI ROMA

METRIP

MEthodological Tools for Railway Infrastructure Protection



"Prevention, Preparedness and Consequence Management of Terrorism and other Security-related Risks Programme"
European Commission - Directorate-General Home Affairs

Objectives

MeTRIP project main objective is to improve the planning of security protection in railway transportation systems developing methodologies, strategies and best practices for the **quantitative evaluation** of the criticalities in Railway Infrastructures

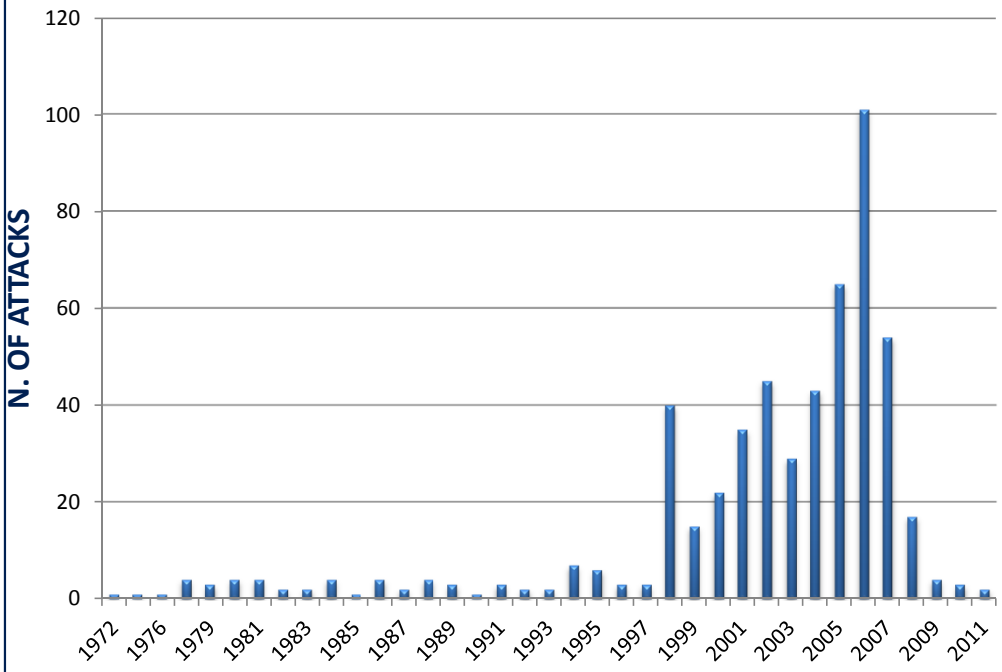
UML MODELS

BAYESIAN NETWORKS

OPTIMIZATION MODELS

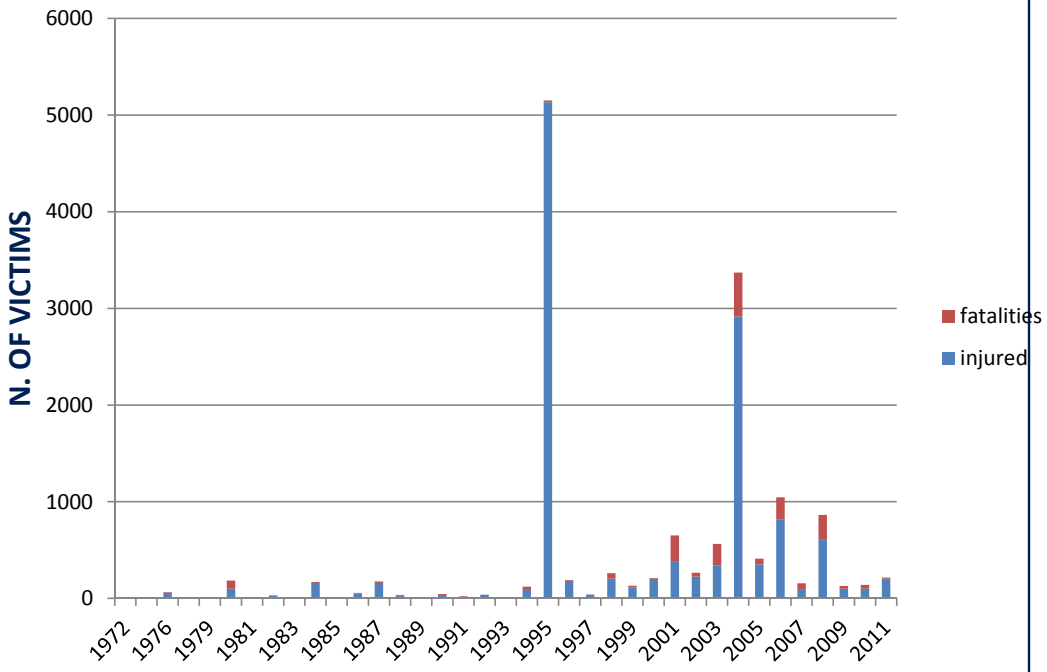
ATTACKS TIME EVOLUTION

OF ATTACKS/YEAR



- # of attacks: 541 from 1972 to 2011
- increased in ’70s, accelerated in ’90s, peaked in 2006

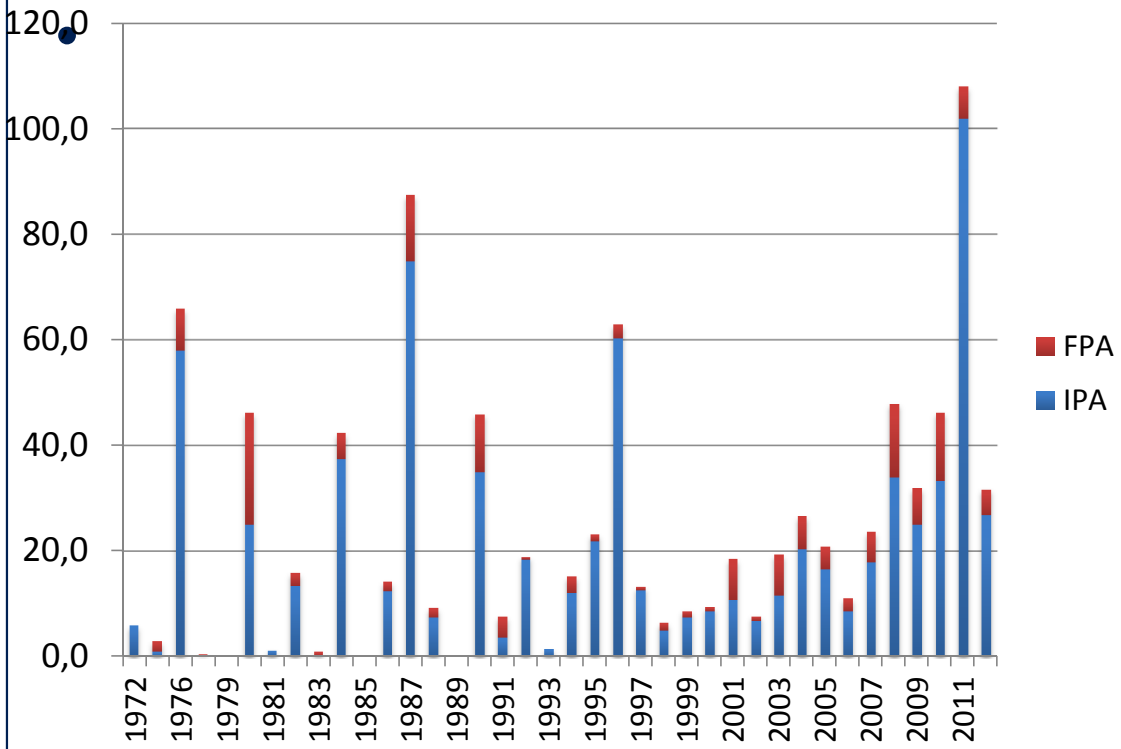
OF VICTIMS/YEAR



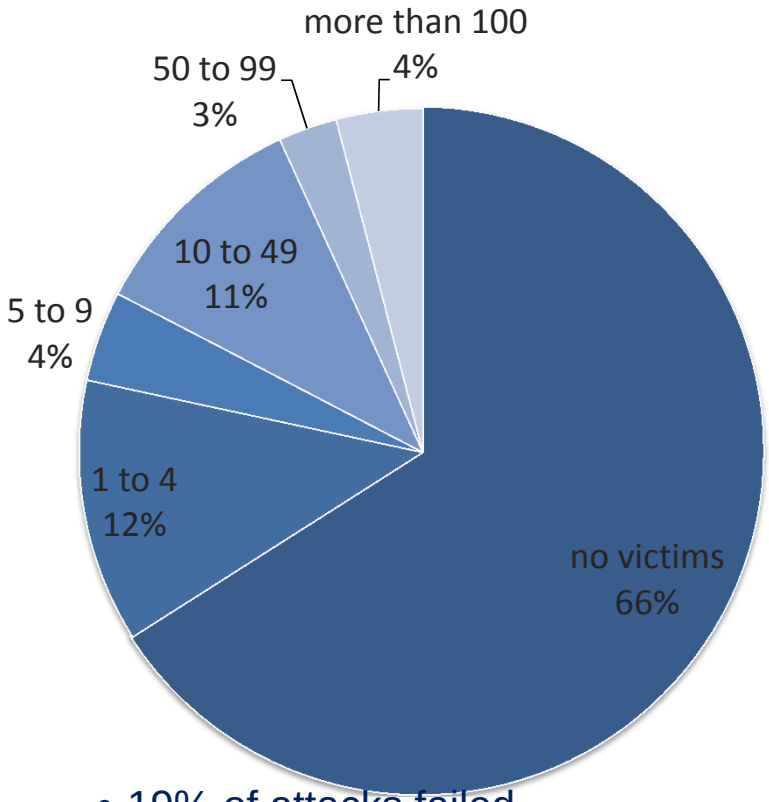
- # of victims increased in last decade
- peaks in ’95 and 2004 due to Tokyo and Madrid attacks

ATTACKS TIME EVOLUTION

LETHALITY DISTRIBUTION/YEAR

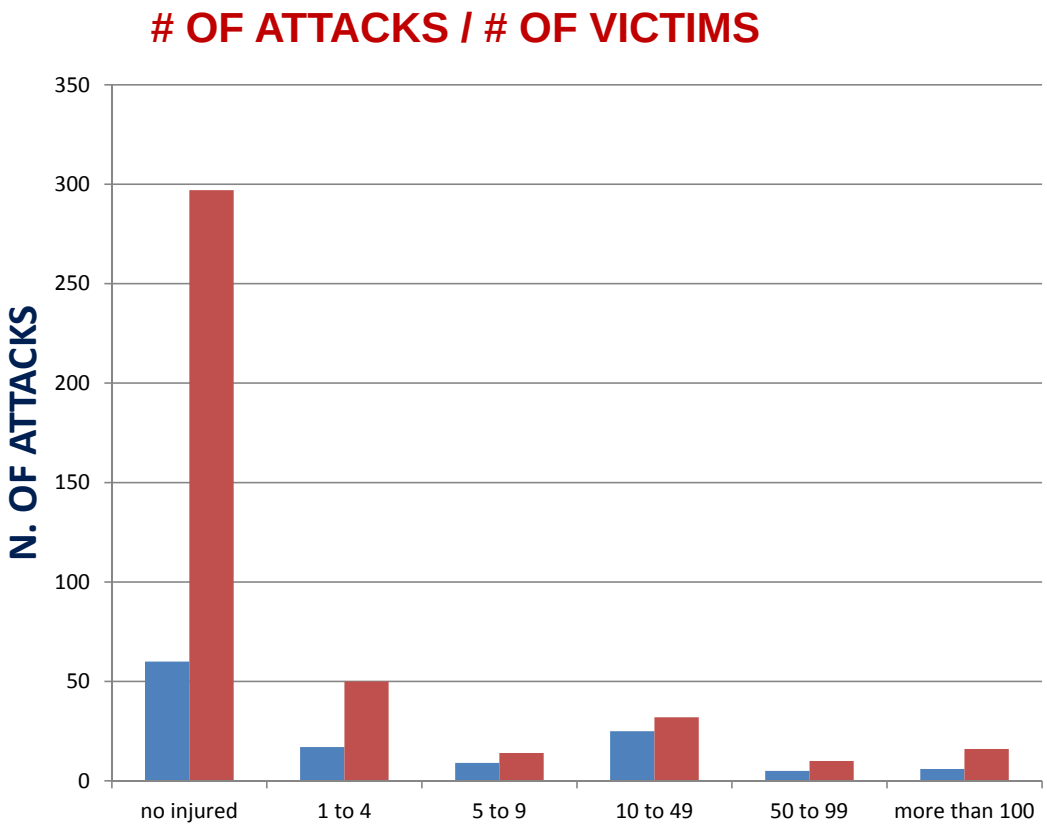


- 1972-1999: FPA < 5 (excepted for ’80, ’87, ‘90) AVG(FPA) = 3.3
- from 2000: FPA > 6, AVG(FPA) = 6.7



- 19% of attacks failed
- 438 attacks perpetrated

ATTACKS TIME EVOLUTION



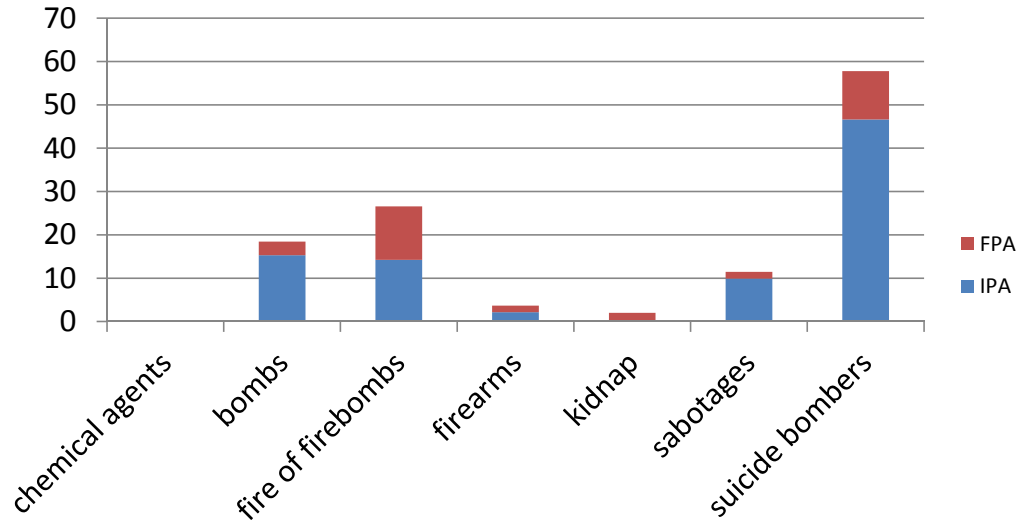
After 2000:

- attacks are more "efficient"
- # of attacks > than those registered in '72-'99
  - 4 times > in "1 to 4" victim/s;
  - 2 times > in "more than 100" victims

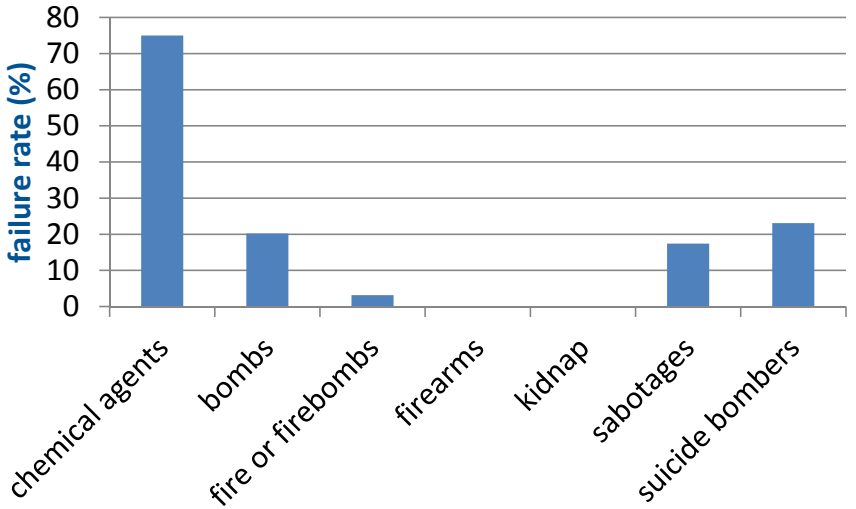
Madrid ('04), London ('05) and Mumbai ('08) attacks (more than 50 deaths) are "success" to replicate

Attacks' distribution by method/technique

Lethality by weapons/methods



Failure rate%



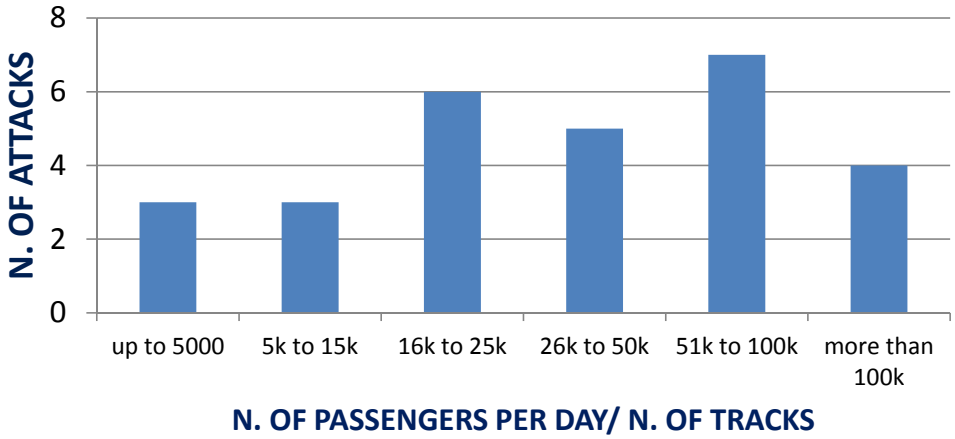
Without considering Tokio assault:

- Suicide bomber is the bloodiest method (FPA=11, IPA=47)
- Fire or firebombs (FPA=12, IPA=14), bombs (FPA=3, IPA=15)

- Chemical agents are doomed to fail (75%)
- Firearms & fire or firebombs (3%) the most reliable

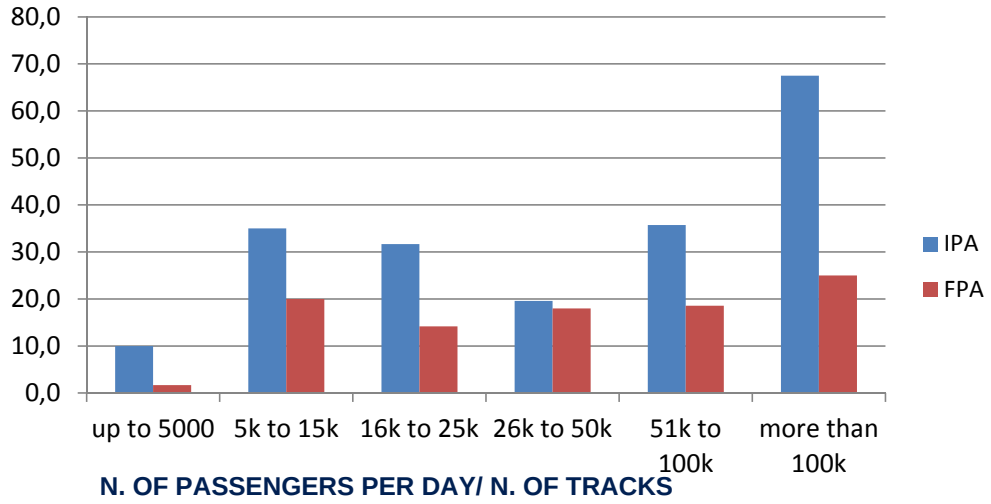
DATA ANALISYS ABOUT STATIONS

 # OF ATTACKS BY # OF DAILY PASS./# OF TRACKS



- # of attacks increases with the ratio, reaching a peak in “51k and 100k”

LETHALITY BY # OF DAILY PASS./# OF TRACKS

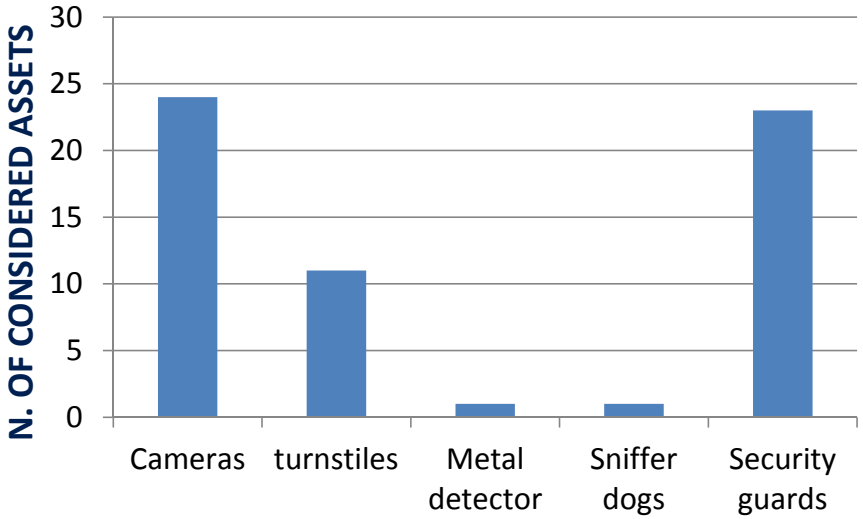


- The # of victims (injured or fatalities) increases with the ratio (in “more than 100k” FPA = 25)

WELL-FREQUENTED STATIONS ARE THE MOST “SUITABLE” TARGET

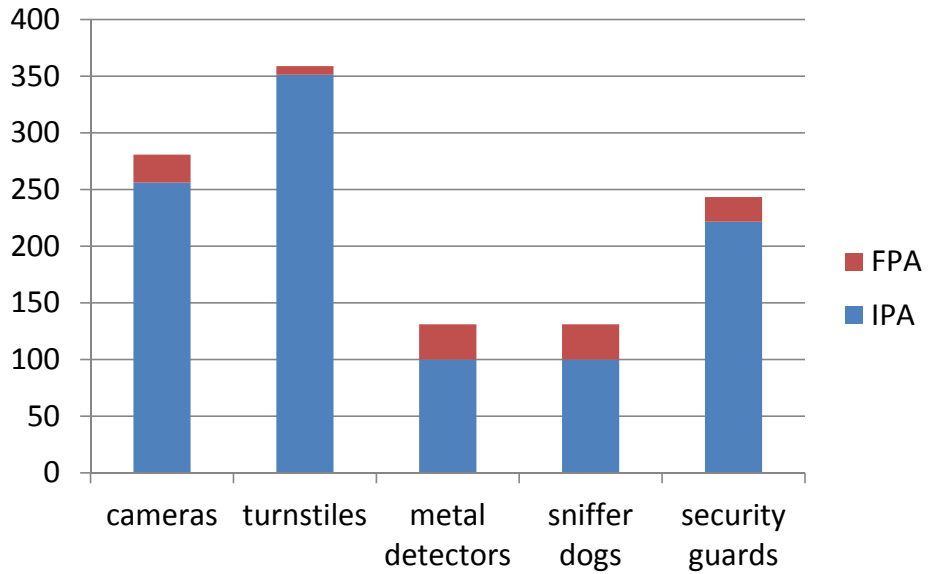
DATA ANALISYS PROTECTION SYSTEMS

PROTECTION SYSTEMS



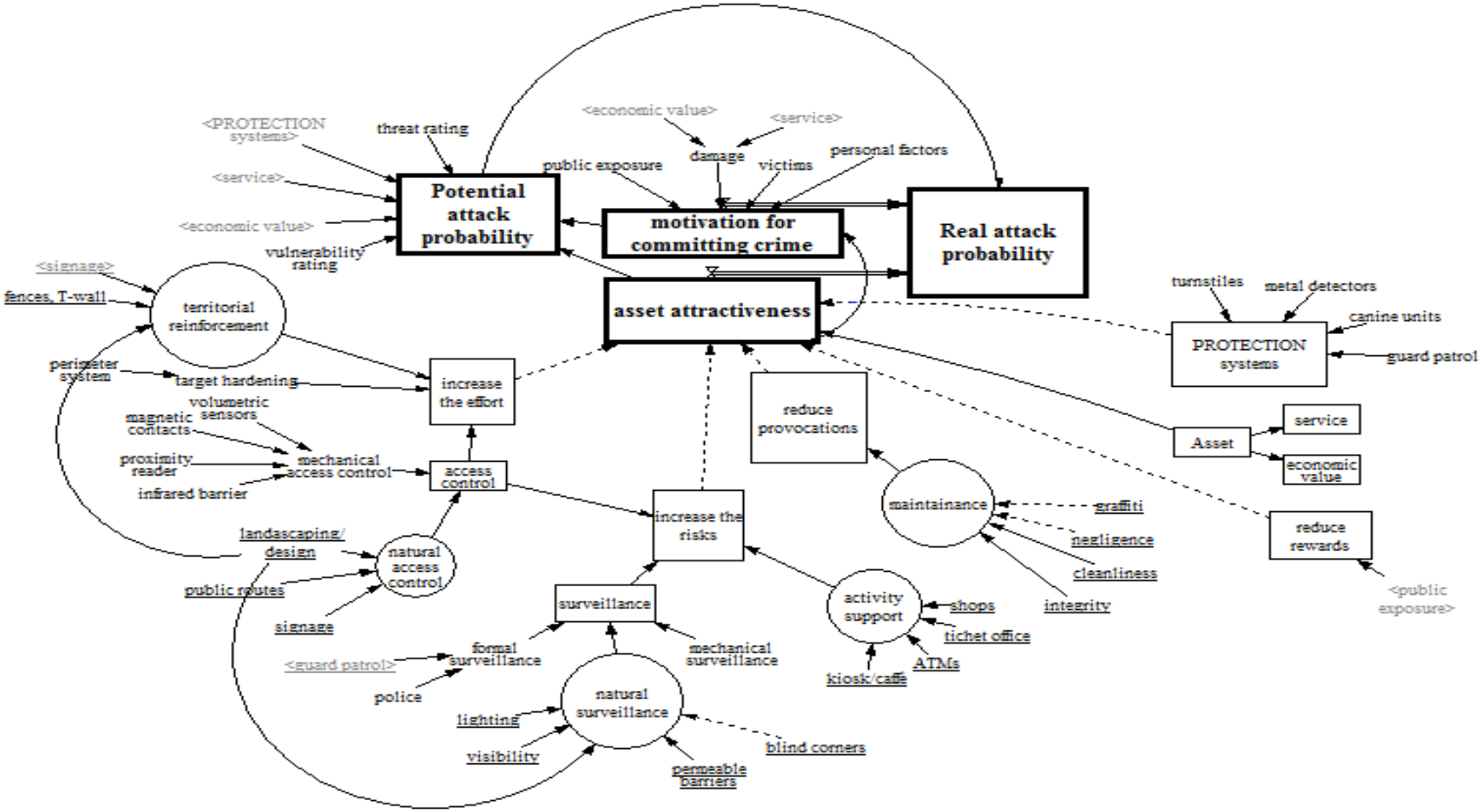
- Cameras the most used, followed by security guards and turnstiles
- Only one asset (Connaught place station in New Delhi) uses metal detector and canine units

LETHALITY BY PROTECTION SYSTEMS

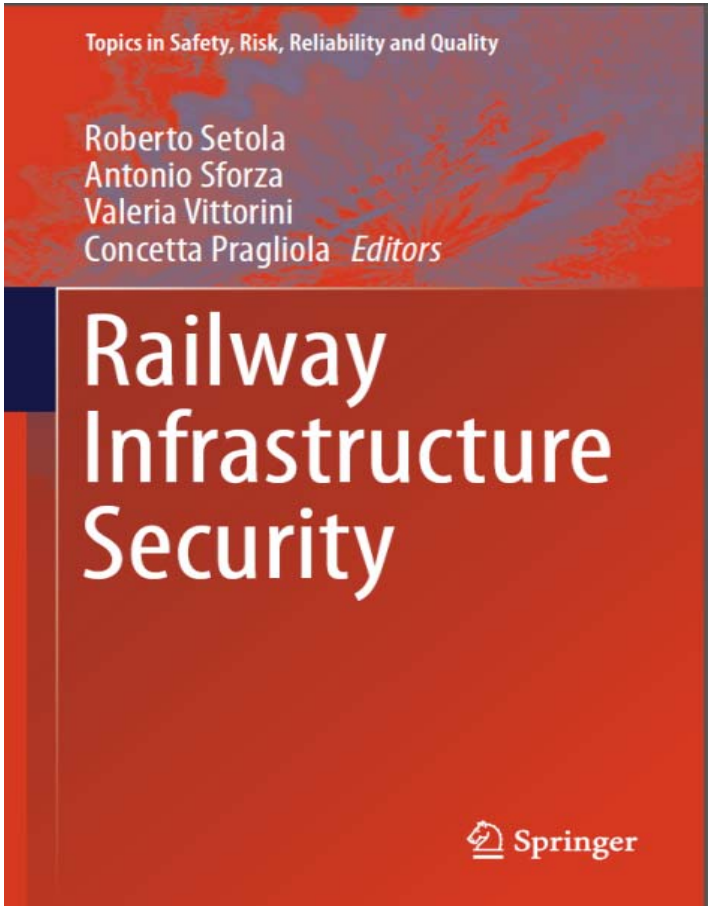


- The most effective to prevent fatalities are (or seem) turnstiles and security guards (not enough data available)

The CPTED-SD model



Railway Infrastructure Security



«Railway Infrastructure Security»: the authors

Dr. Jacques Colliard Head of Security Division of the *International Union of Railways (UIC)*

Dr. Franco Fiumara Head of security Directorate of *Ferrovie dello Stato Italiane*

Eng. Francesco Murolo, consultant of *EAV* and **Eng. Arturo Borrelli** Vehicle Director in *EAV*

Chanan Graf of *Gteam Security Ltd*, leading Israeli consultant in mass transit and railway security

Dr. Klaus Hestbek Lund by *Metroseskabet (DK)*

«Railway Infrastructure Security»
The authors:

Università Campus Biomedico of Rome Team

Ansaldo STS Security Team

DIETI Research Group

The Kent Business School University

The book addresss the issue of increasing critical infrastructure protection in transportation systems.

To reach this aim it is necessary to put together experiences coming from different fields and build a methodology for a quantitative measurement of the criticality of the RIS assets, the definition of a strict intervention strategy and the choice of type, technologies and locations of the protection systems.

This book could be a starting point for the definition of several guidelines for shared security requirements for RIS at European level.

All-hazard : naturally occurring event, human induced events (both intentional and non-intentional) and technology caused events with potential impact on organization, community or society and environment on which it depends

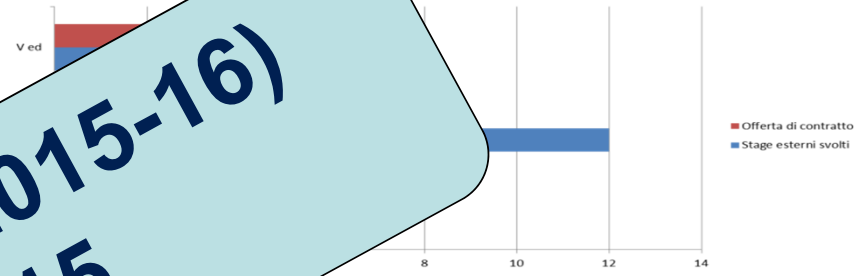
Master in Homeland Security

Master in Homeland Security – Consiglio Scientifico

Comitato Scientifico

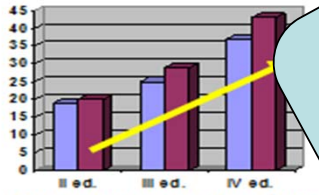
- Dott. Gianluca Ansalone (Esperto di strategia e intelligence)
- Dott. Antonio Apruzzese (Direttore Polizia Postale)
- Dott. Raoul Chiesa (Security Brokers)
- Ing. Luigi D'Angelo (Relazioni Internazionali Protezione Civile)
- Dott. Dario De Marchi (Media Relations di Acquirente Unico SpA)
- Col. Michele Dell'Agli (Guardia di Finanza)
- Dott. Francesco di Maio (Responsabile Security ENAV)
- Ing. Alfonso Farina (Selex Sistemi Integrati)
- Dott. Franco Fiumara (Responsabile Protezione Aziendale FSI)
- Prof. Giorgio Franceschetti (Università Napoli Federico II)
- Prof. Luigi Glielmo (Università Sannio)
- Dott. Stefano Grassi (Responsabile Sicurezza Poste Italiane)
- Dott. Francesco Lambiase (BCManager)
- Dott. Giuseppe Lasco (Direttore Sicurezza Aziendale Terna)
- Col. Iacopo Mannucci Benincasa (Carabinieri)
- Prof. Stefano Panzieri (Università Roma Tre)
- Ing. Concetta Pragliola (Ansaldo STS)
- Dott. Giorgio Riondino (Esperto Comunicazione di Crisi)
- Dott. Damiano Toselli (Responsabile Security Telecom Italia)
- Dott. Umberto Saccone (Responsabile Security ENI)
- Prof. Giuseppe Sciutto (Presidente NITEL)
- Dott. Giuseppe Vozza (Responsabile Sicurezza Gru
- Dott. Domenico Vulpiani (Dirigente Generale d

Rapporto tra stage esterni effettuati e co di lavoro offerti



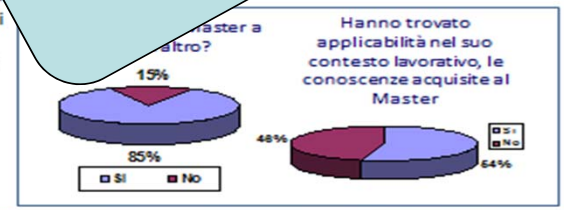
tipologie di contratti offerti, sono compresi sia quelli a determinato, che determinato, che apprendistato.

Sta



Forte incremento sia nel nume
dei candidati che degli iscritti

ex-studenti



Roberto Setola – r.setola@unicampus.it

n Homeland Security – partner

Carabinieri · Polizia di Stato · Guardia di Finanza · Vigili del Fuoco · Forestale · Penitenziaria · Capitanerie di Porto

Roberto Setola – r.setola@unicampus.it

VIII Edizione (a.a. 2015-16)
Dicembre 2015

INTRODUZIONE AL MASTER

VIII edizione del Master di II livello

Master in Homeland Security

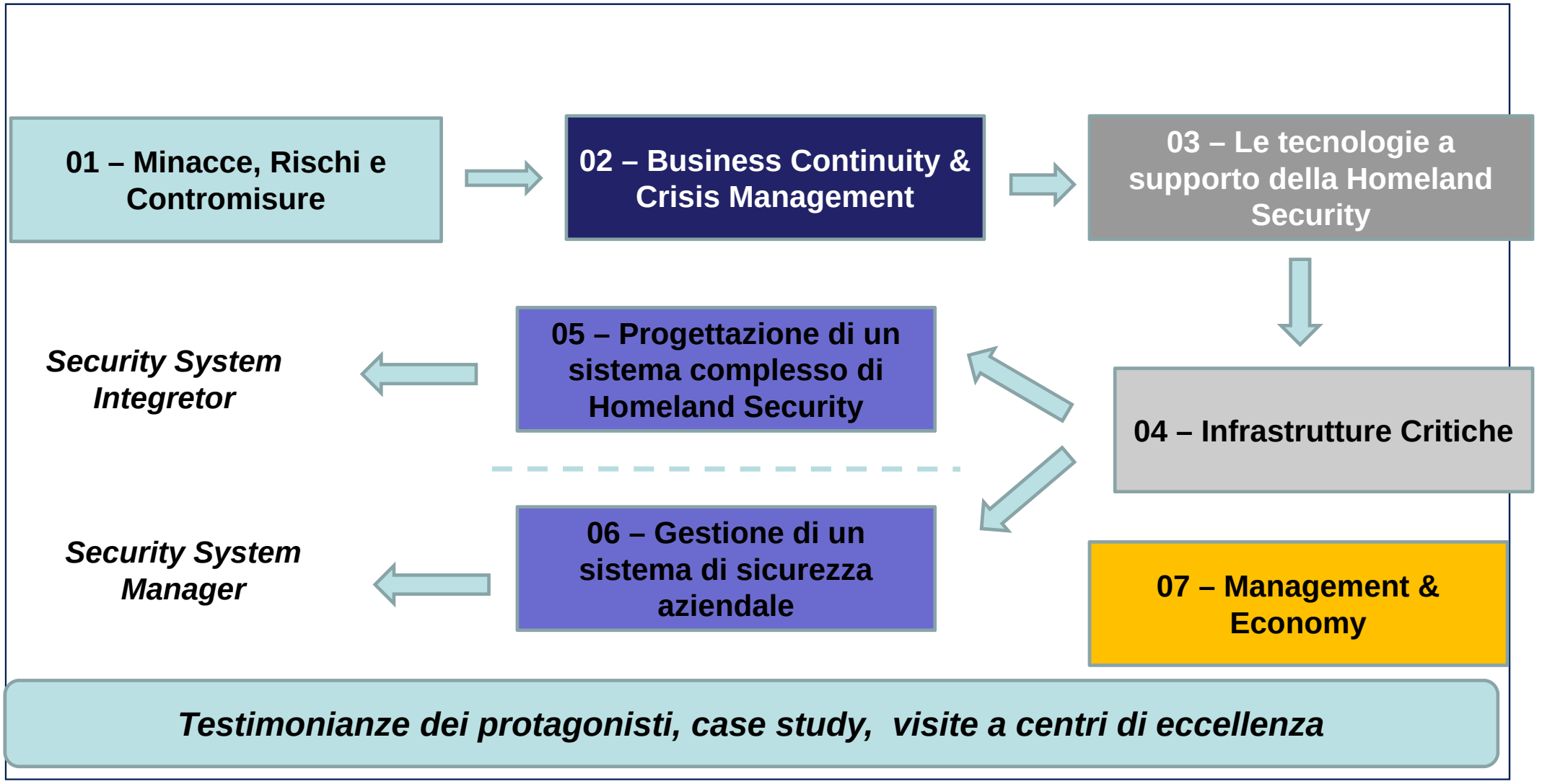
Sistemi, metodi e strumenti per la security e il crisis management

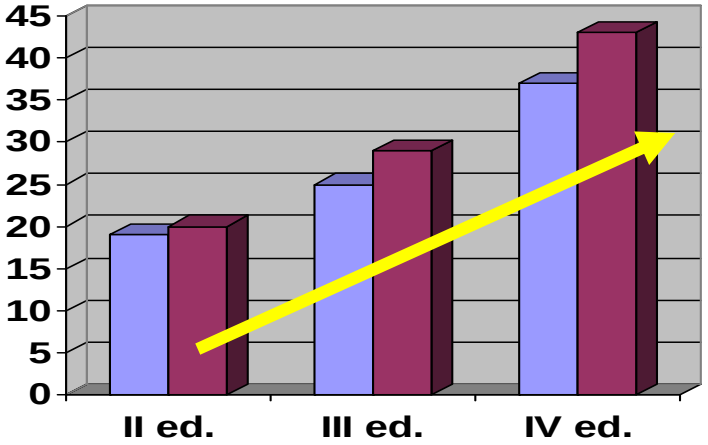
Finalità

formare tecnici e professionisti in grado di supportare il processo di analisi delle esigenze di sicurezza, di identificare le contromisure da adottare, di progettare e sviluppare soluzioni integrate per ciò che riguarda l'attuazione, la gestione e l'esercizio di procedure e sistemi di sicurezza.

Destinatari

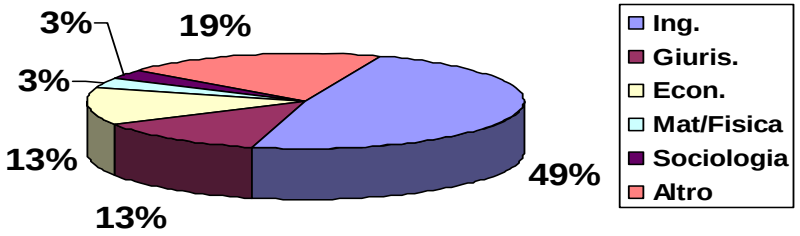
Coloro che aspirano a lavorare come progettisti di sistemi e soluzioni di sicurezza all'interno di aziende pubbliche e private, ovvero a figure professionali o consulenziali di enti e aziende con responsabilità nella gestione di Infrastrutture Critiche, di Protezione Civile, di Sicurezza, Difesa e Controllo del Territorio (Regioni, Comuni, ecc.).


01 – Minacce, Rischi e Contromisure
02 – Business Continuity & Crisis Management
03 – Le tecnologie a supporto della Homeland Security
04 – Infrastrutture Critiche
05 – Progettazione di un sistema complesso di Homeland Security
06 – Gestione di un sistema di sicurezza aziendale
07 – Management & Economy
Security System Integretor
Security System Manager
Testimonianze dei protagonisti, case study, visite a centri di eccellenza



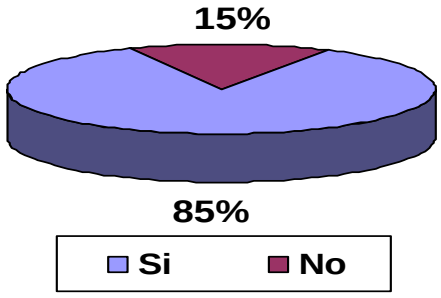
Forte incremento sia nel numero dei candidati che degli iscritti

Background partecipanti

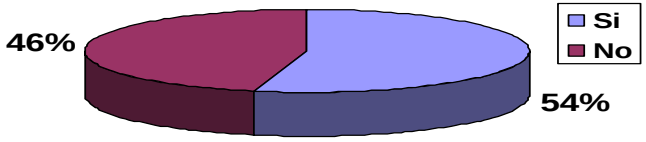


Valutazioni ex-studenti

Consiglierebbe il Master a qualcun altro?



Hanno trovato applicabilità nel suo contesto lavorativo, le conoscenze acquisite al Master



01 – Minacce, Rischi e Contromisure

Elementi normativi, gestionali, ed organizzativi. Metodologia e strumenti per l'analisi del rischio e delle vulnerabilità

Si intendono fornire gli strumenti di base per lo sviluppo di un sistema di sicurezza basato sull'analisi, classificazione e valutazione del rischio, della sua modellazione e gestione attraverso un rigoroso processo che parte dalla analisi delle minacce, delle vulnerabilità e di scenario fino all'individuazione dei possibili impatti e contromisure. Verranno forniti elementi di storia e geopolitica internazionale, fondamenti di diritto, fondamenti di economia, aspetti assicurativi e di trasferimento del rischio, nonché nozioni di normativa tecnica, circa gli stand[illegible]za.

Analisi, qualificazione e quantificazione del contesto
Perchè ?

02 – Business Continuity & Crisis Management

Prevenzione e gestione degli incidenti e delle situazioni di crisi. Sistemi e procedure di Business Continuity e Disaster Recovery. La comunicazione in situazioni di emergenza.

Il modulo ha l'obiettivo di fornire quegli strumenti metodologici ed operativi utili per comprendere i problemi connessi con la gestione delle emergenze, nelle tre dimensioni di prevention, incident handling e crisis management inclusi gli aspetti connessi con la comunicazione verso i media e i cittadini durante una crisi.

Prevenzione, Pianificazione, Incident handling & Recovery Come ?

03 – Le Tecnologie a Supporto della Homeland Security

Illustrazione delle principali tecnologie impiegate nell'ambito della Homeland Security

I processi di controllo del territorio e di mantenimento della sicurezza si avvalgono d strumenti tecnologici di varia natura che consentono da un lato di accrescere la capacità di prevenire le azioni criminose (o gli eventi accidentali capaci di compromettere la sicurezza del servizio e/o dell'infrastruttura) e dall'altro di rilevare nel loro incipit, caratterizzare meglio situazioni di crisi e di affrontarle con maggiore efficacia. Questo modulo ha l'obiettivo di illustrare le principali tecnologie oggi utilizzate evidenziandone potenzialità e limiti e sulle prevedibili evoluzioni future

Metodologie, strumenti, tecnologie (innovazioni) Con quali mezzi ?

04 – Infrastrutture Critiche

Modellistica ed analisi delle principali infrastrutture: energetiche, di trasporto, di telecomunicazione e finanziarie

Questo modulo fornisce gli elementi teorici fondamentali per comprendere le modalità di funzionamento, le architetture e le tecnologie che caratterizzano le principali infrastrutture (trasporto ferroviario, aereo, stradale, di comunicazione, energetiche e finanziarie). Tali elementi sono essenziali per caratterizzare le principali vulnerabilità e minacce che possono affliggere tali strutture e sono un prerequisito essenziale per la progettazione di un efficace sistema di security e di Business Continuity/Crisis Management in grado di tener conto delle problematiche indotte dai sempre più estesi fenomeni di interdipendenza.

Quali le minacce, i rischi, le problematiche
Chi e cosa va protetto ?

05 – Progettazione di un sistema complesso di Homeland Security

Architetture, tecnologie e strumenti per il progetto di sistemi di security moderni

Il modulo si pone l'obiettivo di preparare il discente ad approcciare in modo sistemico il problema della progettazione di sistemi per Homeland Security. Il modulo mira a fornire ai discenti quelle nozioni tecniche di base finalizzate allo sviluppo di un progetto integrato di sicurezza che contemperi gli aspetti di security, di safety ed efficienza nonché le problematiche proprio degli asset fisici, di quelli logici ed organizzativi.

Come progettare ?

06 – Gestione di un sistema di sicurezza aziendale

Elementi normativi, gestionali, ed organizzativi. Metodologia e strumenti per l'analisi del rischio e delle vulnerabilità

Si intendono fornire le nozioni di base sulla security sia dal punto di vista degli strumenti necessari alla valutazione del grado di rischio, sia dal punto di vista dell'impatto che avrebbero eventuali sistemi di sicurezza sulle prestazioni dei sistemi a cui sono applicati. Verranno forniti elementi di storia e geopolitica internazionale, fondamenti di diritto, fondamenti di economia, aspetti assicurativi e di trasferimento del rischio, nonché nozioni di normativa tecnica, circa gli standard per quel che riguarda il management di componenti e di sistemi di sicurezza.

Cosa richiedere & come gestire ?

Fornire strumenti, metodologie e competenze per poter **valutare**, **pianificare**, **definire strategie** per gestire in modo efficace ed efficiente eventi anomali e/o di security (*all hazard*) e per poter essere in grado, in presenza di un tale evento, di gestirlo ……

… con improvvisazione (intelligenza, fantasia e creatività)

Centro Eccellenza Selex SI – Roma, 13 dicembre 2010

III edizione – 2010-11
Telecom Italia

IV edizione – 2011-12
Università CAMPUS Biomedico

r.setola@unicampus.it