

Programma dettagliato insegnamenti **1° PERIODO**

Ins. 1

Security: nozioni di base e discipline correlate (05 febb – 13 febb) - NITEL

Introduzione Homeland Security	Definizioni Tassonomia di base Fondamenti di Storia e Geopolitica Internazionale
Infrastrutture Critiche	Definizioni Quadro nazionale ed Internazionale
Fondamenti di Economia	Valutazione economica del valore strategico di infrastruttura Aspetti assicurativi
Fondamenti di Diritto	Quadro normativo in tema di Security Italia Unione Europea USA
Fondamenti di Sociologia	Contesto storico - geopolitico. Concetto di percezione della sicurezza - terrorismo
Fondamenti di Scienze della Comunicazione	Impatto mediatico – strategie di comunicazione

Ins. 2

Principi e metodi di risk and vulnerably analysis (13 febb - 27 febb) - UNIBO

Introduzione al <u>rischio e alle sue misure</u>	Tipologie (naturali, tecnologici, specifici,...) componenti (probabilità, magnitudo), indici (OSHA, FAR, ecc.), rischio individuale e rischio sociale. Criteri di tollerabilità.
Principali metodologie per la <u>identificazione dei pericoli</u>	Analisi storica, liste di controllo, FMEA/C, What-If, HazOp.
Metodologie di <u>valutazione quali –quantitativa dei rischi</u>	Elementi di base (affidabilità di componenti e strutture complesse), matrici di rischio, LOPA (layers of protection analysis), analisi degli alberi di guasto (fault tree) per identificare e quantificare i modi di guasto di un sistema, alberi degli eventi per evidenziare e determinare la probabilità degli scenari incidentali.
<u>Vulnerabilità dei bersagli</u> <u>Transportation risk analysis:</u>	Collettività, tipologie di strutture industriali e infrastrutture di servizio e criticità. Identificazione dei bersagli e indici di vulnerabilità. Casi esemplificativi del settore industriale e dei trasporti su strada e ferrovia - Elementi di Transportation risk analysis - Analisi pre-crisi e post-crisi per le infrastrutture viarie. Approccio “What if”. Modelli di simulazione dei sistemi di trasporto durante gli eventi terroristici: modelli di domanda; modelli di offerta; modelli di interazione domanda-offerta. I modelli di evacuazione. - Infrastrutture critiche ed effetto domino: aumento dei bersagli ed estensione delle aree di danno.

Ins. 3

Le tecnologie a supporto della Homeland Security (27 febb – 12 mar) - ELSAGDATAMAT

Tecnologie per la security governance	Metodologie e strumenti automatici a supporto dei processi di analisi del rischio, pianificazione della sicurezza, gestione della sicurezza, etc.
Tecnologie per la sicurezza logica	<ul style="list-style-type: none">○ Cenni sulle tecniche crittografiche per la protezione dei dati e delle reti di comunicazione○ La sicurezza dei sistemi SCADA (Supervisory Control And Data Acquisition)
Tecnologie per la sicurezza fisica	<ul style="list-style-type: none">○ Normativa di riferimento in Italia ed Europa;○ Sensoristica<ol style="list-style-type: none">1. Prestazioni dei sensori<ul style="list-style-type: none">• Probability of Detection (PD)• False Alarm Rate (FAR)• Nuisance Alarm Rate (NAR)• Vulnerability to Defeat (VD);2. Rivelatori di sostanze pericolose (droghe/esplosivi, agenti NBCR);3. Rivelatori elettro-ottici long range.○ Tecnologie per la videosorveglianza<ol style="list-style-type: none">1. Schemi trasmissivi (unicast, multi cast, ecc.);2. Codifica e trasmissione dei flussi video;3. Metadattazione dei flussi video (MPEG-7);4. Evoluzione delle codifiche video.5. Tecniche di base per l'analisi delle scene○ Biometria<ol style="list-style-type: none">1. tecniche, stato dell'arte e prospettive
Tecnologie per l'intelligence e il supporto alle decisioni	I sistemi di supporto alle decisioni, alle investigazioni e all'intelligence da fonti aperte per il controllo del territorio

Ins. 4

Reti (infrastrutture, trasporti, energia, telecomunicazioni) (12 mar – 21 mar) – SELEX COMMS

Elementi di Teoria delle Reti	<ul style="list-style-type: none">• Introduzione alle reti di telecomunicazioni:• Topologie di Rete e servizi• Comunicazione e modi di trasferimento• Stack protocollari: il modello OSI ed il TCP/IP• Indirizzamento ed instradamento per le reti IP• Cenni sulle reti locali "Ethernet" e senza filo "Wi-Fi"• Protocolli di trasporto ed applicazioni (in particolare basate su TCP ed UDP)
Reti di Comunicazione	<ul style="list-style-type: none">• Il ruolo strategico delle comunicazioni nel contesto HLS: il costo della non comunicazione nelle emergenze• Scenari: le reti di telecomunicazioni in un contesto di HLS• I requisiti delle reti TLC in un contesto HLS

	<ul style="list-style-type: none"> • Le soluzioni di rete
Attuatori e Sensori	Presentazione delle principali caratteristiche dei sensori e delle tecnologie correlate
Case study	Presentazione di alcuni progetti inerenti a soluzioni di reti in un contesto di Homeland Security

2° PERIODO

Ins. 5

Architettura e progettazione degli impianti di security (02 apr – 17 apr) –

GRUPPO FS

Introduzione	La security in ambito ferroviario: aspetti tecnici, normativi e gestionali
Aspetti normativi per la security	-la tutela dei dati personali ed il controllo dei lavoratori -Normativa sulla privacy:D.lgs. 196/03; Provvedimento generale sulla videosorveglianza 29/04/2004Lo statuto dei lavoratori: Legge 300/70
Sistemi tecnici di security	La sicurezza passiva (recinzioni perimetrali, porte/finestre blindate o corazzate, serrature) La sicurezza attiva (sistemi TVCC e loro architettura e tecnologia, sistemi di allarme, classi di sensori di rilevamento e loro principi di funzionamento, sistemi di controllo accessi) Sistemi di trasporto dati in ambito ferroviario e loro possibili applicazioni per la security
La protezione dei treni	- La protezione dei treni di merci speciali (prodotti pregiati, sostanze nucleari - La gestione degli spostamenti potenzialmente critici (tifosi e manifestanti)
Sistemi SW	- Sistemi SW per la gestione degli impianti integrati di security e principali filtri di video analisi - Linee guida per la predisposizione ed allestimento di una “control room” (aspetti tecnici ed organizzativi) - ERASM
Tecnologie di ultima generazione	- Overview delle tecnologie di ultima generazione - Esempi di applicazione (case studies) in ambito ferroviario
La normativa sul Segreto di Stato NATO-UEO:	Le misure di sicurezza per i locali e per la gestione dei documenti classificati
La gestione dei flussi e deflussi	La gestione dei flussi e deflussi ai e dai treni in occasione di interesse della protezione civile (grandi eventi, calamità)
Un case history	Sviluppo di un caso reale

Ins. 6

Progettazione di un sistema complesso per la Homeland Security (18 apr – 15 mag) – SELEX SI

Il Processo di Progettazione Architeturale dei Sistemi Complessi: Introduzione	Introduzione alla struttura del processo di progettazione architeturale, definizione delle principali fasi e delle relative interdipendenze
Definizione del Problema ed Analisi del Bisogno	Principali metodiche applicabili per la implementazione della fase iniziale e preparatoria del processo di Progettazione Architeturale
Descrizione Architeturale e Modellazione di Sistemi Complessi	Metodi e standard applicabili per la descrizione architeturale e la modellazione strutturata di sistemi complessi
Modellazione ed Integrazione della Componente Umana	Principali metodiche applicabili per la trattazione degli aspetti progettuali derivanti dalla integrazione della componente umana nella modellazione architeturale dei sistemi (sociotecnici) complessi
Metodi per la Analisi delle Alternative	Principali metodiche per la analisi comparata di soluzioni realizzative alternative finalizzate alla individuazione della soluzione che rappresenta il migliore bilanciamento tra il livello dei risultati ed il rispetto di condizionamenti e vincoli economici.

Ins. 7

Crisis management (15 mag – 6 giu) – POSTE ITALIANE

Il contesto normativo e legislativo di riferimento italiano ed europeo	<p>a. La pubblica amministrazione digitale e sistema pubblico di connettività: aspetti di riflessione nell'ambito della sicurezza nazionale</p> <p>b. Direttiva Europea e un possibile modello nazionale di individuazione delle Infrastrutture Critiche</p> <p>c. Le riforme europee ed italiane nel settore della sicurezza e della privacy</p> <p>d. Antiterrorismo e strategia normativa</p> <p>e. Data retention: equilibrio tra privacy e protezione degli asset nazionali</p> <p>f. La legge 48 del 2008 e tutela degli asset critici informatizzati</p> <p>g. Infrastrutture critiche, informatica e cyberterrorismo: rischi, minacce e coordinamento delle azioni di mitigazione</p> <p>h. CNAIPIC e sicurezza informatica nel sistema paese</p>
La fase conoscitiva	<ul style="list-style-type: none"> o Cosa è una crisi o cosa significa Crisis management o i possibili generatori di Crisi (alcuni esempi) o definizione di incidente, emergenza e crisi o gli eventi che possono portare ad una crisi o I costi potenziali diretti ed indiretti di una crisi o i passi principali per la gestione di una crisi o i rapporti con i media
La gestione delle crisi in azienda	<ul style="list-style-type: none"> - La policy di crisis Management - la classificazione degli eventi - l'identificazione e la classificazione delle aree e dei

	<p>sistemi critici in azienda</p> <ul style="list-style-type: none"> - l'identificazione e la classificazione dei fornitori - Strutture , ruoli e responsabilità per la gestione della crisi – unita di crisi - Il crisis management Board ed il crisis team - le fasi della crisi - Il processo di gestione della crisi - Le procedure operative per la gestione degli incidenti e delle crisi
<p>Il Business Continuity Planning & Disaster recovery (In IT)</p> <p>Business Continuity Maturity Model Il code of practice Bs 25999-1 e lo schema di certificazione : BS 25999 -2 Il CSIRT in azienda Le infrastrutture critiche del sistema paese</p>	<ul style="list-style-type: none"> ▪ Cosa è un BCP ▪ Quali sono gli eventi che gestisce ▪ Quali sono gli obiettivi e le priorità di un BCP ▪ Il ciclo continuo di un BCP ▪ Relazioni tra i controlli preventivi e piano di emergenza post incidente (contingency plan) ▪ Le componenti principali di un BCP ▪ La componente di Recovery ed il Disaster recovery (IT)

Ins. 8

Testimonianze e analisi casi di studio (21 mag – 06 giu)

Azienda	Titolo sottomodulo	Descrizione contenuto
Poste Italiane	L'esperienza di Poste Italiane nel furto di identità digitale	<p>Le misure antiphishing</p> <p>La comunicazione ed informazione / formazione</p> <p>La prevenzione</p> <p>Monitoraggio della rete</p> <p>La centrale allarmi antiphishing</p> <p>Il contrasto</p> <p>Monitoraggio prodotti e canali</p> <p>Cooperazione FFPP e Magistratura</p> <p>La nuova sicurezza per il cliente per l'anno 2009</p>
Poste Italiane	Enterprise Fraud Management System: un approccio integrato alle frodi aziendali.	<p>Il monitoraggio dei canali online</p> <p>Il monitoraggio dei canali offline</p> <p>Il progetto Oracolo: controllo dei documenti e furto di identità</p> <p>Le frodi cross channel</p> <p>Postemobile: telecomunicazioni e banca sul cellulare, sicurezza e frodi</p> <p>La Security Room di Poste Italiane</p>
Enel Spa	La gestione delle emergenze e delle crisi per la continuità del sistema elettrico	<p>L'intervento illustra il modello di crisis management adottato da Enel Spa, realizzato anche sulla base dell'esperienza maturata a seguito del black out della rete elettrica del settembre 2003. In particolare, saranno descritti gli elementi organizzativi, procedurali, logistici e tecnici a supporto del modello,</p>

		nonchè le relative modalità di verifica e test periodico.
Ansaldo STS	Analisi del rischio applicata a sistemi di trasporto a guida vincolata.	Richiami di analisi del rischio qualitativa e quantitativa. Raccolta delle informazioni (documenti di progetto, dati statistici, sopralluoghi sul campo, ecc.), modelli di calcolo di vulnerabilità e rischio, interpretazione e rappresentazione dei risultati. Mitigazione del rischio e valutazione costi/benefici. Strumenti di supporto. Rapporti di esperienze pratiche.
AIC	Protezione delle Infrastrutture Critiche	Il termine Protezione delle Infrastrutture Critiche (in inglese Critical Infrastructure Protection, da cui la sigla CIP) indica una diversa strategia di approccio alla sicurezza delle grandi infrastrutture tecnologiche che nasce dall'esigenza di adeguarla al mutato contesto tecnologico e geo-politico. Quello che emerge, sempre più, è la necessità di offrire soluzioni "All-Hazard" con l'obiettivo di garantire adeguati livelli di "service continuity". L'intervento illustrerà le principali azioni intraprese da governi ed organismi sovra-nazionali sul tema con specifico riferimento alla direttiva europea 2008/114/CE su questo tema di recente emanazione
Ferrovie		
AIC & ENAV	Sicurezza del trasporto Aereo	Verranno illustrate le moderne strategie per la gestione della sicurezza del sistema di trasporto aereo e di come questo si è evoluto dopo gli eventi del 11/9
AIC	Sicurezza dei Sistemi di Controllo nell'ambito della trasmissione elettrica	Verranno illustrate alcune delle moderne strategie per la gestione della sicurezza del sistema elettrico sia dal punto di vista del profilo organizzativo che di quello tecnico ed informatico
Ansaldo STS	Architettura e funzionalità di un sistema di security per il trasporto metropolitano	Contesto di riferimento: caratteristiche e vulnerabilità dei sistemi, problematiche ed esigenze dell' esercente. Tecnologie di monitoraggio e protezione: sottosistemi anti-intrusione e controllo accessi, videosorveglianza intelligente, rilevamento suoni anomali, rete di comunicazione, sistema di gestione integrato. Sistema di gestione della security (Security Management System, SMS): architettura hardware e software, principali funzionalità, interfaccia utente, integrazione dei dati e correlazione degli allarmi. Attività di ricerca e prospettive future: strumenti di supporto al progetto, reti di smart-sensor wireless, motori di rilevamento di eventi complessi, nuove funzionalità SMS.