SERIT
SEcurity Research in Italy

2011

Prefazione

In un settore così ampio, complesso e delicato come la sicurezza, è significativo che oltre 150 persone in rappresentanza del mondo dell'industria, dell'accademia, delle istituzioni e degli utenti finali, stanno contribuendo a definire le linee di ricerca dei prossimi anni ed i loro sforzi sono rispecchiati nel presente documento.

La sua presentazione sottolinea l'importanza attribuita alla ricerca ed innovazione in ambito sicurezza.

La speranza è che questo documento possa offrire un solido quadro di riferimento rispetto al quale molti programmi di ricerca europei, nazionali, regionali e anche privati possano essere concepiti, delineati e attuati. Non può naturalmente essere considerato un piano rigido a lungo termine, ma esso deve intendersi come un documento vivo che sarà periodicamente aggiornato, per tenere in conto di nuove informazioni e delle mutate circostanze.

Un grazie a tutti coloro che stanno contribuendo al lavoro.

Cristina Leone
Sandro Massa

Indice

Introduzione

Per ricerca in ambito ***Homeland Security*** si intende lo sviluppo di capacità e tecnologie volte ad individuare, prevenire, contrastare e gestire l'impatto di atti criminali e dolosi, inclusi quelli terroristici, che possano nuocere ai cittadini, alle organizzazioni, alle infrastrutture ed ai beni materiali ed immateriali.

Si considerano inoltre tutte le attività di ricerca e sviluppo rivolte alla mitigazione dei rischi, alla gestione delle crisi e all'assicurazione della continuità operativa, a valle di eventuali attacchi/incidenti, in un'ottica *all hazards approach*, che tenga conto anche di disastri naturali, antropici e industriali e rischi emergenti.

Un'analisi socio economica degli eventi, che, nell'ultimo decennio, hanno messo a repentaglio la Homeland Security, sia in Europa che negli Stati Uniti, dimostra che i disastri naturali e/o industriali hanno contribuito in maniera tristemente significativa sia in termini di perdite economiche che di perdite di vite umane. Da qui la necessità di considerare il problema della Homeland Security in modo sinergico al contesto geo-fisico-politico nel quale opera l'*asset* o il sistema da proteggere.

E' indispensabile preparare adeguatamente la società verso i rischi, che possono presentarsi, sviluppando la ricerca nella direzione di soluzioni efficienti ed economicamente efficaci per le sfide della sicurezza.
Tuttavia, le minacce si modificano continuamente e divengono sempre più complesse e sofisticate e solo con una innovazione continua è possibile garantire che, le risposte tecnologiche mantengano nel tempo la loro validità.
Le misure di politica pubblica e gli investimenti del settore privato in ricerca e sviluppo devono tener conto dell'evoluzione degli scenari (ad esempio i cambiamenti climatici) ed essere flessibili ed adattabili. Il concetto di security va spostato progressivamente verso il concetto di *resilience*: non basta solo proteggere ma serve garantire la continuità del servizio.

La sicurezza, la legalità e la salvaguardia del territorio, costituiscono condizioni imprescindibili per una buona qualità della vita dei cittadini e per lo sviluppo economico dell'Italia.
Purtroppo, gli anni recenti hanno evidenziato in maniera drammatica, da un lato, la fragilità delle società occidentali e dei loro sistemi complessi (p.e. il sistema del trasporto aereo e ferroviario) e, dall'altro, la fortissima esigenza di maggior sicurezza.

Si potrebbe affermare che i tragici eventi di New York, Londra e Madrid rappresentano un punto di arrivo per la percezione collettiva della gravità della minaccia portata dal terrorismo, che spesso viene alimentata da situazioni di crisi lontane dai propri confini; al tempo stesso, però, l'11 settembre è anche il punto di partenza per l'avvio accelerato del processo di sviluppo di nuovi mezzi tecnologici necessari per garantire una maggiore sicurezza della collettività.

Dal punto di vista della sicurezza, l'Italia si inserisce nel contesto europeo e internazionale (sia per la natura dei problemi che per le possibili risposte, compresa la cooperazione internazionale, sia europea che trans-atlantica), ed intende dedicare ai vari aspetti della sicurezza la necessaria attenzione e le imprescindibili risorse.

Che cos'è SERIT?

SERIT (*SEcurity Research in Italy*) è la Piattaforma Tecnologica Nazionale sulla Sicurezza, promossa congiuntamente da CNR e Finmeccanica.
SERIT è il tavolo dove, con il contributo degli stakeholder nazionali, utenti finali, industrie, istituzioni e centri di ricerca, si sono individuati i seguenti obiettivi di alto livello per la Sicurezza, in sinergia con le linee strategiche della ricerca europea:

- Studiare e realizzare sistemi e tecnologie per proteggere i cittadini e gli *asset* sensibili italiani.
- Studiare e realizzare sistemi e servizi per il monitoraggio del territorio e di prevenzione dei rischi emergenti, in sinergia con i sistemi per la prevenzione delle catastrofi naturali e per la gestione delle crisi;
- Studiare e realizzare sistemi e tecnologie per il controllo delle frontiere;
- Aumentare la competitività del sistema Paese, attraverso un'efficace programmazione e gestione delle attività di ricerca nell'ambito delle tematiche proprie della sicurezza, individuando risultati concreti e collocabili sul mercato;
- Rafforzare le iniziative internazionali tese a sviluppare tecnologie per la Security, supportando le linee di ricerca prioritarie nel VII e VIII Programma Quadro.

SERIT è un forum indipendente, aperto, che si basa sul lavoro volontario dei suoi membri.

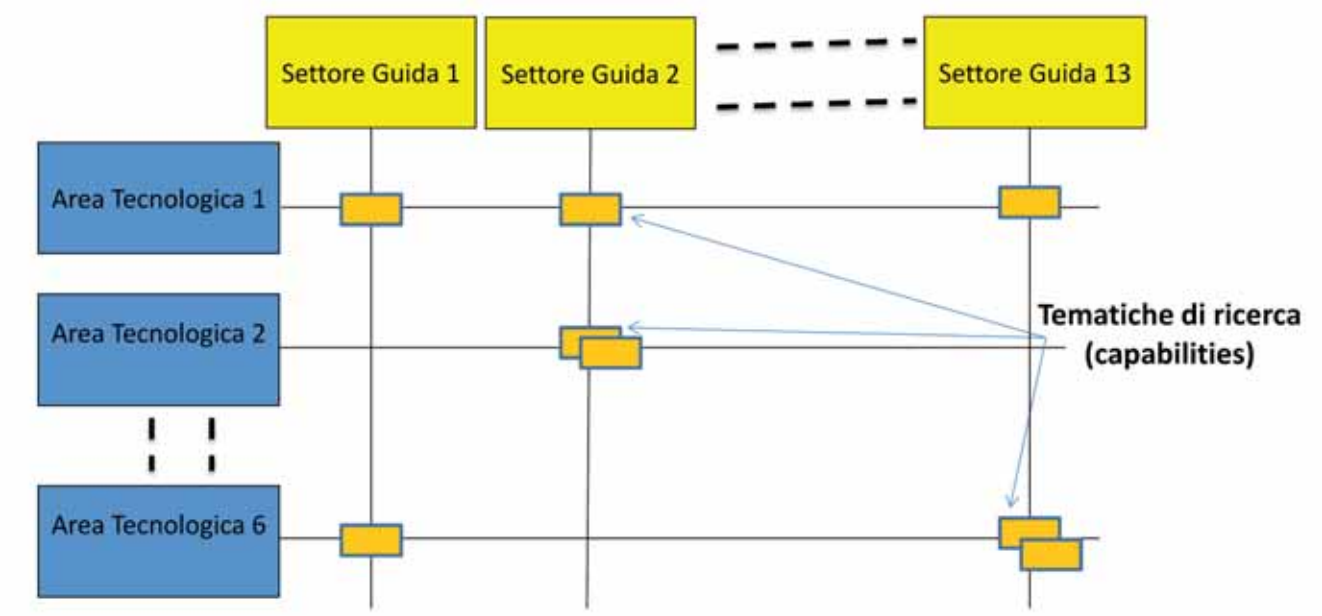
Metodologia

SERIT è strutturata secondo un'organizzazione a matrice:

- **Settori Guida**: Missioni prioritarie per l'Italia
- **Aree Tecnologiche**: Domini tecnologici prioritari

I membri dei Settori Guida hanno identificato le problematiche prioritarie da risolvere (sottotematiche di ricerca), in maniera *top-down*.

I membri delle Aree Tecnologiche hanno generato in maniera *bottom-up* le risposte tecnologiche (*Capability*), alle esigenze identificate dai Settori Guida.



Le attività svolte ad oggi hanno permesso di identificare anche una lista di tecnologie specifiche per ogni capability, la cui *roadmap*, verrà sviluppata nel proseguo del lavoro della piattaforma.

La lista completa delle *capability* identificate è riportata di seguito.

Settori Guida:

- Sicurezza ferroviaria
- Protezione dell'approvvigionamento, della generazione e della distribuzione di energia elettrica
- Sicurezza del trasporto multimodale
- Sicurezza del trasporto su strada
- ICT per la Sicurezza
- Sicurezza dei confini
- Sicurezza aeroportuale
- Tecnologie satellitari per il controllo del territorio e dell'ambiente
- Sicurezza nel costruito
- Sicurezza integrata nei beni culturali
- Sicurezza nucleare
- Sicurezza agroalimentare
- Sicurezza & Salute

Aree Tecnologiche:

TA 1: Sorveglianza & Situation Awareness

TA 2: Comunicazioni

TA 3: Detection & Identification Systems

TA 4: Tecnologie per Crisis Management e per la Protezione di Persone, Asset e Infrastrutture

TA 5: Information Processing and Management

TA 6: CBRNE

TA1	Settori Guida												
Capability	1. Sicurezza ferroviaria	2. Protezione dell'approvvigionamento,[…] energia elettrica	3. Sicurezza del trasporto multimodale	4. Sicurezza del trasporto su strada	5. ICT per la Sicurezza	6. Sicurezza dei confini	7. Sicurezza aeroportuale	8. Tecnologie […] dell'ambiente	9. Sicurezza nel costruito	10. Sicurezza integrata nei beni culturali	11. Sicurezza nucleare	12. Sicurezza agroalimentare	13. Sicurezza & Salute
TA1.1 Analisi integrate per rilevamento di comportamenti anomali (analisi per immagini / analisi varie), sensori per la generazione di Early Warning	x		x							x			
TA1.2 Data Fusion di sensori eterogenei	x			x		x			x	x			
TA1.3 Elaborazione di immagini satellitari (SAR, ottico) ad alta risoluzione								x	x				
TA1.4 Tecnologie abilitanti per il settore spaziale						x		x					
TA1.5 Sensori per il monitoraggio delle infrastrutture di produzione di energia e delle reti di distribuzione		x			x								
TA1.6 Sistemi di localizzazione, navigazione e guida assistita						x		x					
TA1.7 Sistemi di sorveglianza perimetrale	x	x					x						
TA1.8 Piattaforme di sorveglianza marittima, terrestre e aerea								x					
TA1.9 Strumenti di supporto alla sorveglianza mediante riconoscimento di scene e cross correlation di informazioni	x												
TA1.10 Sensori per la sorveglianza marittima e costiera, basati a terra o imbarcati						x							

TA2	Settori Guida												
Capability	1. Sicurezza ferroviaria	2. Protezione dell'approvvigionamento,[…] energia elettrica	3. Sicurezza del trasporto multimodale	4. Sicurezza del trasporto su strada	5. ICT per la Sicurezza	6. Sicurezza dei confini	7. Sicurezza aeroportuale	8. Tecnologie […] dell'ambiente	9. Sicurezza nel costruito	10. Sicurezza integrata nei beni culturali	11. Sicurezza nucleare	12. Sicurezza agroalimentare	13. Sicurezza & Salute
TA2.1 Sistemi di trasmissione dati da mezzi in movimento			x	x				x					
TA 2.2 Reti wireless ad-hoc e di sensori				x				x		x			
TA2.3 Sistemi per la diffusione delle informazioni in situazioni critiche						x							x
TA2.4 Integrazione del segmento satellitare a supporto di applicazioni evolute			x					x					
TA2.5 Architetture evolutive dei sistemi di comunicazione per first responders						x							
TA2.6 Middleware, architetture di rete e comunicazione (Network Centric Communication), per l'integrazione di reti e sistemi eterogenei		x	x			x							
TA2.7 Studio architetture Software Defined Radio & Cognitive Radio per applicazioni di sicurezza								x					
TA2.8 Protezione e disturbo del canale di trasmissione dati								x					
TA2.9 Architetture di rete orientate al fast deployment						x							
TA2.10 Sicurezza di Rete		x			x			x					

TA3	Settori Guida												
Capability	1. Sicurezza ferroviaria	2. Protezione dell'approvvigionamento,[…] energia elettrica	3. Sicurezza del trasporto multimodale	4. Sicurezza del trasporto su strada	5. ICT per la Sicurezza	6. Sicurezza dei confini	7. Sicurezza aeroportuale	8. Tecnologie […] dell'ambiente	9. Sicurezza nel costruito	10. Sicurezza integrata nei beni culturali	11. Sicurezza nucleare	12. Sicurezza agroalimentare	13. Sicurezza & Salute
TA3.1 Detection ed imaging di persone e oggetti attraverso gli ostacoli (fuoco, muri, smog, metalli e altro)	x		x	x		x	x						
TA3.2 Sviluppo dei sistemi di monitoraggio diretto (sensori,…) / indiretto (comandi primari/ secondari del veicolo) e monitoraggio in remoto dei parametri dello stato del guidatore	x		x	x	x		x						
TA3.3 Individuazione di eventi anomali basata sull'analisi integrata di misure ambientali, comportamentali e fisiologiche, incluse le biometriche	x		x		x	x	x						
TA3.4 Check-point biometrico del futuro con auto accreditamento passeggeri	x		x		x	x	x						
TA3.5 Soluzioni che individuano minacce collegate ai conducenti di mezzi di trasporto pubblico			x	x	x								
TA3.6 Soluzioni robuste e efficienti per interoperabilità tra sistemi di gestione dell'identità elettronica e dell'autenticazione multi-biometrica nel dominio sia fisico che logico					x								

TA4	Settori Guida												
Capability	1. Sicurezza ferroviaria	2. Protezione dell'approvvigionamento,[…] energia elettrica	3. Sicurezza del trasporto multimodale	4. Sicurezza del trasporto su strada	5. ICT per la Sicurezza	6. Sicurezza dei confini	7. Sicurezza aeroportuale	8. Tecnologie […] dell'ambiente	9. Sicurezza nel costruito	10. Sicurezza integrata nei beni culturali	11. Sicurezza nucleare	12. Sicurezza agroalimentare	13. Sicurezza & Salute
TA4.1 Sistemi innovativi di anti-intrusione	x												
TA4.2 Analisi della deformazione e dei danni dell'infrastruttura in seguito ad atti terroristici o eventi naturali e loro riabilitazione									x	x			
TA4.3 Sviluppo di componenti, tecniche e metodologie per lo studio e l'analisi dei rischi sugli edifici e sugli impianti (mappe di vulnerabilità delle aree fruibili, controllo di valori soglia, etc)									x				
TA4.4 Sistemi robotici cooperativi (manned e unmanned) per la valutazione remota e preventiva dell'area interessata dall'evento e l'erogazione delle prime azioni di intervento (Robotic Rescue).										x			
TA4.5 Sistemi di assistenza e/o cooperativi per i veicoli di soccorso e di intervento, finalizzati a garantire il tempestivo raggiungimento delle aree di crisi				x									
TA4.6 Piattaforme e sistemi di comando e controllo, mono o multi - operatore, di vario livello (da C2 a C4I), con funzionalità di autoapprendimento, simulazione e training	x												
TA4.7 Metodologie e strumenti per l'analisi del rischio e l'ottimizzazione costo/benefici basati su simulazione e modellistica analitica	x	x				x				x		x	
TA4.8 Sistemi di Situation Awareness per gestire localmente situazioni anomale con l'obiettivo di prevenire effetti domino e circoscrivere le conseguenze negative		x											

TA5	Settori Guida												
Capability	1. Sicurezza ferroviaria	2. Protezione dell'approvvigionamento,[…] energia elettrica	3. Sicurezza del trasporto multimodale	4. Sicurezza del trasporto su strada	5. ICT per la Sicurezza	6. Sicurezza dei confini	7. Sicurezza aeroportuale	8. Tecnologie […] dell'ambiente	9. Sicurezza nel costruito	10. Sicurezza integrata nei beni culturali	11. Sicurezza nucleare	12. Sicurezza agroalimentare	13. Sicurezza & Salute
TA5.1 Fusione delle informazioni raccolte da diverse sorgenti al fine di aumentare e migliorare il contenuto informativo			x			x							
TA5.2 Sistemi ICT sicuri e resistenti agli attacchi (sicurezza del dato)		x			x								
TA5.3 Piattaforme, architetture ed algoritmi per l'analisi in tempo reale di grandi volumi di dati (high performance computing)					x								
TA5.4 Metodologie e sistemi per il monitoraggio di grandi architetture di rete ICT al fine di detettare anomalie, tentativi di accesso non autorizzato, incidenti		x			x								
TA5.5 Realizzazione di algoritmi e processi per l'estrazione automatica e l'elaborazione del contenuto informativo di immagini										x			
TA5.6 Modelli architetturali e tecnologie per l'integrazione, l'elaborazione, la presentazione e la diffusione delle informazioni, considerando la molteplicità delle organizzazioni coinvolte, ognuna con specifici compiti istituzionali, e le esigenze di riservatezza dei dati						x							

TA6	Settori Guida												
Capability	1. Sicurezza ferroviaria	2. Protezione dell'approvvigionamento,[…] energia elettrica	3. Sicurezza del trasporto multimodale	4. Sicurezza del trasporto su strada	5. ICT per la Sicurezza	6. Sicurezza dei confini	7. Sicurezza aeroportuale	8. Tecnologie […] dell'ambiente	9. Sicurezza nel costruito	10. Sicurezza integrata nei beni culturali	11. Sicurezza nucleare	12. Sicurezza agroalimentare	13. Sicurezza & Salute
TA6.1 Sensori di elevata sensibilità per la rivelazione di composti in tracce (esplosivi, droghe, chimici, biologici, veleni, e loro precursori) per apparati fissi o mobili						x	x					x	
TA6.2 Sensori per monitoraggio a distanza di pericoli chimici e biologici da postazione mobile o fissa							x						x
TA6.3 Piattaforme multisensori intelligenti per la riduzione dei falsi allarmi nel monitoraggio di bio-hazard			x		x	x						x	
TA6.4 Tecnologie microfluidiche accoppiate a nanostrutture molecolari per la detezione di biohazard						x						x	
TA6.5 Grandi portali di nuova generazione con attivazione neutronica o raggi X per la rivelazione di materiale nucleare o esplosivo dentro i container con l'impiego di rivelatori passivi che operano in ambiente ostile			x								x		
TA6.6 Tecnologie di scansione rapida, da onde millimetriche a raggi X, per la ricostruzione di immagini e rivelare pericoli da postazione fissa al fine di rilevare esplosivi ed altri materiali pericolosi							x						
TA6.7 Nanotecnolgie per sistemi in spettrometria di massa: applicazioni nella rivelazione di esplosivi, droghe (metaboliti e impurezze).						x	x					x	
TA6.8 Strumenti compatti ed efficienti per la rivelazione di parti metalliche di armi e munizioni o detonatori							x						
TA6.9 Strumentazione portatile attiva o passiva per il monitoraggio di materiale radioattivo in discariche o in container commerciali								x			x		

1. Sicurezza Ferroviaria

Introduzione

Garantire livelli elevati di security per i sistemi di trasporto su rotaia è un obiettivo fondamentale per gli operatori e i responsabili delle infrastrutture ferroviarie. Il termine security viene utilizzato nella sua più ampia accezione di significato, comprendendo tutte le minacce provenienti dall'esterno del sistema di trasporto su rotaia, come quelle dovute ad eventi naturali (esempio piogge, frane) e ad azioni intenzionali tendenti a recare danno alle persone ed alle cose.

Il trasporto su rotaia è altamente esposto a minacce, sia per le dimensioni della rete di trasporto e della sua penetrazione nel territorio e nei centri abitati, sia per il numero di passeggeri e di merci trasportati per anno. Al fine di prevenire e proteggere le infrastrutture ferroviarie da incidenti/attacchi, è necessario condurre azioni di ricerca e di innovazione industriale aventi come obiettivo globale quello di studiare, specificare, progettare e sperimentare, sulla base delle conoscenze sistemistiche di processo e delle capacità di sviluppo tecnologico presenti sul territorio italiano presso le aziende e gli organismi di ricerca, metodologie di analisi e progettazione di sistemi integrati avanzati di sorveglianza e di controllo, in grado di fornire un elevato livello di "security" ai sistemi di trasporto su ferro, sia per i passeggeri che per le merci.
Di seguito si descriveranno in modo sintetico e non esaustivo i principali asset per i quali occorre, prioritariamente, effettuare azioni di ricerca ed innovazioni che, sulla base della disponibilità attuale delle tecnologie, promettono un sensibile incremento dei livelli di security.

SOTTOTEMATICHE DI RICERCA:

Sicurezza dei Sistemi di Controllo e Segnalamento

L'obiettivo fondamentale della ricerca è la realizzazione ed integrazione di tecnologie e procedure finalizzate alla

protezione dei sistemi necessari alla circolazione ferroviaria nei confronti di sabotaggi e attacchi terroristici, soprattutto di tipo informatico (protezione fisica e logica degli apparati informatici). Si fa riferimento sia a “Sistemi vitali”, a sicurezza intrinseca per gestione del Traffico (*interlocking*, sistemi di blocco), sia a “Sistemi non-vitali”, quali supervisione del traffico, telecomando itinerari, servizi generali (es. prenotazioni).

Protezione delle infrastrutture

Nell’ambito della security fisica è di notevole interesse lo sviluppo di sistemi di monitoraggio e protezione di edifici (centri di controllo, depositi, aree aperte al pubblico, ecc.) e linee ferroviarie (inclusi rilevati, ponti e gallerie).

Controllo degli accessi

Si è manifestata l’esigenza di sviluppare sistemi di monitoraggio delle persone per il rilevamento di comportamenti anomali e minacce o, comunque, per rilevarne l’accesso a locali tecnici riservati ad operatori appositamente autorizzati.

Trasporto merci

Si richiede di sviluppare strumenti di controllo di contenuto ed integrità dei carri merci finalizzati a prevenire e rilevare situazioni di rischio legati alla pericolosità del carico.

Le principali capability da sviluppare sono:

TA1.1 Analisi integrate per rilevamento di comportamenti anomali (analisi per immagini / analisi varie), sensori per la generazione di Early Warning	Pag.44
TA1.2 Data Fusion di sensori eterogenei	Pag.45
TA1.7 Sistemi di sorveglianza perimetrale	Pag.50
TA1.9 Strumenti di supporto alla sorveglianza mediante riconoscimento di scene e cross correlation di informazioni	Pag.52
TA3.1 Detection ed imaging di persone e oggetti attraverso gli ostacoli (fuoco, muri, smog, metalli e altro)	Pag.68
TA3.2 Sviluppo dei sistemi di monitoraggio diretto (sensori,…) / indiretto (comandi primari/ secondari del veicolo) e monitoraggio in remoto dei parametri dello stato del guidatore	Pag.69
TA3.3 Individuazione di eventi anomali basata sull'analisi integrata di misure ambientali, comportamentali e fisiologiche, incluse le biometriche	Pag.70
TA3.4 Check-point biometrico del futuro con auto accreditamento passeggeri	Pag.71
TA4.1 Sistemi innovativi di anti-intrusione	Pag.75
TA4.6 Piattaforme e sistemi di comando e controllo, mono o multi - operatore, di vario livello (da C2 a C4I), con funzionalità di autoapprendimento, simulazione e training	Pag.80
TA4.7 Metodologie e strumenti per l'analisi del rischio e l'ottimizzazione costo/benefici basati su simulazione e modellistica analitica	Pag.81

2. Protezione dell'approvvigionamento, della generazione e della distribuzione di energia elettrica

Introduzione

Il sistema elettrico nazionale, nelle sue componenti di Generazione, Trasmissione e Distribuzione, ha l'obiettivo di assicurare alla nazione uno sviluppo sostenibile in un mercato competitivo globale. La caduta del Sistema elettrico o di parti importanti dello stesso può difatti provocare effetti di caduta a cascata di tutti gli altri sistemi tecnologici vitali per la nazione, dalle telecomunicazioni ai trasporti, dalla finanza alla sanità.
Con la liberalizzazione dei mercati, il Sistema elettrico è divenuto sempre più complesso, e di conseguenza vulnerabile a diversi tipi di minacce, dagli atti di terrorismo ai disastri naturali. In aggiunta, la penetrazione

sempre più forte delle tecnologie ICT necessarie alla gestione del Sistema, rende lo stesso sempre più vulnerabile alle nuove minacce informatiche. È importante che lo sviluppo di tecnologie ICT adeguate sia in grado di garantire la flessibilità, la sicurezza del Sistema (e/o di parti di esso), e la resilienza, intesa come la capacità del Sistema elettrico di continuare a fornire il servizio atteso anche in presenza di eventi avversi multipli (come indicato anche nel SET-Plan della Commissione Europea "*Investing in the Development of Low Carbon Technologies*" http://ec.europa.eu/energy/technology/set_plan/set_plan_en.htm).
Da menzionare infine che gli Stati Membri dell'Unione europea hanno inoltre adottato le misure necessarie per conformarsi alla "Direttiva Europea relativa all'individuazione e alla designazione delle infrastrutture critiche europee e alla valutazione della necessità di migliorarne la protezione" (114/08/CE).

SOTTOTEMATICHE DI RICERCA:

Studio della complessità, delle interazioni e delle vulnerabilità dovute alle interdipendenze

L'obiettivo della ricerca è quello di aumentare la conoscenza delle vulnerabilità del Sistema elettrico (sia fisiche

che cyber), studiare gli effetti a cascata indotti dalla caduta del Sistema elettrico verso altri sistemi o viceversa, diminuire le possibilità di caduta a cascata attraverso l'attivazione di procedure di *information sharing* tra gli operatori di Reti tra loro interdipendenti (sia nello stesso settore che in settori diversi).

Monitoraggio della rete

Nell'ambito della sicurezza del sistema di produzione e fornitura elettrica, assume un ruolo importante il monitoraggio della rete, e cioè quell'insieme di azioni utili ad analizzare, in modo continuo, gli impianti di generazione, trasmissione e distribuzione dell'energia elettrica, al fine di assicurare la funzionalità essenziale anche in condizioni di emergenza a seguito di eventi catastrofici o di atti di sabotaggio.

Prevenzione degli effetti a cascata

L'obiettivo della ricerca è quello di ridurre i rischi connessi ad eventi critici ad un livello di accettabilità combinando azioni di prevenzione, rilevazione, diagnosi e mitigazione. Risultano fondamentali per il raggiungimento di tale obiettivo le attività di ricerca focalizzate allo sviluppo di metodi e strumenti per consentire di analizzare correttamente lo stato della rete elettrica, rilevare eventuali situazioni anomale e individuare la parte del sistema interessata al fine di isolarla ed impedire effetti-domino. Il tutto può essere conseguito con un approccio progettuale di tipo *self-healing* e l'adozione di sistemi di controllo decentralizzato con capacità di *self- management* e *self-reaction*.

Sistemi di sicurezza integrata per la protezione degli asset del Sistema elettrico

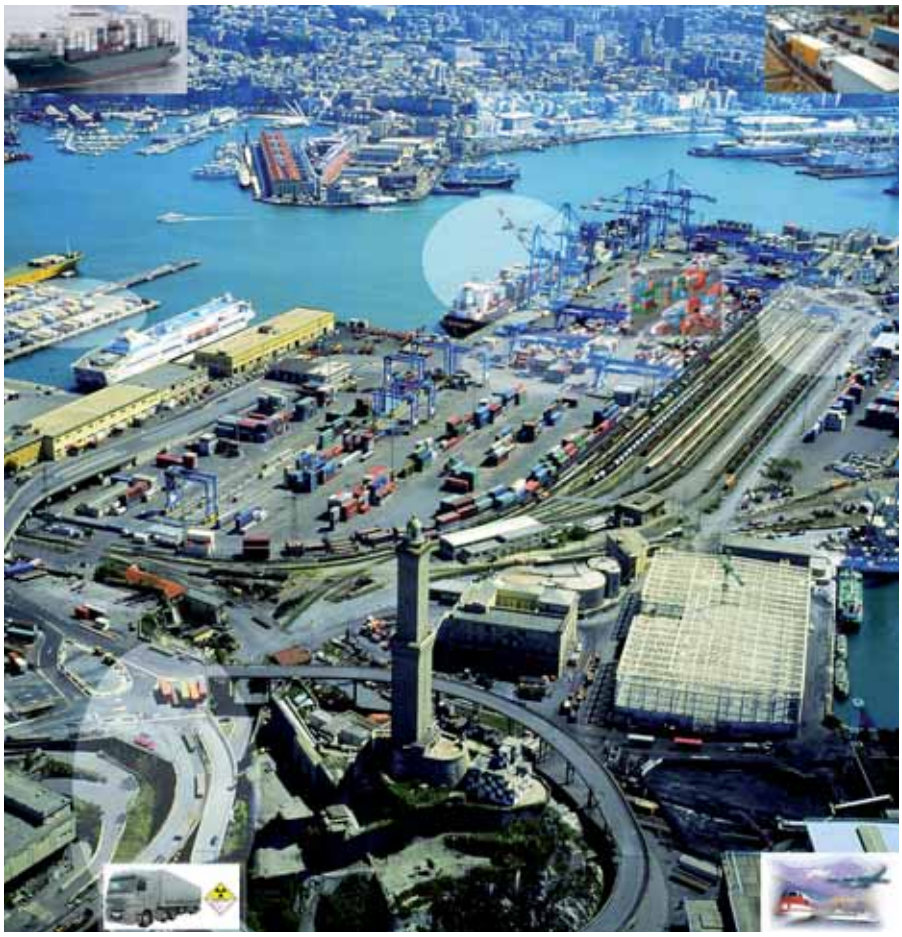
L'obiettivo della ricerca è lo sviluppo e la predisposizione di adeguati piani di sicurezza integrata, comprendenti quindi la sicurezza fisica, logica e procedurale, per gli asset del Sistema elettrico, con particolare riferimento alle centrali di produzione di energia, al fine di garantire la continuità di esercizio.
Il tutto in una visione di crescente penetrazione delle tecnologie ICT nei sistemi di controllo e gestione (SCADA) del Sistema elettrico e la conseguente necessità di essere progettati, installati, operati e mantenuti per resistere a un intenzionale *cyber assault* senza perdere alcuna funzione vitale.

Le principali capability da sviluppare sono:

3. Sicurezza del trasporto multimodale

Introduzione

L'incremento della mobilità in Europa ed in Italia e la sempre maggiore integrazione di diverse tipologie di trasporto, rendono il sistema più fragile e complesso, generando scenari sensibili a possibili azioni dolose e terroristiche.
L'obiettivo della ricerca è quello di sviluppare nuovi servizi e tecnologie per assicurare un'efficiente gestione della mobilità delle persone e delle merci, rendendola oltre che più razionale, informatizzata, efficiente, anche più protetta e sicura. La ricerca sarà inoltre finalizzata allo sviluppo di piattaforme tecnologiche innovative a supporto dei trasporti collettivi per una gestione integrata della sicurezza del trasporto multimodale/co-modale.



SOTTOTEMATICHE DI RICERCA:

Sviluppo di sistemi innovativi, elettronici, fisici e ICT per aumentare l'affidabilità e la cooperazione dei sistemi di trasporto multimodale

L'attività ha lo scopo di analizzare e sviluppare gli aspetti legati alle tecnologie e alla gestione delle infrastrutture di trasporto, al fine di delineare al meglio l'affidabilità dei sistemi, la gestione dei dati e favorire gli automatismi che permettano di realizzare un sistema tecnologico di trasporto multimodale capace di garantire elevati livelli di qualità e di sostenibilità.

Trasporto multimodale merci, incluse le merci pericolose: tendere ad un processo continuo

La razionalizzazione del trasporto delle merci e la relativa logistica comporta un'alta concentrazione di traffici e il ricorso alla ferrovia e a varie forme di intermodalità. L'obiettivo della ricerca è quello di definire i processi cooperanti al trasporto multimodale (Infrastrutture e Supply chain) attraverso l'utilizzo delle tecnologie più appropriate ai fini della sicurezza e della valutazione del rischio, considerando anche la gestione ed il controllo di merci pericolose.

Sensori anti-Intrusione e per la tracciabilità dei container

La tracciabilità e la messa in sicurezza dei container rappresenta uno degli ambiti principali di attenzione per la sicurezza Nazionale e Internazionale. Il processo di tracciabilità è ad oggi complesso ed articolato anche per la diversità di piattaforme tecnologiche e logistiche impiegate nel trasporto multimodale delle merci. L'azione di ricerca è volta pertanto alla definizione di un'architettura, dei protocolli e delle infrastrutture tecnologiche ed

informatiche atte a garantire l'individuazione rapida del container e la certezza e l'integrità delle merci trasportate in ogni momento ed in ogni fase del trasporto di tipo multimodale.

Monitoraggio dello stato del guidatore (livello di attenzione)

Nell'ambito della sicurezza trasporto multimodale di persone e merci, l'identificazione sicura e lo stato del conducente dei mezzi, nonché le sue capacità di condurre una guida sicura, rappresentano tematiche che richiedono notevole attenzione per la criticità delle conseguenze che potrebbero verificarsi sia in caso di comportamenti di guida inadeguati a garantire il livello di sicurezza richiesto per la missione (es. trasporto sostanze tossiche o merci pericolose), sia in caso di azioni criminali o terroristiche mirate in primo luogo al conducente stesso. Il principale obiettivo dell'azione di ricerca è quello di prevenire o ridurre i rischi del trasporto legati a potenziali incidenti (accidentali o conseguenti ad atti di terrorismo o di criminalità) dovuti alle condizioni di guida e allo stato psico-fisico del conducente (ad esempio dolosamente alterato), che potrebbero generare scenari critici per la sicurezza e l'incolumità dei cittadini (es. trasporto di sostanze tossiche, inquinanti, infiammabili,...).

Le principali capability da sviluppare sono:

4. Sicurezza del trasporto su strada

Introduzione

Il trasporto su strada, per dimensione e problematiche di controllo, costituisce un ambito di ricerca rilevante per la sicurezza, rappresentando un settore essenziale per garantire la gestione delle crisi oltre che, allo stesso tempo, uno scenario sensibile.

Gli obiettivi di ricerca individuati mirano principalmente a:

- sviluppare soluzioni tecnologiche e sistemi innovativi per la prevenzione e la sicurezza del trasporto su strada e, in generale a supporto delle esigenze dei vari settori, attraverso la realizzazione di:
  - tecnologie per la sicurezza dei trasporti e dell'infrastruttura stradale,
  - strumenti a supporto del monitoraggio e controllo di aree o obiettivi sensibili,
  - soluzioni finalizzate ad assicurare una tempestiva mitigazione della portata e durata delle situazioni di emergenza;
- sviluppare un sistema nazionale per l'erogazione di servizi di sicurezza stradale ai cittadini in movimento, basati sulla cooperazione veicoli-infrastruttura.

SOTTOTEMATICHE DI RICERCA:

Sistemi e tecnologie di sicurezza per i veicoli

L'azione di ricerca sui sistemi e tecnologie di sicurezza per i veicoli riguarda lo sviluppo di sistemi e tecnologie innovative finalizzate a:

- accrescere le misure di prevenzione contro atti di terrorismo o di criminalità inerenti il trasporto su strada, riducendo i rischi di potenziali scenari sensibili e la possibile portata delle situazioni di emergenza;

- garantire mezzi per la tempestività ed efficacia di intervento nella gestione delle situazioni di emergenza.

Veicoli speciali per il presidio diffuso della sicurezza della popolazione e dell'ambiente

L'azione di ricerca in tale ambito riguarda trasversalmente diversi domini di applicazione in ambito sicurezza e protezione civile, per la prevenzione di attacchi terroristici e/o la mitigazione e gestione delle eventuali crisi, puntando a soluzioni che facilitino la capillarità diffusa del presidio sul territorio e garantendo al tempo stesso flessibilità ed adattabilità di utilizzo, in funzione delle esigenze operative e delle aree individuate a rischio.
La ricerca risponde all'esigenza di accrescere la sicurezza dei confini, delle aree o scenari sensibili, a tutela dell'incolumità e della salute della popolazione, della preservazione dell'ambiente e dell'integrità dei beni materiali, assicurando nel contempo la continuità nell'erogazione di servizi di pubblica utilità e delle reti infrastrutturali.

Sistemi e Tecnologie per la Sicurezza dell'Infrastruttura stradale

La ricerca in tale ambito mira a sviluppare, attraverso tecniche non distruttive (NDT), sistemi e metodologie per l'analisi in tempo reale dell'infrastruttura stradale, ai fini della sicurezza della circolazione in seguito ad atti di terrorismo, atti vandalici, o eventi naturali.

Monitoraggio e Controllo del Traffico in Itinere

La ricerca risponde all'esigenza di gestire in sicurezza il trasporto stradale mediante un sistema di monitoraggio basato su un data fusion di sensori e di procedure atte al controllo e alla gestione del flusso veicolare, al fine di garantire un intervento rapido nel caso di eventi a rischio per l'anti intrusione e l'incolumità di pedoni,edifici e conducenti.

Le principali capability da sviluppare sono:

5. ICT per la sicurezza

Introduzione

Le tecnologie ICT hanno ormai assunto un ruolo pervasivo nella vita quotidiana, non solo relativamente ad attività strettamente pertinenti alle comunicazioni ed all'elaborazione dell'informazione, ma anche e soprattutto in una vasta gamma di domini applicativi, dalla gestione delle infrastrutture critiche (reti di distribuzione di energia, infrastrutture di telecomunicazione, reti di trasporto, etc.) alla fornitura di servizi, alle aziende ed al cittadino (*e-procurement, e-government, e-health*, etc.). Contestualmente, si sono anche accentuati i problemi di sicurezza relativi sia a malfunzionamenti che ad attacchi di tipo intenzionale ai sistemi ICT. Basti pensare che società specializzate nella sicurezza informatica - come ad esempio McAfee nel report "*Night Dragon*", pubblicato a Febbraio 2011 - segnalano che è in corso, in tutto il mondo, una drammatica escalation dei "*cyber-attacks*" contro le multinazionali del settore petrolchimico, energetico e petrolifero. Appare quindi evidente che la protezione efficace ed efficiente delle risorse strategiche, sia materiali che immateriali, passi innanzitutto attraverso l'impiego di strumenti e tecniche che mettano le tecnologie ICT al servizio della sicurezza. L'obiettivo finale è quindi quello della realizzazione di una infrastruttura ICT fidata, che consenta la raccolta di dati da sorgenti multiple ed eterogenee, la trasmissione degli stessi su infrastrutture di connessione sicure ed affidabili, l'elaborazione dei dati in tempo reale, la correlazione delle varie fonti di informazione mediante tecniche sofisticate, la generazione di allarmi in corrispondenza dell'identificazione di eventi potenzialmente pericolosi ed il filtraggio automatico (ed il ranking) dei segnali di allarme.

SOTTOTEMATICHE DI RICERCA:

Sistemi di accesso

L' obiettivo della ricerca riguarda la sicurezza dell'intero ciclo del processo per l'accesso informatico a un sistema ICT. Questo processo concerne l'autenticazione, l'autorizzazione e la profilazione per le persone singole o i gruppi, gli oggetti fisici, le entità, le istanze informatiche e le applicazioni. Per implementare questo processo, si ricorre a tecnologie ICT di accesso che garantiscono sia la sicurezza nel mondo reale (varchi, etc.) sia in quello virtuale (*e-Government*, etc.).

Sicurezza delle reti da attacchi e intrusioni

L'obiettivo della ricerca ha lo scopo di rendere maggiormente resiliente e sicuro il sistema interconnesso delle reti critiche nazionali e le singole infrastrutture. Tipicamente, ciò si ottiene mediante un *enforcement* delle difese perimetrali utilizzando sia sistemi passivi (*firewall*) che attivi (*intrusion detection and prevention*), nonché mediante l'evoluzione delle tecnologie per la progettazione dei protocolli e dei servizi di rete e, parallelamente, tramite il monitoraggio dello stato della rete e del traffico. Inoltre, questo può avvenire tramite l'implementazione di meccanismi per la sicurezza intrinseca dei sistemi non presidiati e la realizzazione di reti per comunicazioni sicure. Il controllo e la prevenzione delle intrusioni delle reti ICT sono di fondamentale importanza perché su queste si basano molti altri aspetti vitali della moderna società. A scopo preventivo e investigativo ricopre particolare interesse la tematica della *lawful interception*.

Information management su sistemi ad alte prestazioni

L' obiettivo della ricerca riguarda lo sviluppo di tecnologie per l'Information Management, anche basate su piattaforme ad alte prestazioni, per garantire la sicurezza globale dei cittadini. Queste tecnologie devono contribuire ad accrescere la sicurezza in vari contesti, compresi la protezione dei sistemi ICT, delle infrastrutture critiche e dei beni. Le tecnologie sviluppate offriranno un insieme di strumenti a supporto del processo per la sicurezza composto di tre fasi: pianificazione, controllo, reazione. In quest'ambito vi è anche notevole spazio per le tecnologie per la raccolta di flussi d'informazioni, acquisiti ad esempio tramite strumenti di videosorveglianza.

Studio e sviluppo di sistemi per la gestione della crisi
L'obiettivo della ricerca è indirizzato allo studio di sistemi per migliorare la funzionalità e gli interventi in situazioni di crisi, in vari contesti.

Le principali capability da sviluppare sono:

TA1.5 Sensori per il monitoraggio delle infrastrutture di produzione di energia e delle reti di distribuzione	Pag.48
TA2.10 Sicurezza di Rete	Pag.65
TA3.2 Sviluppo dei sistemi di monitoraggio diretto (sensori,…) / indiretto (comandi primari/ secondari del veicolo) e monitoraggio in remoto dei parametri dello stato del guidatore	Pag.69
TA3.3 Individuazione di eventi anomali basata sull'analisi integrata di misure ambientali, comportamentali e fisiologiche, incluse le biometriche	Pag.70
TA3.4 Check-point biometrico del futuro con auto accreditamento passeggeri	Pag.71
TA3.5 Soluzioni che individuano minacce collegate ai conducenti di mezzi di trasporto pubblico	Pag.72
TA3.6 Soluzioni robuste e efficienti per interoperabilità tra sistemi di gestione dell'identità elettronica e dell'autenticazione multi-biometrica nel dominio sia fisico che logico	Pag.73
TA5.2 Sistemi ICT sicuri e resistenti agli attacchi (sicurezza del dato)	Pag.85
TA5.3 Piattaforme, architetture ed algoritmi per l'analisi in tempo reale di grandi volumi di dati (high performance computing)	Pag.86
TA5.4 Metodologie e sistemi per il monitoraggio di grandi architetture di rete ICT al fine di detettare anomalie, tentativi di accesso non autorizzato, incidenti	Pag.87
TA6.3 Piattaforme multisensori intelligenti per la riduzione dei falsi allarmi nel monitoraggio di bio-hazard	Pag.93

6. Sicurezza dei confini

Introduzione

La crescita di capacità dei sistemi finalizzati alla sicurezza dei confini nazionali è un tema particolarmente rilevante nel contesto della *Homeland Security*. I rischi connessi da tenere in considerazione a questo riguardo sono di varia tipologia: essi riguardano l'immigrazione clandestina, l'attacco/sequestro criminale di mezzi di trasporto, attentati e azioni terroristiche, azioni di rapina di merci trasportate, nonché quelli derivanti dal trasporto-rilascio irregolare di merci pericolose o a particolare rischio di inquinamento ambientale, così come dal traffico illegale di merci.

La sicurezza in questo ambito è quindi da riferire all'insieme dei confini marittimi, terrestri e aerei nazionali, con gli specifici requisiti che per essi singolarmente si pongono. Le capacità di controllo sono ricercate essenzialmente con riferimento all'entrata nello spazio nazionale di persone, merci e relativi mezzi di trasporto. Tali capacità sono da ricercarsi anche in contigui spazi internazionali (marittimi e aerei) sia per i rischi di diretto interesse nazionale per i trasporti in tali spazi, sia per i rischi anticipabili sullo spazio nazionale per connessi transiti in entrata dei suoi confini. Il controllo di tali spazi internazionali impone anche una crescente specifica cooperazione tra sistemi e organizzazioni di Stati diversi.
Il supporto sempre più incisivo per la sicurezza dei confini è da collegare anche a specifiche evoluzioni della gestione della sicurezza presso i varchi transfrontalieri terrestri nazionali per i vari tipi di trasporto (aeroporti, porti, varchi ferroviari, varchi stradali).
La crescita della sicurezza dei confini implica la necessità di un'evoluzione spinta a livello tecnologico e sistemistico, nonché organizzativo.

SOTTOTEMATICHE DI RICERCA:

Sistemi di sorveglianza Integrata per il monitoraggio terrestre e aereo

Per il contesto aereo le esigenze e evoluzioni prospettate sono primariamente da inquadrare in piani per la sicurezza a livello internazionale. Specifiche connessioni a livello nazionale emergono con i sistemi di sicurezza degli aeroporti. Una minaccia potenziale per il territorio nazionale può essere rappresentata da piccoli aeromobili utilizzati per atti terroristici cercando di superare i correnti dispositivi di sorveglianza aerea civile e militare.
Questo scenario, inerente l'ambito aereo dei confini, è da considerarsi a "priorità medio-alta" dal punto di vista nazionale. Per il contesto terrestre la sicurezza dei confini si esplicita in prima istanza nella possibilità di controllare i punti nevralgici (dogane, porti, varchi transfrontalieri stradali, stazioni e varchi transfrontalieri internazionali) con le applicazioni di controllo del territorio.
Ulteriore esigenza è la sorveglianza dell'intero perimetro frontaliero territoriale italiano per il contenimento di attività illegali (traffico droga / immigrazione clandestina). La complessità che deriva da questa esigenza è mitigata dal fatto che la relativa sorveglianza è da ricondurre a una dimensione di appartenenza alla E.U. Questo scenario, inerente l'ambito terrestre dei confini, è da considerare a priorità medio-alta dal punto di vista nazionale.

Sorveglianza dei confini marittimi

Per quanto attiene alla sorveglianza dei confini marittimi, considerando la rilevante estensione costiera italiana e la posizione particolare del paese all'interno del quadro Mediterraneo, si ritiene che essa sia meritoria (priorità alta) dei principali approfondimenti relativi a questa tematica.
La sorveglianza di un confine marittimo così esteso richiede la conoscenza della situazione su un'area di mare estesa praticamente all'intero Mediterraneo per poter operare in modo tempestivo tenendo conto del quadro di riferimento complessivo. Conseguentemente l'obiettivo principale in questo ambito è l'integrazione, in un quadro coerente, di tutti i sistemi di sorveglianza marittima attualmente operanti nel territorio italiano. Merita comunque sottolineare che lo sviluppo delle capabilities generalmente prefigurate, pur se coltivate per l'ambito marittimo, possono essere valorizzate per la loro ampia riusabilità anche negli altri contesti (terrestre, aereo).

Le principali capability da sviluppare sono:

7.Sicurezza aeroportuale

Introduzione

L'obiettivo di questo settore di ricerca è lo sviluppo di soluzioni (sistemi, tecnologie e organizzazioni) atte a migliorare le capacità di sorveglianza di un moderno sistema aeroportuale per aumentare i livelli di sicurezza (security) e migliorare i servizi disponibili ai passeggeri. Il tutto deve essere realizzato mantenendo un adeguato livello di servizio offerto ai passeggeri: check-in veloce, controllo automatico dei bagagli e delle persone svolto in maniera rapida, non invasiva ed a costi sostenibili per gli operatori della sicurezza.

Gli aeroporti rappresentano i punti di ingresso e di uscita al/dal territorio nazionale. Considerando e riconoscendo l'importanza ed il valore degli attuali strumenti normativi e tecnologici, le sfide poste dalla necessità di mobilità dei cittadini e la continua evoluzione delle minacce alla sicurezza aeroportuale, richiedono un approccio integrato fra l'industria, gli operatori della sicurezza ed i vari enti governativi coinvolti.

L'obiettivo principale di questo tema è la valutazione delle necessità di ricerca per affrontare, in un quadro coerente, tutti i aspetti relativi al presidio in sicurezza delle infrastrutture, dei perimetri aeroportuali e dei passeggeri.

I principali asset aeroportuali da prendere in considerazione sono:

- gli aeroplani
- le infrastrutture informatiche e di comunicazione, ripartite in:
  - servizi passeggeri
  - servizi dedicati al personale dell'aeroporto
  - sistemi per il controllo del movimento degli aeroplani a terra
  - sistemi di telecomunicazione
- le infrastrutture aeroportuali, ripartite in:
  - aree 'air side'
  - aree 'land side' esterne ed interne
  - infrastruttura di trasporto adiacente

Tutti questi asset devono essere analizzati per la loro sensibilità alle possibili minacce che comprendono:

- attacchi contro l'integrità delle reti di comunicazione
- attacchi contro i sistemi di gestione del personale e dell'informazione
- incursioni non autorizzate nelle aree riservate ('sterili') e protette
- attacchi con sostanze chimiche, biologiche, radiologiche, nucleare ed esplosive (NBCRE)
- attacchi contro le infrastrutture con mezzi pilotati o non pilotati da terra ed dall'aria.

Particolare attenzione andrà anche posta agli aspetti legati alle normative e alle procedure, al fine di supportare il necessario coordinamento tra le amministrazioni e le agenzie competenti a livello nazionale ed internazionale.

SOTTOTEMATICHE DI RICERCA:

Controllo dei bagagli e delle persone, inclusi sistemi biometrici

L'obiettivo della ricerca è di sviluppare tecnologie e sistemi innovativi per velocizzare e rendere maggiormente automatizzate e affidabili le operazioni di controllo dei bagagli e dei passeggeri.

Acquisizione e gestione dei dati biometrici

L' obiettivo della ricerca è di sviluppare e integrare nuovi sistemi basati su tecnologie biometriche per il riconoscimento e l'autenticazione delle persone su scala locale ed allargata alle procedure di espatrio.

Sicurezza ATM

L'obiettivo della ricerca è lo sviluppo di sistemi, tool e tecnologie per migliorare la sicurezza (*security*) dei sistemi gestione del traffico aereo, in modalità gate-to-gate, contro le minacce antropiche.

Protezione piazzali ed edifici aeroportuali

L'obiettivo della ricerca è lo sviluppo di sistemi, tool e tecnologie per migliorare la sicurezza (*security*) nel sedime aeroportuale per la gestione della movimentazione degli aeromobili e dei veicoli di supporto e di sicurezza.

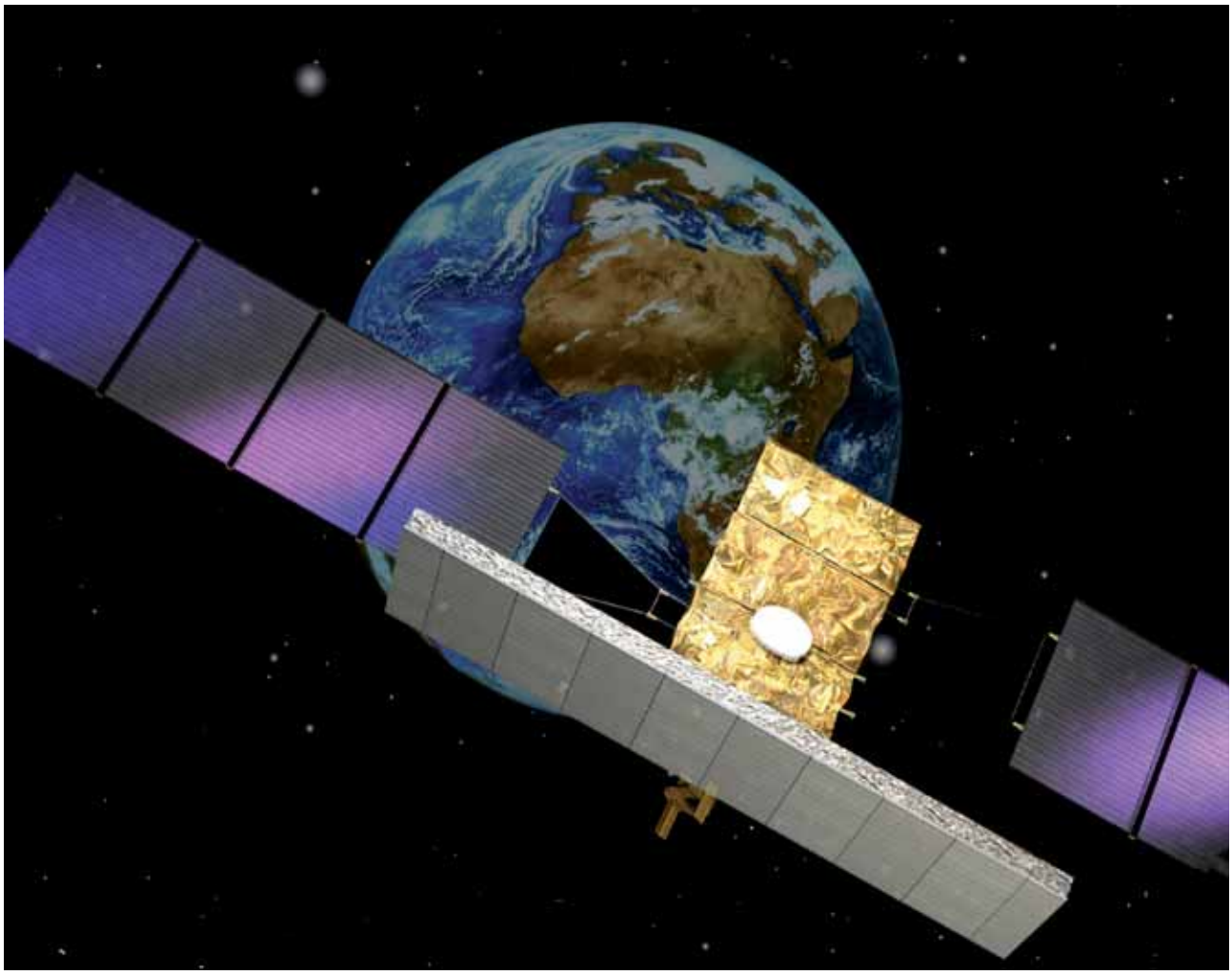
Le principali capability da sviluppare sono:

TA1.7 Sistemi di sorveglianza perimetrale	Pag.50
TA3.1 Detection ed imaging di persone e oggetti attraverso gli ostacoli (fuoco, muri, smog, metalli e altro)	Pag.68
TA3.2 Sviluppo dei sistemi di monitoraggio diretto (sensori,…) / indiretto (comandi primari/ secondari del veicolo) e monitoraggio in remoto dei parametri dello stato del guidatore	Pag.69
TA3.3 Individuazione di eventi anomali basata sull'analisi integrata di misure ambientali, comportamentali e fisiologiche, incluse le biometriche	Pag.70
TA3.4 Check-point biometrico del futuro con auto accreditamento passeggeri	Pag.71
TA6.1 Sensori di elevata sensibilità per la rivelazione di composti in tracce (esplosivi, droghe, chimici, biologici, veleni, e loro precursori) per apparati fissi o mobili	Pag.91
TA6.2 Sensori per monitoraggio a distanza di pericoli chimici e biologici da postazione mobile o fissa	Pag.92
TA6.6 Tecnologie di scansione rapida, da onde millimetriche a raggi X, per la ricostruzione di immagini e rivelare pericoli da postazione fissa al fine di rilevare esplosivi ed altri materiali pericolosi	Pag.96
TA6.7 Nanotecnolgie per sistemi in spettrometria di massa: applicazioni nella rivelazione di esplosivi, droghe (metaboliti e impurezze).	Pag.97
TA6.8 Strumenti compatti ed efficienti per la rivelazione di parti metalliche di armi e munizioni o detonatori	Pag.98

8.Tecnologie satellitari per il controllo del territorio e dell'ambiente

Introduzione

Negli ultimi anni il ruolo delle tecnologie satellitari ha assunto sempre maggiore importanza. Il satellite sfruttando le funzionalità acquisite nel campo delle Comunicazioni, dell'Osservazione della Terra e della Navigazione, è in grado di fornire servizi complementari a quelli terrestri sia per il controllo del territorio e l'ambiente che per



la gestione delle infrastrutture critiche (in quest'ultimo caso sia in situazioni normali sia quando queste operano in condizioni di crisi). Le recenti catastrofi naturali (uragano Katrina, Tsunami ed altri ancora) così come gli attacchi terroristici (quali l'attacco WTC o Mumbai) hanno evidenziato la necessità di un'adeguata gestione del periodo immediatamente successivo all'accadimento dell'evento. In particolare, è necessario attivare specifiche soluzioni in grado di gestire le operazioni di soccorso e permettere la continuità delle attività di business nonostante le distruzioni generate dall'evento disastroso. Il ruolo della tecnologia satellitare inteso nel molteplice aspetto di comunicazione, navigazione e Osservazione della Terra, è la soluzione chiave per supportare in maniera efficace le operazioni di emergenza (si veda ad esempio il supporto fornito dai satelliti tra cui quelli della costellazione COSMO/SKYMED in occasione del terremoto dell'Abruzzo) e di continuità del business, così come la fase di prevenzione e monitoraggio. È fondamentale indirizzare queste soluzioni non solo in casi di situazioni di emergenza, ma nel complesso dell'economia nazionale ed internazionale, considerando che infrastrutture critiche spesso dipendono profondamente dai servizi satellitari. Non va infine dimenticato che ulteriori servizi offerti dal sistema satellitare sono la localizzazione e la sincronizzazione temporale, servizi questi sempre più spesso utilizzati anche nella gestione di molteplici infrastrutture critiche.

SOTTOTEMATICHE DI RICERCA:

Tecnologie abilitanti per il settore spaziale

Uno degli obiettivi di maggior rilievo delle tecnologie per satelliti di nuova generazione è, insieme alle funzioni di osservazione e sorveglianza, lo sviluppo di soluzioni che puntino ad una sensibile riduzione di masse e consumi, guidati da una maggiore integrazione funzionale tra payload e bus. Questo trend evolutivo consentirà una riduzione degli apparati di bordo rispetto ai prodotti esistenti che svolgono a bordo del satellite funzioni simili. Le tecnologie per questi satelliti di nuova generazione sono rivolte ad un massimo utilizzo degli elevati investimenti nazionali per l'accesso allo spazio, realizzati con il lanciatore VEGA, e di aprire possibilità anche per il mercato commerciale di export offrendo prodotti nazionali più competitivi e che consentano elevati risparmi per l'utente finale e ritorno (tecnologico, occupazionale, etc) per il sistema paese Italia. Per quanto riguarda lo sviluppo di nuove tecnologie rivolte a migliorare notevolmente i tempi di rivisita di costellazioni di satelliti con masse e consumi ridotti esiste una notevole capacità e competenza nazionale nel settore, grazie soprattutto all'esperienza maturata con il progetto COSMO SkyMed e GALILEO.
Studi sul volo in formazione di satelliti (di varie gamme dimensionali inclusi mini e micro), analisi dei sistemi di comunicazione e controllo per la gestione della costellazione durante il volo (ad esempio la posizione ed il sincronismo), tecnologie per lo scambio dei dati tra i satelliti in formazione e terra, trasmissioni di elevate moli di dati osservati via DRS, sono solo alcune delle tematiche che l'industria italiana è in grado di affrontare e che risulteranno cruciali ai fini della competitività in ambito internazionale.

Monitoraggio Ambientale

L'obiettivo della ricerca è di sviluppare metodologie e servizi atti a fornire informazioni a supporto della riduzione di rischi ambientali e della loro prevenzione.

Tecnologie per la protezione dei sistemi di comunicazione satellitare, a supporto dell'infrastruttura terrestre e di applicazioni evolute (e.g. UAV)

L'obiettivo è di sviluppare nuove tecnologie per sistemi di comunicazione satellitari duali, flessibili, complementari e integrabili con l'infrastruttura wireless e terrestre, in grado di offrire la gestione operativa di possibili situazioni di crisi, garantire in maniera continuativa il controllo dei confini, aumentare il livello di sicurezza dei cittadini, assicurare il coordinamento degli interventi in zone di rischio (*peace keeping*). Attualmente i profili di protezione dei sistemi spaziali ad uso civile, in mancanza di stringenti requisiti di sicurezza ed un ovvio contenimento dei costi, non sono stati pienamente implementati i livelli di protezione adeguati a tutela di minacce di tipo intrusivo. Odiernamente i livelli di sicurezza per applicazioni unicamente civili sono limitati dai vincoli di Sicurezza Nazionale, mentre nei sistemi spaziali per applicazioni duali di ultima generazione sono stati implementati elevati livelli di sicurezza. Per esigenze sempre più pressanti di "*Security of Space*" dove l'infrastruttura spaziale sta configurandosi come infrastruttura critica, è di vitale importanza estendere anche al mondo dei sistemi spaziali per applicazioni civili questo tipo di protezione dei canali di comunicazione.
L'obiettivo sarà perseguito attuando una serie di attività che mirano al raggiungimento di una piena integrazione dei sistemi satellitari di Comunicazioni e di Navigazione con l'infrastruttura terrestre. In diversi ambiti civili sta crescendo sempre di più l'esigenza di poter comunicare efficacemente scambiando dati acquisiti ed informazioni nelle condizioni più diverse al fine di gestire situazioni di crisi o aver la possibilità di poter sorvegliare il territorio più efficacemente di quanto oggi non si faccia, riducendo drasticamente il rischio per la vita umana (i piloti di mezzi aerei che devono spegner incendi, sorvolare zone terremotate, sorvegliare le coste, ecc) e i costi.
Tale esigenza può essere soddisfatta solo se si riesce a disporre di infrastrutture di comunicazione particolari basate su accesso satellitare da far operare in situazioni e contesti altrettanto particolari, come può essere uno scenario di crisi quali una zona terremotata, dissestata geologicamente o semplicemente poter sorvegliare in maniera più continuativa un territorio ben specifico ed esteso.
L'introduzione di veicoli aerei senza pilota o Unmanned Aerial Vehicle (UAV) è stata la prima e significativa risposta all'esigenza su descritta. Già in ambito militare tali velivoli senza pilota hanno conosciuto una sensibile evoluzione tecnologica che li rende oggi, in quanto a manovrabilità ed efficienza, simili ad aerei con pilota.

L'Italia è tra le Nazioni che, con la sua industria aeronautica stanno proponendo nuovi modelli di UAV per varie applicazioni sia militari che civili mirate, quest'ultime, all'utilizzo da parte della Protezione Civile Nazionale o di altri Enti preposti alla gestione di crisi o semplicemente a compiti di sorveglianza.

Le principali capability da sviluppare sono:

9. Sicurezza nel Costruito

Introduzione

Assicurare la sicurezza nel costruito rappresenta un'esigenza dal tremendo impatto sociale, come recentemente testimoniato dall'evento sismico del 6 Aprile 2009 in Abruzzo. Tale esigenza assume un carattere ambivalente, dal momento che riguarda sia la Safety (rischio legato ad eventi naturali) che la Security (eventi terroristici), e necessita di una risposta estremamente variegata in funzione sia dell'eterogeneità dei rischi naturali (simico,

idrogeologico,..) ed antropici, che del suo impatto nelle diverse fasi di vita del costruito. In particolare, da un punto di vista delle tecnologie di osservazione e *sensing*, è di primaria importanza assicurare un monitoraggio *long-term* della struttura ai fini di una corretta manutenzione e programmazione degli interventi di consolidamento. D'altra parte, la necessità di un *quick damage assessment*, a seguito di eventi di crisi, richiede lo sviluppo e l'impiego di tecnologie speditive sia per la valutazione veloce dello stato che per l'identificazione di anomalie nel comportamento dinamico della struttura.

SOTTOTEMATICHE DI RICERCA:

Controlli sugli elementi di un edificio
L'obiettivo della ricerca consiste nel promuovere ed incrementare la sicurezza del costruito attraverso verifiche e controlli degli edifici per il mantenimento in efficienza, la prevenzione contro i rischi naturali (sismi, frane..) ed antropici, la costruzione di modelli dinamici delle strutture, la gestione delle situazioni di crisi a valle di attacchi terroristici e disastri naturali. Risulta importante assicurare una diagnosi preventiva per analizzare le

problematiche inerenti ad una inadeguata progettazione ed ottenere informazioni sia sulle modalità costruttive che sullo stato di degrado della struttura, dovuto anche al suo normale invecchiamento. In tale ambito, il controllo ai fini della verifica delle condizioni di sicurezza ed integrità di strutture civili (edifici, ponti, etc.), sia in fase d'opera che nel costruito, ed il monitoraggio sia dei movimenti delle strutture che delle deformazioni del territorio circostante rivestono carattere di necessità, anche ai fini dell'identificazione di modelli del comportamento delle strutture in relazione all'esposizione ai diversi tipi di rischio. Inoltre, la diagnostica risulta importante per la verifica della bontà e dell'efficacia delle operazioni di *reinforcement* e pone sfide interessanti, in termini di attività di ricerca, legate alla necessità di monitorare nuovi materiali (FRP, CAM, SMA).
Inoltre, la necessità di un *quick damage assessment* della struttura, a seguito di un evento di crisi, richiede un'analisi speditiva dello stato e del comportamento dinamico della struttura. Tale esigenza è particolarmente sentita nella fase di gestione della crisi, perché ha impatto sia sulla definizione delle priorità nella programmazione degli interventi, che per la situation awareness riguardante le strutture ed infrastrutture da impiegare nelle fasi immediatamente successive alla crisi.
Risulta di interesse un monitoraggio delle strutture che sia continuo nel tempo, capace anche di una diagnostica veloce e *on-demand* a seguito di situazioni di crisi, multi-sensoriale, multi-scalare (visione globale della struttura e del territorio e diagnostica di dettaglio) multi-risoluzione, multi-profondità con carattere di bassa o nulla invasività. Esso richiede da un lato sistemi avanzati basati su reti wireless e di sensori e dall'altro l'integrazione di tecniche di diagnostica non invasiva basate su *sensing* elettromagnetico e/o acustico.

Sviluppo di nuove tecnologie per la sicurezza degli edifici e degli impianti

L'obiettivo della ricerca riguarda il controllo continuo degli edifici con il duplice fine di evitare danni e malfunzionamenti degli impianti, anche conseguenti ad attacchi terroristici, e fornire inoltre supporto alla gestione delle situazioni di crisi con particolare riferimento alle procedure di evacuazione.

Sistemi di monitoraggio dell'integrità strutturale

L'obiettivo della ricerca è di sviluppare sistemi avanzati basati su reti wireless e di sensori per la verifica delle condizioni di sicurezza ed integrità di strutture civili (edifici, ponti, acquedotti, etc.) sia in fase d'opera che nel costruito, che nelle fasi successive a situazioni di crisi..

Le principali capability da sviluppare sono:

TA1.2 Data Fusion di sensori eterogenei	Pag.45
TA1.3 Elaborazione di immagini satellitari (SAR, ottico) ad alta risoluzione	Pag.46
TA4.2 Analisi della deformazione e dei danni dell'infrastruttura in seguito ad atti terroristici o eventi naturali e loro riabilitazione	Pag.76
TA4.3 Sviluppo di componenti, tecniche e metodologie per lo studio e l'analisi dei rischi sugli edifici e sugli impianti (mappe di vulnerabilità delle aree fruibili, controllo di valori soglia, etc)	Pag.77

10.Sicurezza integrata dei Beni Culturali

Introduzione

I beni culturali rappresentano una ricchezza inestimabile per il nostro Paese per cui tutti gli aspetti legati alla loro sicurezza sia preventiva che nel corso di situazioni critiche costituiscono punti focali di interesse.
Il problema della sicurezza dei beni culturali (beni mobili, immobili, archeologici e naturali) coinvolge problematiche sia di Safety, con riferimento a rischi connessi ad alterazioni ambientali e a calamità naturali (inondazioni, terremoti, frane, incendi), sia di Security a riguardo di danni connessi all'intervento umano su di essi. In generale, in connessione con processi di fruizione vanno garantiti, da un lato, il rispetto di condizioni di valorizzazione di Beni Culturali, con particolare attenzione a esistenza o prospettive di candidature a siti UNESCO, dall'altro, la sicurezza stessa dei visitatori. Cruciale è anche la realizzazione di strumenti per la gestione di situazioni inerenti manomissioni o furti. E' noto, infatti che il Patrimonio culturale, per il valore simbolico che rappresenta per l'identità di un popolo, finisce per essere uno dei primi obiettivi del fenomeno terroristico (ne sono una testimonianza gli attentati contro la Galleria degli Uffizi e la Basilica di S. Giovanni in Laterano).Non meno rilevanti sono per i beni mobili le problematiche connesse a condizioni di movimentazioni e a rischi che si possono determinare durante situazioni di trasporto. Proteggere dei siti di rilevanza per il patrimonio culturale richiede una combinazione di tecniche e pone una serie di sfide tecnologiche rilevanti: sono dunque necessari approcci sistemici unitari e, in particolare, un'integrazione di competenze che consentano l'individuazione di metodologie e tecnologie integrabili, idonee al trattamento di sistemi complessi, come ad esempio le aree archeologiche. Purtroppo, recenti esperienze hanno dimostrato, come non vengano sempre pianificate e adottate tutte le misure preventive necessarie alla protezione di beni culturali: è necessario,dunque, adottare strategie organizzative supportate da elementi tecnologici che consentano di ridurre sensibilmente i rischi.

SOTTOTEMATICHE DI RICERCA:

Controllo e monitoraggio delle opere esposte al pubblico e sicurezza dei visitatori

L'obiettivo della ricerca è la realizzazione di sistemi integrati atti a garantire la sicurezza delle opere esposte (beni mobili, immobili, archeologici e naturali) sia nel corso di movimentazioni, sia da eventuali manomissioni o furti sia da alterazione ambientali legate alla fruizione e a calamità naturali (inondazioni, terremoti, frane, incendi) o guasti improvvisi. Realizzazione di sistemi integrati atti a garantire la sicurezza dei visitatori, nel rispetto della valorizzazione e tutela, mediante rivelazione di situazioni di rischio ambientale sia per le opere esposte che per le opere in custodia, di Beni Culturali e anche ad aumentare la sicurezza della fruizione dei siti di interesse culturale (naturale o di aree archeologiche) mediante l'identificazione individuale e nominativa dei visitatori. In particolare la sicurezza di persone e visitatori di siti archeologici o edifici museali presenta un doppio aspetto: da un lato la sintesi e la messa in opera di tecniche per il riconoscimento automatico di persone, la analisi automatica di scene e l'identificazione di comportamenti potenzialmente maligni tramite analisi di osservazioni connesse temporalmente, ma anche l'approfondimento dei temi legati alla privacy delle persone che visitano un sito di valore culturale che pone problemi in quanto riguarda attività svolte nel tempo libero e/o da turisti provenienti da culture diverse e potenzialmente soggetti a legislazioni diverse.

Sistemi per la gestione integrata e remota della sicurezza

L' obiettivo della ricerca sussiste nel rispondere all'esigenza di Sicurezza riguardante sia il rischio collegato ad eventi dolosi o terroristici sia rischi che si possono determinare durante il trasporto includendo tecnologie dell'informazione per:

- sviluppare la sicurezza dei Beni Culturali nelle aree di fruizione e durante il trasporto: tracciabilità e monitoraggio della visita, gestione integrata nell'ambito di Piani di Emergenza (identificazione di oggetti e procedure per l'evacuazione di emergenza);
- realizzare il monitoraggio continuo per la mitigazione del rischio durante il trasporto di emergenza;
- supportare gli aspetti organizzativi: valutazione di impatto, elaborazione di schemi di protezione del patrimonio artistico mobile.

Gestione delle emergenze in caso di atti criminosi e disastri

L'obiettivo della ricerca è relativo allo sviluppo di tecniche per gestire in maniera efficace l'intervento sui luoghi di crisi in modo da evitare di danneggiare permanentemente la futura possibilità di eseguire restauri. La questione focale riguarda, da un lato, lo studio di strumenti, ad esempio robotici, per interventi mirati, dall'altro, la capacità di monitoraggio dinamico degli interventi e il relativo adattamento delle procedure e piani di intervento in caso di eventuale pericolo. Inoltre, nei casi in cui i processi di evoluzione degli scenari di crisi prevedano processi a tempistica monitorabile (ci riferiamo ad eventi come incendi, allagamenti, frane), si può far ricorso a tecnologie innovative per osservare in tempo reale l'evoluzione dei fenomeni, utilizzare tecniche predittive/simulative veloci e predisporre piani di intervento adeguati). Segnaliamo, infine, su questo aspetto gestionale della crisi la rilevanza degli aspetti di *training*. Anche in questo caso si segnala la possibilità di interventi trasversali (es., i vigili del fuoco intervengono non solo in un museo o in una chiesa ma anche in una abitazione civile) ma può essere preso in considerazione data la rilevanza del nostro paese la predisposizione di strumenti di addestramento mirati ad allenare le specificità dell'intervento in una area di interesse culturale (es., vecchi edifici, perdita di reperti, possibilità di furti, etc.). Poiché l'addestramento carta e penna ha efficacia limitata e le esercitazioni sul campo sono estremamente costose e difficili da allestire in modo realistico può essere importante valutare l'efficacia di strumenti software ad immersione totale e predisporre ambienti virtuali o di gioco serio che sfruttano tecniche ICT innovative (addestramento tramite "*serious games*").

Le principali capability da sviluppare sono:

TA1.1 Analisi integrate per rilevamento di comportamenti anomali (analisi per immagini / analisi varie), sensori per la generazione di Early Warning	Pag.44
TA1.2 Data Fusion di sensori eterogenei	Pag.45
TA 2.2 Reti wireless ad-hoc e di sensori	Pag.57
TA4.2 Analisi della deformazione e dei danni dell'infrastruttura in seguito ad atti terroristici o eventi naturali e loro riabilitazione	Pag.76
TA4.4 Sistemi robotici cooperativi (manned e unmanned) per la valutazione remota e preventiva dell'area interessata dall'evento e l'erogazione delle prime azioni di intervento (Robotic Rescue).	Pag.78
TA4.7 Metodologie e strumenti per l'analisi del rischio e l'ottimizzazione costo/benefici basati su simulazione e modellistica analitica	Pag.81
TA5.5 Realizzazione di algoritmi e processi per l'estrazione automatica e l'elaborazione del contenuto informativo di immagini	Pag.88

11.Sicurezza nucleare

Introduzione

L'interesse attuale per le tecnologie nucleari in numerosi paesi, tra cui anche l'Italia, ha messo in evidenza la necessità di assicurare la massima sicurezza, dal punto di vista della Security,. La parola italiana "Sicurezza" può generare ambiguità poiché si riferisce ai due aspetti di Security e Safety che, specialmente per il settore nucleare, hanno connotati e applicazioni diverse. Sebbene i due temi possano essere, in taluni casi, legati in ambito nucleare, è opportuno chiarire che lo scopo di questa iniziativa è incentrata principalmente sullo sviluppo

di tecnologie atte ad assolvere i compiti relativi alla Security nel quadro delle normative internazionalmente riconosciute. La sicurezza è sempre stata una priorità essenziale nella progettazione, sviluppo ed esercizio delle istallazioni nucleari, includendo non solo le centrali nucleari ma anche tutte le strutture dove vi sia un attività legata alla manipolazione di elementi radioattivi, come ad esempio nei reparti radiologici degli ospedali, nei laboratori di ricerca, nei depositi. Le nuove potenziali minacce della criminalità organizzata e del terrorismo hanno evidenziato l'urgenza di analizzare più nel dettaglio anche i già pure elevati standard di Security di tali installazioni. Ricercare e sviluppare nuovi sistemi e tecnologie per assicurare e incrementare le già pur elevate condizioni Security delle installazioni nucleari è l'obiettivo principale della tematica. Tali mezzi hanno lo scopo di soddisfare principi di protezione adeguati ed impedire che aggressioni esterne possano compromettere i principi stabiliti dalle normative applicabili a livello internazionale.

SOTTOTEMATICHE DI RICERCA:

Sicurezza nella movimentazione e nel trasporto

Il sotto-tema si propone l'obiettivo di analizzare il trasporto e la movimentazione del materiale nucleare riducendo i rischi a fronte di eventi critici intenzionali.
Tale obiettivo verrà perseguito attraverso l'approfondimento delle tematiche relative all'analisi e realizzazione di sistemi per il trasporto di materiale radioattivo e di sistemi di gestione e controllo, eventualmente anche in remoto, dei veicoli di movimentazione e trasporto del materiale nucleare.

Tra i numerosi risultati attesi potranno essere anche studiati, ad esempio, sistemi elettronici di controllo per il trasporto e la movimentazione di materiale nucleare, sistemi per garantire l'idoneo trasporto o la tracciabilità di materiale nucleare.

Sicurezza nello stoccaggio del materiale radioattivo

Il sotto-tema si propone l'obiettivo di definire le caratteristiche di un sistema di protezione fisica e controllo dei residui radioattivi (solidi e liquidi) sia nei siti dove sono prodotti sia in depositi centralizzati definitivi, inclusi quelli geologici per i rifiuti ad alta attività.
L'obiettivo verrà perseguito attraverso lo studio dell'architettura del sistema di Security per le diverse tipologie di rifiuti e di depositi.
I risultati attesi saranno relativi alla definizione delle caratteristiche tecniche principali delle diverse tipologie di deposito, con la verifica dei parametri tecnici da utilizzare per la difesa da atti intenzionali.

Sicurezza negli impianti

Il sotto-tema si propone l'obiettivo di analizzare gli aspetti per una migliorata difesa da aggressioni.
L'obiettivo verrà perseguito attraverso l'approfondimento delle seguenti *tematiche di ricerca*:

- Individuazione delle tecnologie migliori per la rilevazione delle aggressioni
- Caratterizzazione delle informazioni (segnali), utili per la security
- Individuazione delle tecnologie con riferimento ai requisiti già noti relativi alla protezione fisica

I risultati attesi saranno mirati ad individuare le migliori soluzioni tecniche per la protezione e la dissuasione.

Apparecchiature Nucleari per la Sicurezza

L'obiettivo del sotto-tema riguarda la ricerca e sviluppo di nuovi Apparati/Sistemi/Componenti (ASC) che utilizzino e/o rivelino radiazioni ionizzanti.
L'obiettivo verrà perseguito attraverso lo sviluppo di metodi, tecniche e procedure relative a specifiche *tematiche di ricerca* già individuate; tra esse si segnalano:

- Rivelatori per l'individuazione di materiali "sensibili" (U/Pu) che possano essere utilizzati anche senza ispezionare l'impianto dall'interno
- Rivelatori innovativi per condizioni ostili (radiazioni intense, alte temperature, stress meccanici e chimici) atti a monitorare il campo di radiazione,
- Rivelatori per il monitoraggio radiologico di tipo passivo che minimizzino l'impiego umano riducendone la dose associata
- Studio di fattibilità di magneti superconduttori per applicazioni in ambienti ad alta fluenza neutronica.

Le principali capability da sviluppare sono:

TA6.5 Grandi portali di nuova generazione con attivazione neutronica o raggi X per la rivelazione di materiale nucleare o esplosivo dentro i container con l'impiego di rivelatori passivi che operano in ambiente ostile	Pag.95
TA6.9 Strumentazione portatile attiva o passiva per il monitoraggio di materiale radioattivo in discariche o in container commerciali	Pag.99

12.Sicurezza Agroalimentare

Introduzione

Il settore agroalimentare è secondo in Italia per dimensione, dopo il metalmeccanico e primo a livello europeo, seguito dal metalmeccanico; è inoltre il terzo per fatturato nell'Unione Europea, dopo Francia e Germania. Il settore si compone di filiere agroalimentari allineate su una moltitudine di attori che complessivamente occupano 2,5 milioni di addetti, e rappresentando il motore economico e occupazionale più importante del Paese.

L'obiettivo della sicurezza agroalimentare è sviluppare e applicare sistemi atti a garantire l'integrità della filiera ed ad impedire l'alterazione dei cibi lungo la stessa.
Tali sistemi, tecnologicamente avanzati, diventeranno uno strumento di grande importanza a supporto dell'efficacia ed efficienza del sistema di controllo pubblico (es. dogane, NAS, Istituti Ministeriali) nell'attività istituzionale per la garanzia della sicurezza e del benessere del cittadino, del *made in Italy* e delle importazioni di materie prime alimentari.
A tale fine è necessario prevenire le alterazioni indotte non solo da un non corretto *handling* lungo tutta la filiera, ma anche quelle causate da azioni di *tampering* con l'introduzione illegittima di sostanze chimiche, biologiche o radiologiche nel cibo, nonché quelle conseguenti al non corretto funzionamento di altre infrastrutture quali la rete elettrica, i trasporti e le telecomunicazioni.
Tale prevenzione è possibile mediante lo sviluppo di tecnologie atte ad impedire azioni come la manipolazione non autorizzata delle derrate, a permettere la tracciabilità e riconoscibilità delle stesse, a sviluppare capacità

di diagnosi per l'individuazione di sostanze estranee, di rischi dovuti al cambiamento climatico e di evidenze di manipolazione e/o di non corretta conservazione,
Lo sviluppo di tecnologie, strumenti e metodologie in grado di prevenire l'alterazione e le frodi di alimenti protetti da marchi ed indicazioni di origine ha dunque l'obiettivo sia di garantire la sicurezza dei cittadini, tramite la tutela delle filiere alimentari, sia di tutelare il *made in Italy* alimentare.
Le moderne tecnologie possono fornire un fondamentale supporto a tutte le strategie di tutela relative alla sicurezza alimentare, intesa nel suo senso più ampio:

- possibilità di identificare rapidamente (negli alimenti e non solo) la presenza di contaminanti introdotti volontariamente: security,
- possibilità di individuare precocemente organismi e microrganismi alieni in prodotti vegetali o negli alimentari freschi o trasformati, potenziali responsabili di pandemie vegetali, animali o umane: food security,
- capacità di analizzare e quantificare la presenza di contaminanti biotici ed abiotici (tossine, patogeni umani, pesticidi) negli alimenti: food safety.

capacità di prevenire incidenti e di governare l'evento indesiderato verso il contenimento del danno e la minimizzazione dell'impatto: *food security*. Per fronteggiare possibili problemi derivanti da attacchi terroristici o criminali alla filiera agroalimentare è necessario sostenere sì un sistema di controllo, che peraltro già esiste, ma è ancora più strategico per il Paese sviluppare strumenti tecnologici innovativi che permettano di mettere in sicurezza la filiera agroalimentare nel medio-lungo periodo, di dissuadere attentatori e prevenire atti di terrorismo, sabotaggio e criminalità, di garantirne un funzionamento continuo nel tempo, e nel caso di azioni terroristiche, di assicurare una mitigazione degli effetti, una gestione della crisi e un rapido recupero della funzionalità della filiera.

Grazie ad un processo di consultazione con le imprese agroalimentari, i centri di ricerca e le università, nell'ambito della piattaforma SERIT, sono emersi diversi urgenti ambiti di ricerca che, se attivati, avrebbero grande impatto sulla *security* per il settore agroalimentare.

SOTTOTEMATICHE DI RICERCA:

Sicurezza nel trasporto e nei sistemi di logistica avanzata degli alimenti

Le filiere agroalimentari utilizzano infrastrutture fisse e mobili per la produzione alimentare. Il trasporto e la distribuzione degli alimenti richiedono punti di immagazzinamento e smistamento, magazzini, porti, stazioni, e anche mezzi di trasporto diversi. Le filiere comprendono periodi di trasporto con distanze spesso rilevanti (es. frutta, carne, pesce dal Sud America all'Europa) da compiere con aerei, navi, treni, automezzi. Queste fasi costituiscono un punto estremamente critico per la conservazione della catena del freddo, da un lato, e per la possibilità di manipolazione che offrono. Dall'altra parte, le condizioni economiche e il prezzo al mercato dei prodotti non consentono al momento di effettuare controlli approfonditi sulla merce, che porterebbero a inevitabili aumenti di prezzo non sostenibili. Sono quindi richieste nuove soluzioni per aumentare in modo relativamente poco costoso la sicurezza del trasporto, definita come "sicurezza intrinseca" in quanto garantita dal meccanismo stesso, piuttosto che imposta dall'esterno. L' Obiettivo è identificare e progettare nuove soluzioni distributive a "sicurezza intrinseca" per alimenti e derrate, dotati di tecnologie innovative dedicate alla diminuzione del rischio di accesso al prodotto e con sistemi real-time automatizzati di identificazione e controllo delle unità logistiche.

Sensoristica e diagnostica per la determinazione rapida di contaminanti microbiologici, tossine, composti chimici e sostanze pericolose

La prevenzione dei rischi dovrebbe comprendere misure di monitoraggio e di allerta, oltre che prevedere meccanismi in grado di rilevare i pericoli in tempo per prevenire l'attacco (*detect-to-protect*). I dispositivi di rilevamento dovrebbero essere in grado non solo di identificare gli agenti tossici, ma anche di dare l'allarme in caso di un loro ritrovamento/rilascio a livelli pericolosi in modo da attuare tempestivamente adeguate misure correttive ed evitare l'allargamento del pericolo (*detect-to-treat*). Una piattaforma ideale per il rilevamento di sostanze chimiche e biologiche pericolose dovrebbe essere poco costosa e di facile uso, versatile (cioè adattabile ai vari sistemi di diagnosi chimica e biologica per fronteggiare qualsiasi emergenza), multifunzionale

(tale da integrare più processi di analisi in un unico dispositivo), di pronto impiego (portatile e automatizzata) e ad elevato flusso di analisi (*high throughput*). Dovrebbe inoltre avvalersi di sistemi diagnostici rapidi (misure in tempo reale), sensibili, selettivi, precisi e accurati, e tali da permettere l'analisi simultanea di più analiti (*multiplexing*) per un elevato numero di campioni. L' obiettivo è applicazione di biotecnologie, nanotecnologie, e nuovi materiali per la realizzazione di nuovi sistemi sensoristici e di sistemi diagnostici avanzati e rapidi per il controllo e la gestione della sicurezza lungo tutta la filiera agroalimentare (campo/processi/prodotto).

Piattaforme ICT per il governo della sicurezza e dell'integrità della filiera

Quest'area di ricerca dovrà promuovere linee di ricerche in campi avanzati, come l'ICT avanzato e la sensoristica intelligente, in grado di generare innovazioni di processo e di prodotto atti a garantire una maggiore *security* alimentare in ogni fase della catena, partendo dalle materie prime fino al momento del consumo, passando attraverso le fasi di trasformazione, confezionamento e distribuzione. Anche la lotta alle frodi rappresenterà un'area da esplorare al fine di trovare delle soluzioni di contrasto al fenomeno, la cui cifra, fornita dall'Italian Food Sounding, si attesta attorno ai 21 miliardi di dollari, circa dieci volte il valore reale delle esportazioni dall'Italia. Questo indica una forte richiesta da parte del mercato verso il prodotto *Made in Italy*, senza un adeguato supporto di garanzia di originalità e sicurezza da parte dei produttori. L' obiettivo è lo sviluppo di nuove piattaforme ICT dotate di avanzati sistemi micro- e nanotecnologici per il monitoraggio e controllo di rischi al fine di garantire l'integrità delle filiere agroalimentari lungo tutte le fasi, con particolare riguardo alla prevenzione dei punti di rottura della filiera e alla loro vulnerabilità per azioni dirette e indirette.

Le principali capability da sviluppare sono:

TA4.7 Metodologie e strumenti per l'analisi del rischio e l'ottimizzazione costo/benefici basati su simulazione e modellistica analitica	Pag.81
TA6.1 Sensori di elevata sensibilità per la rivelazione di composti in tracce (esplosivi, droghe, chimici, biologici, veleni, e loro precursori) per apparati fissi o mobili	Pag.91
TA6.3 Piattaforme multisensori intelligenti per la riduzione dei falsi allarmi nel monitoraggio di bio-hazard	Pag.93
TA6.4 Tecnologie microfluidiche accoppiate a nanostrutture molecolari per la detezione di biohazard	Pag.94
TA6.7 Nanotecnolgie per sistemi in spettrometria di massa: applicazioni nella rivelazione di esplosivi, droghe (metaboliti e impurezze).	Pag.97

13. Sicurezza & Salute

L'obiettivo della tematica Sicurezza & Salute, è elaborare strategie e meccanismi per reagire alle minacce di origine dolose o accidentali che possono affliggere i vari tasselli che compongono il sistema Salute per migliorarne l'efficienza e l'efficacia in corrispondenza di emergenze sanitarie, incluse quelle più propriamente

sanitarie. Nel caso di scenario immediatamente successivo al verificarsi di eventi catastrofici (inondazioni, terremoti, attentati ecc) il personale medico e paramedico, operante in condizioni di estremo disagio, deve essere in grado di valutare le condizioni generali dell'infortunato, prestare in loco le prime cure anche mediante il deployment di strutture sanitarie , provvedere nel caso al suo trasferimento presso le strutture che più efficacemente possono prestargli il soccorso necessario.
Durante le emergenze sanitarie (e non) le sale operatorie e le sale sanitarie da campo, vengono classificate come reparti ad alto rischio infettivo in quanto in esse si registrano elevati valori di incidenza di infezione ospedaliera. L'obiettivo da perseguire è orientato verso l'abbattimento della carica microbica ambientale nel suo insieme, verso lo sviluppo di sistemi per migliorare la sicurezza dei pazienti nei trattamenti terapeutici e chirurgici, includendo le capacità di deployment e di prestazioni sanitarie da campo.

SOTTOTEMATICHE DI RICERCA:

Emergenze Sanitarie

In uno scenario di emergenza sanitaria i problemi che il personale medico deve affrontare sono molteplici e varie: a) rendere il paziente identificabile in maniera certa da parte del personale incaricato del suo trasferimento; b) rendere il paziente localizzabile in maniera rapida da parte dello stesso personale; c) rendere le informazioni relative allo stato generale del paziente disponibili al personale medico della struttura di destinazione; d) rendere le stesse informazioni disponibili in tempo reale ad un centro di coordinamento che possa in tal modo assegnare la corretta priorità agli interventi.

Si deve altresì porre attenzione alla gestione in sicurezza dei presidi che sono utilizzati per il ricovero dei pazienti. In quest'ottica, la salvaguardia dei presidi ospedalieri (o di primo soccorso) dalla presenza di endotossine quali ad esempio il lipopolisaccaride (LPS) presente nella membrana esterna dei batteri Gram-negativi, assume una rilevanza non trascurabile.
Un altro aspetto importante coinvolge la gestione dei dispositivi Risonanza Magnetica per immagini. In questo caso devono essere valutati i rischi dovuti all'esposizione a intensi campi magnetici statici e variabili nel tempo (campi RM) e le eventuali riduzioni di prestazioni delle apparecchiature, durante un'attività diagnostica intensa e continuativa (tipica di situazioni di emergenza a seguito di evento avverso).

Sicurezza in ambito ospedaliero

L'obiettivo della ricerca riguarda:

- l'abbattimento della carica microbica ambientale nel suo insieme;
- Studio degli effetti biologici e genotossici di intensi campi magnetici statici e alternati; monitoraggio in continuo delle prestazioni delle apparecchiature di Risonanza Magnetica durante attività intensa e continuativa.
- Monitoraggio in continuo dell'esposizione degli operatori ai campi magnetici statici e alternati generati da piccole e grandi apparecchiature biomedicali (Magnetoterapia, Incubatrici Neonatali, Monitor dei parametri vitali, Elettrocardiografi, etc.) utilizzate durante l'attività diagnostica.
- Sviluppo di sistemi, metodologie e strumenti per l'identificazione di farmaci e dispositivi bio-medicali contraffatti o illeciti al fine di contrastarne la loro diffusione e commercializzazione. Un farmaco contraffatto, è inappropriato a curare un malato e può causare anche lo sviluppo di resistenza da parte di virus/batteri ad un determinato principio attivo.

In un contesto così particolare, diventa fondamentale tutelarsi dai possibili rischi che potrebbero alterare le prestazioni e l'affidabilità degli apparati elettromedicali e nello stesso tempo garantire le prestazioni funzionali dei rice-trasmettitori wireless che possono essere suscettibili a loro volta alle emissioni prodotte dagli stessi apparati elettromedicali. Protezione della popolazione esposta a campi magnetici.

Sicurezza nei prodotti-procedimenti farmaceutici

L' obiettivo della ricerca consiste nell'affrontare i problemi relativi all'identificazione e prevenzione della diffusione di farmaci scaduti e/o contraffatti che potrebbero costituire un potenziale pericolo per i pazienti. A ciò si aggiunge il fatto che gruppi criminali e terroristici vedono nel lucroso mercato dei farmaci contraffatti uno strumento per incrementare i loro guadagni da re-investire poi in altre attività criminali. In quest'ambito la lotta alla contraffazione diviene una della priorità per la sicurezza in ambito sanitario

Le principali capability da sviluppare sono:

TA2.3 Sistemi per la diffusione delle informazioni in situazioni critiche	Pag.58
TA6.2 Sensori per monitoraggio a distanza di pericoli chimici e biologici da postazione mobile o fissa	Pag.92

Prossimi Passi

L'apertura della piattaforma SERIT ad una più amplia platea di soggetti nazionali ha fatto emergere la necessità di esplorare ambiti di ricerca afferenti a domini non inizialmente trattati.

L'attuale situazione geopolitica ha posto l'accento sul tema prioritario della sicurezza nel trasporto marittimo, a cui verrà dedicato un nuovo settore guida, successivamente dettagliato nel proseguo del lavoro.

Dal dibattito sempre vivo tra i membri della piattaforma, le istituzioni nazionali ed europee e dall'evoluzione degli scenari potrà nascere la possibilità di ampliare le attività verso nuovi settori e focalizzare l'agenda di ricerca su alcune priorità specifiche.

Si introduce di seguito:

Settore Guida 14: Sicurezza nel Trasporto Marittimo

Per Sicurezza nel trasporto marittimo si intende quell'insieme di misure atte a monitorare il traffico navale di, tracciare quello merci e controllare il trasporto passeggeri, ciò al fine di salvaguardare la vita umana in mare e tutelare l'ambiente marino e costiero nonché prevenire azioni illecite contro navi ed infrastrutture portuali.

L' emergente richiesta di soluzioni afferenti ai temi della sicurezza relativamente al trasporto marittimo nasce sostanzialmente da due grandi "driver": garantire la sicurezza della navigazione e, al tempo stesso, migliorare le performance di gestione delle linee di traffico per rendere anche più efficienti le cosiddette "autostrade del mare", come canale di trasporto assimilabile a quello su gomma, in termini di sicurezza, efficacia e costo, incomparabile per quanto attiene le quantità dei volumi movimentati.

Per conseguire il raggiungimento di questi obiettivi occorre, tra l'altro, sviluppare e il potenziare le capacità di monitoraggio delle navi (VTMIS – Vessel Traffic Monitoring/Management Information Sistem) insieme al tracciamento delle merci della filiera marittima, nonché l'interoperabilità funzionale con i sistemi informativi attraverso una piattaforma info-telematica a supporto delle strutture operative, quali istituzioni, armatori, spedizionieri,etc.
Le soluzioni realizzative dovranno essere configurate secondo i diversi scenari afferenti il trasporto via mare, integrando le seguenti funzionalità: :

- supporto per la multimodalità, nell'accezione di integrabilità con nodi intermodali esistenti;
- adozione di metodologie e soluzioni architetturali orientate ai servizi
- monitoraggio del traffico marittimo, rilevazione di situazioni di rischio e tempestiva comunicazione di allarmi tra gli operatori (centri di controllo di terra, operatori di bordo e operatori marittimi);

E' evidente che su questo tema si realizza una forte sinergia con gli sviluppi connessi al monitoraggio marittimo, che ha come obiettivo principale la determinazione della presenza, nelle aree di interesse, di unità non cooperative.
Gli obiettivi della ricerca si riassumono nel:

- miglioramento delle capacità di rilevamento attraverso una più elevata risoluzione e un ampliamento dell'area marittima osservata, in particolare grazie al potenziamento di
  - sensori per la rilevazione dati (radar, AIS, radio, telecamere, etc.)
  - sistemi di elaborazione e fusione dei dati e presentazione su cartografia dello scenario operativo
- incremento dell'interoperabilità tra le diverse piattaforme adibite al controllo del traffico marittimo (mediante lo sviluppo di capacità operative semi-automatica per aspetti procedurali e tecnici, anche tra diversi Stati), al fine di consentire lo scambio di informazioni utili per :
  - garantire la cooperazione transazionale e la continuità delle operazioni, mediante un approccio net-centrico (es. VTMIS Safeseanet);
  - condividere informazioni al fine di elaborare uno scenario utile ed efficace per la gestione congiunta delle emergenze.

Area Tecnologica 1: Sorveglianza & Situation Awareness

.

Per ***Sorveglianza & Situation Awareness*** si intende il processo di osservazione di persone, oggetti, aree di diversa vastità in conformità a norme definite o comportamenti attesi (in accordo con le direttive di sicurezza dei diversi sistemi vigenti), inclusa la capacità di esercitare le funzioni di Comando & Controllo in reazione al verificarsi di un evento.

In particolare, questa tematica è incentrata sul rilevamento automatico di eventi anomali, il riconoscimento di potenziali minacce, e la capacità di reazione (*comando e controllo*) in scenari complessi.

La capacità di monitorare un'area (come un. singolo accesso, un piazzale aeroportuale, etc.) o un asset (ad esempio, un edificio, un'infrastruttura ferroviaria, etc) è potenziata dalla possibilità di fondere informazione provenienti da diverse tipologie di sensori che rilevano differenti parametri (per esempio traccia radar + video EO + immagine satellitare).

La Sorveglianza è resa maggiormente efficiente dalla capacità di assicurare un monitoraggio costante ed esaustivo (osservazione h24, dati raccolti da differenti sensori).
Tipicamente la **Sorveglianza** può essere distinta in:

- sorveglianza di punto (singolo accesso),
- sorveglianza perimetrale (o di confine),
- sorveglianza di area (anche molto estesa).

La Sorveglianza è legata anche alle funzionalità di *Geocasting, Positioning e Supporto alla Navigazione.*

La funzionalità di **Situation Awareness** include la capacità di elaborare dati eterogenei e di sintetizzarli in un unico quadro operativo e si esplicita attraverso l'integrazione di **Centri di Comando e Controllo (C2)**, ai quali afferiscono le tecnologie necessarie per lo sviluppo e l'implementazione di:

- Common Operational Picture (COP), intesa come capacità di sintesi delle informazioni provenienti dai diversi sensori, mezzi, strumenti e squadre operative impiegate sul campo;
- Interfaccia uomo-macchina (HMI) per Situation Awareness / Enhanced Situation Awareness (inclusa l'integrazione di dati derivanti dai sistemi cognitivi);
- Strumenti di Decision Support (inclusi l'analisi cognitiva, workflow procedurali, correlazione tra dati, etc);
- Tools e strumenti di simulazione per gli scenari e Lesson Learnt;
- Sistemi Esperti di data-fusion e reasoning, per l'allerta precoce ed il supporto alle decisioni (inclusa la capacità di elaborazione sulla base di informazioni relative ad eventi pregressi); Architetture per sistemi netcentrici a supporto della diffusione di comandi e informazioni utili.

Le tecnologie per la sorveglianza includono:

- Sensori:
  - ElettrOttico (ad ampio spettro), Radar, CCTV, sensori stand off, sigilli elettronici, RFID, etc;
  - Reti di sensori (wireless, cablate, etc.);
- Piattaforme:
  - Piattaforme aeree, navali, satellitari, terrestri (fisse e mobili) ,UAV, …
  - Sistemi di sorveglianza & Situation Awareness integrati;
- Centri di Comando e Controllo.

TA1.1 Analisi integrate per rilevamento di comportamenti anomali (analisi per immagini / analisi varie), sensori per la generazione di Early Warning

La capacità umana di cogliere un comportamento anomalo in una situazione complessa ed avvertirne la potenziale pericolosità deriva da capacità ad alto livello del sistema nervoso centrale di filtrare e correlare informazioni diverse e, soprattutto, di definire uno standard di "normalità" relativo ad azioni simili in situazioni diverse: ad esempio, un uomo che corre per prendere un tram non è pericoloso, un uomo che corre lontano da una persona che urla potrebbe esserlo. Il limite degli umani è dunque nella loro limitata capacità sensoriale. D'altro canto, mentre la capacità di rilevazione di eventi semplici da parte dei molteplici tipi di sensori disponibili è molto superiore a quella umana, la rilevazione automatica di comportamenti anomali, all'attuale stato dell'arte, è limitata a situazioni ben precise, a comportamenti semplici e strettamente codificati e ad input sensoriali omogenei. Un salto di qualità nello sfruttamento delle potenzialità dei sensori sempre più raffinati e più compatti che la tecnologia sta mettendo a disposizione, richiede lo sviluppo sia della capacità di sfruttare congiuntamente sensori di vario tipo (informazioni acustiche, visive, olfattive, tracce di sostanze chimiche, radioattività,...) che della capacità di comprendere la potenziale pericolosità di un evento / comportamento in un dato contesto. L'integrazione di informazioni da sensori eterogenei richiede a sua volta una capacità avanzata di data fusion, in cui sia possibile misurare la rilevanza degli stimoli sensoriali in base alla situazione sotto analisi. L'apprendimento di che cosa significhi "anomalia" richiede la definizione di algoritmi e procedure di apprendimento automatico che rendano il sistema in grado di estrarre eventi significativi dopo l'addestramento (parzialmente guidato) su grandi moli di dati relativi a situazioni note. Una componente necessaria è la capacità di descrivere il contesto e gli scenari in modo omogeneo, basandosi su primitive astratte e sulle loro relazioni spazio-temporali, sfruttando ontologie di scenari e metodi di *graph matching* per riconoscere lo scenario corrente. Allo stesso modo, l'implementazione di simulatori di scenari in grado di fornire una elevata quantità di dati di training relativi ai comportamenti che si vuole etichettare sia come normali che come anomali rappresenta una soluzione per incrementare la capacità dei sistemi di rispondere efficacemente in fase di testing e di funzionamento on-line. La definizione della struttura di un "evento pericoloso" comporta la selezione di input sensoriali eterogenei, la capacità di analisi dello scenario e di valutazione dei rischi potenziali. La rilevazione di un evento pericoloso avverrà tramite l'analisi di una selezione degli input sensoriali più rilevanti nello scenario considerato, guidata da un'analisi del rischio.

L'attività di ricerca sarà focalizzata su casi di studio rilevanti per i settori guida di riferimento, definiti tenendo conto di situazioni e comportamenti specifici e di dotazioni sensoriali realistiche.

Technology relevance:

1. Video Analisi di scene complesse [113-1; 113-2]
2. Sensori alternativi (odori, tracce chimiche, radiazioni) [110-14; 200-10;200-11;200-12; 200-26]
3. Reti di sensori eterogenei [408-1; 408-3]
4. Data fusion avanzato [113-4]
5. Definizione di scenari di rischio e *risk analysis* [301A]
6. Metodologie di *learning* automatico e semi-automatico [114-1; 114-2]
7. *Crowd behaviour modelling* [120-6, 120-14]
8. Interfacce uomo-macchina avanzate (*focus on attention, comportamento dell'operatore ⇔ man-in-the-loop*) [303B-14]
9. Modelli di scenario e di eventi simulati [114-5]

Settori Guida di riferimento: 1,3,10

TA1.2 Data Fusion di sensori eterogenei

La fusione di dati sensoriali rappresenta uno dei campi di ricerca e tecnologici di maggiore importanza per l'implementazione di molte applicazioni nel settore della Sicurezza: queste ultime vanno da sistemi con capacità di individuare situazioni ed eventi anomali in un'area sorvegliata, sino a dispositivi mirati al potenziamento delle capacità percettive degli osservatori. La definizione generalmente accettata di "*data fusion*" è quella di processi che si occupano di associare, correlare e combinare dati ed informazioni provenienti da una o più sorgenti di dati, al fine di ottenere stime di identità e posizione, nonché di definire al meglio le informazioni spaziali e temporali relative a situazioni e minacce di vario tipo, valutandone nel contempo anche il significato.

Il processo è caratterizzato da un continuo raffinamento delle stime e degli stati e dalla valutazione dell'eventuale necessità di ulteriori sorgenti di dati o di modifiche del processo stesso. (*Data Fusion Lexicon, JDL Data Fusion Subgroup 1987*).

Quest'ultima definizione dovrebbe essere integrata con l'impiego della conoscenza e delle informazioni strutturate contenute nei *database*, in modo da consentire un'interpretazione più ampia dei dati sensoriali.

La Data Fusion è alla base di numerose linee di ricerca: dall' Intelligenza Artificiale, orientata alla capacità di realizzare funzioni di "consapevolezza" (*awareness*), fino allo sviluppo di algoritmi rapidi per incrementare la precisione di singoli sensori o per la realizzazione di immagini iperreali, ove differenti tipologie di informazioni sono sintetizzate in un'immagine singola, che permette all'osservatore umano una rapida ed esaustiva comprensione della situazione. Lo sviluppo di questa capability per migliorare la competitività nazionale, potrebbe includere una lista di obiettivi, quali:

- Rivelazione di allarmi provenienti da situazioni di coincidenza o anticoincidenza di eventi generati da sensori eterogenei, eventualmente tramite l'analisi di serie storiche;
- Ricerca e Standardizzazione di librerie di algoritmi per migliorare precisione/risoluzione/affidabilità di sistemi sensoriali standard tramite l'impiego di dati che provengono da altre sorgenti;
- Capacità di correlare e presentare ad un supervisore umano più immagini di scene simultanee per facilitare il processo decisionale (*human awareness*);
- Capacità di correlare immagini simultanee di scene e di integrarle con una conoscenza generale preesistente per individuare un' evoluzione attesa della situazione;
- Capacità di realizzare e gestire lo scambio dati di grandi reti di sensori eterogenei;
- Ricerca e progettazione di algoritmi e metodologie di fusione dati di Osservazione della Terra (OT) multisorgente (acquisiti da piattaforma satellitare e da piattaforma aerea), multirisoluzione spaziale (dell'ordine dei 10 m fino a 50 cm) e multitemporali (con frequenza di acquisizione variabile), atti ad implementare catene di processamento che generino mappe tematiche multiscala a supporto delle attività decisionali ed operative.

Technology relevance:

1. *Sensor modelling*, [306B-1]
2. Sviluppi sulle *Neural Networks*, [114-2]
3. Sviluppi sulle *Kernel Machines*, [114-1; 114-3]
4. Miglioramento della comunicazione in reti di sensori (es: *multihop protocols*), [413-1; 413-5; 416-15]
5. Metodologie di apprendimento semplice e rinforzato (es. *Bayesian Learning*), [114-3]
6. Analisi di Eventi Complessi [113-4; 114-4; 114-5]
7. Tecniche *Knowledge-based* , [114-1]
8. Elaborazione ed integrazione di dati da piattaforme satellitari aeree e terrestri di Osservazione della Terra [113-1; 113-2; 113-3; 113-4]
9. Metodologie di estrazione di mappe cartografiche multispaziali e multi temporali [113-8; 113-12].

Settori Guida di riferimento: 1,4,6,9,10

TA1.3 Elaborazione di immagini satellitari (SAR, ottico) ad alta risoluzione

Questa capability si riferisce alla necessità di garantire maggior sicurezza agli operatori impegnati in operazioni di "*Safe & Rescue*", nonché alla possibilità di assistere al meglio le imbarcazioni sulle rotte di migrazione. Per far ciò, è necessario ottenere informazioni circa i regimi meteo-marini, a livello locale, in aree ove si ritiene probabile la presenza di natanti in difficoltà, e migliorare la capacità di localizzazione dei natanti stessi o di oggetti alla deriva pericolosi per la navigazione. Ciò premesso, il lavoro si articola su diverse linee, che richiedono la messa a punto di tecniche:

- per la stima accurata dei regimi correntometrici e ondosi da dati SAR ad alta risoluzione temporale (ad es. integrazione di dati ENVISAT, TERRA-SAR, Cosmo-SkyMed);
- di geocodifica in tempo reale di immagini ottiche ad alta risoluzione spaziale. Queste tecniche, per ovvie limitazioni tecnologiche, si riferiranno ad aree relativamente piccole riprese sull'intera immagine;
- di rivelazione in tempo reale da dati SAR ad alta risoluzione (ad esempio dati TERRA-SAR, Cosmo-SkyMed) di oggetti alla deriva, eventualmente semisommersi.

Le tecniche del punto 1 si basano sul fatto che il segnale retrodiffuso dalla superficie del mare in dati SAR dipende dal regime di rugosità (onde capillari) della superficie stessa. Poiché il regime di rugosità viene modulato, oltre che da forzanti quali, per esempio, vento, pioggia, etc., dal regime correntometrico ed ondoso, alla base di queste tecniche vi è la necessità di mettere a punto algoritmi di inversione dai quali (noti i forzanti meteorologici e le intensità della radiazione retrodiffuso) si ottengano informazioni circa lo stato del mare.

Il punto 2 richiede la messa a punto di tecniche basate, per esempio, sulla triangolazione per la definizione della posizione relativa di diversi satelliti. Ciò facendo è possibile diminuire i tempi di integrazione necessari a migliorare la localizzazione del satellite in acquisizione e, pertanto, giungere a risultati di geocodifica più accurati e in tempi più brevi.

Le tecniche di cui al punto 3 sono complementari a quelle ottiche e permettono la sorveglianza anche durante le ore notturne ed in avverse condizioni meteorologiche. L'ulteriore integrazione di dati SAR ed ottici aumenta la probabilità di scoperta di oggetti alla deriva.

Technology relevance:

1. Raccolta, Classificazione e analisi di Dati (as. es. meteorologici, delle Reti Geodetiche Nazionali, satellitari) [113-3; 113-8; 300B-3; 401-3; 401-4]
2. Tecniche di inversione elettromagnetica (*Inverse scattering problems*) [114-3]
3. Solutori elettromagnetici ultraveloci (*Fast Multilevel Physic Optics methods*) [114-3]
4. Processazione parallela di dati SAR (*Parallel/pipeline multiprocessor SAR data processing*) [113-1]
5. Analisi frattale e decomposizione *wavelet* (*Fractal analysis and wavelet decomposition*) [113-1]
6. Tecniche di classificazione *object-oriented* per il riconoscimento automatico di oggetti [116-1; 116-4]

Settori Guida di riferimento: 8,9

TA1.4 Tecnologie abilitanti per il settore spaziale

Uno degli obiettivi di maggior rilievo delle tecnologie per satelliti di nuova generazione è lo sviluppo di soluzioni che puntino ad una sensibile riduzione di masse e consumi, guidati da una maggiore integrazione funzionale tra *payload* e *bus*. Questa tendenza evolutiva consentirà una riduzione degli apparati di bordo rispetto ai prodotti esistenti che svolgono funzioni simili. In tale contesto sono rilevanti sia quelle tecnologie che consentono una elevata integrazione delle funzioni radio, sia il concepimento e la progettazione di *chip* ad alta capacità di calcolo miniaturizzati che mantengano tuttavia le caratteristiche di alta resistenza alle radiazioni e all'ambiente spaziale imposte dalla normativa. Lo studio dei nuovi sistemi di propulsione permetterà una maggiore manovrabilità e diminuzione di costi. Per quanto riguarda lo sviluppo di nuove tecnologie volte a migliorare notevolmente i tempi di rivisita di costellazioni di satelliti con masse e consumi ridotti, esiste una notevole capacità e competenza nazionale nel settore, grazie soprattutto all'esperienza maturata con il progetto COSMO SkyMed e GALILEO. Studi sul volo in formazione di satelliti (inclusi mini e micro), analisi dei sistemi di comunicazione e controllo per la gestione della costellazione durante il volo, tecnologie per lo scambio dei dati tra i satelliti in formazione e terra, trasmissioni di elevate moli di dati osservati via DRS, sono solo alcune delle tematiche che l'industria italiana è in grado di affrontare e che risulteranno cruciali ai fini della competitività in ambito internazionale. Altre possibili opzioni potranno essere identificate anche sulla base dei risultati derivanti dalle attività in via di attivazione e delle tecnologie abilitanti che si renderanno disponibili per l'implementazione di funzionalità ancora più mirate.

La riduzione dei costi e il miglioramento di precisione e sensibilità rendono possibili le funzionalità di sorveglianza accurata, finalizzate anche al controllo delle zone marine e costiere. Tra i miglioramenti che potranno consentire queste potenzialità e che sono alla portata degli operatori nazionali sia dell'industria sia della ricerca,si citano:

- Gli studi di sistema mirati all'ottimizzazione delle costellazioni satellitari (con uso di AIS, radar, e Elettro-Ottico incluse le bande Iperspettrale e IR) e rivolti a rispondere a requisiti di *Early Warning/ Responsiveness*;
- I miglioramenti della AIS signal detection (*Receiver technology, Antennas, On board / ground signal processing*);
- Il miglioramento, anche tramite tecniche ICT e di signal processing, di radar dedicati all'osservazione marina (*Sea clutter effect*, *Vessel signature database*);
- Lo sfruttamento della tecnologia GNSS (Multi-constellation e multi-frequency) che potrà potenziare in modo decisivo la precisione e l'accuratezza delle operazioni di sorveglianza (incluso il PRS in grado di garantire gli importanti requisiti di continuità e robustezza);

Più in generale, esiste una larga competenza e capacità di potenziamento della sorveglianza legata all'integrazione di "osservatori" dallo spazio con "osservatori" posizionati a terra o sul mare e tale capacità potrà portare a decisi incrementi della competitività del Paese in questo Settore.

Technology relevance:

1. Sistemi di propulsione avanzata, *Hybrids, Resistojet* [215-5]
2. Attuatori e sensori a dimensioni ridotte, MEMS technology [110-21]
3. *System on-a-chip* ad alta capacità di calcolo e dimensioni ridotte [111; 200-28]
4. Sistemi di comunicazione miniaturizzata [118]
5. Inter-satellite *communication capability* e *Formation Flying* [118]
6. GNSS *multi-constellation- multi-frequency satellite Receiver* (inclusi ricevitori PRS) [401-2]
7. *Integrated Communication functionalities relevant to PVT information* [118, 413, 416]
8. *ADS-B (Automatic Dependant Surveillance- Broadcast) for aircraft surveillance* [306A-2; 205-2; 401-2]
9. AIS *Payload for Maritime Security and Safety* [118-1]
10. Satelliti per l'osservazione della terra e sensori *payload* [401-3; 215-6; 215-9]

Settori Guida di riferimento: 6,8

TA1.5 Sensori per il monitoraggio delle infrastrutture di produzione di energia e delle reti di distribuzione

Rete di trasmissione AT (a cui sono connesse le centrali di produzione elettrica): fornisce agli operatori dei centri di controllo delle reti elettriche informazioni accurate in tempo reale sullo stato del sistema, per garantire in fase preventiva, o di ripristino in fase correttiva, condizioni di funzionamento stabili e sicure. L'attuazione di queste funzioni spesso è impedita dall'incertezza conoscitiva del sistema elettrico (imprecisione della modellazione), o dalle limitazioni del monitoraggio. I tradizionali sistemi di supervisione, controllo e acquisizione dati (SCADA), sono infatti in genere caratterizzati da una scansione asincrona e non sufficientemente frequente dei campionamenti, da ritardi nella comunicazione, da tolleranza nelle misure. Oggi le moderne tecnologie di comunicazione satellitari, utilizzando misuratori di fasori (*Phasor Measurement Unit - PMU*), consentono di realizzare un sistema in grado di misurare in tempo reale grandezze che interessano un'ampia area del sistema elettrico (*Wide Area Measurement System, WAMS*), consentendo il controllo di stabilità di grandi reti interconnesse ed evitando la propagazione di disservizi e black-out.

Rete di distribuzione BT: il nuovo contesto energetico ha portato ad incentivare l'impiego di nuove tecnologie di produzione elettrica con il coinvolgimento sempre più significativo di impianti di taglia medio-piccola da connettere alle reti di distribuzione in prossimità degli utenti. Questa nuova configurazione, definita Generazione Distribuita o Diffusa (GD), garantisce la possibilità di diversificare le fonti energetiche da convertire in energia elettrica, aumentando in modo sostanziale lo sfruttamento di quelle rinnovabili. La penetrazione della GD nel sistema elettrico non è però esente da una serie di inconvenienti, dovuti al fatto che le attuali reti di distribuzione sono state progettate e gestite come reti passive(presuppongono cioè che non vi sia iniezione di potenza attiva dall'utente verso la rete). Il funzionamento di una rete di distribuzione resa attiva (*smart grid*) richiede pertanto l'impiego di "controllori" capaci di monitorare le condizioni complessive del sistema, di risolvere le problematiche di intervento delle protezioni, di controllare i parametri di qualità del sevizio di distribuzione (livelli di tensione, compensazione delle armoniche, etc.), ed eventualmente coordinare il passaggio a regimi di funzionamento particolari della rete (ad esempio, l'operatività in isola di porzioni del sistema di distribuzione).

Per le infrastrutture di comunicazione richieste dalle reti di distribuzione, l'industria nazionale ha sviluppato diverse potenzialità di offerta che costituiscono un asset importante per lo sviluppo del mercato, particolarmente sotto l'aspetto della sorveglianza infrastrutturale di sicurezza: protezione contro l'*islanding***;** monitoraggio della tensione in rete, telecontrollo e ricerca guasti in rete MT tramite connettività wireless**;** monitoraggio e la gestione degli impianti di generazione, sia da parte dei gestori d'impianto che, eventualmente, del gestore di rete tramite reti *wired (ADSL e derivate)*.

Technology relevance:

1. Misuratori di fasori (*Phasor Measurement Unit - PMU*), [107-7; 111; 303B-10]
2. Controllo integrato in tempo reale per reti di distribuzione in Media Tensione (*Distribution Management System* - DMS) [107-10;311A-1;509A-2]
3. Stima dello Stato (*State Estimation*) della rete sulla base di misure locali o remote [107-10; 113-4; 113-8; 114-3]
4. Ottimizzazione del controllo (*Optimal Control*) per definire i valori ottimali delle grandezze controllate [107-10;113-8;114-4]
5. Esecuzione del controllo (*Control Scheduling*); che elabora e invia i parametri ottimali di regolazione[107-10;114-4; 311A-1]
6. Controllore di utenza (gestione intelligenti degli apparecchi utilizzatori - *smart building*) [107-10]

Settori Guida di riferimento: 2,5

TA1.6 Sistemi di localizzazione, navigazione e guida assistita

Per la sicurezza dei confini e per quella aereo-portuale viene richiesta una sempre maggiore accuratezza di informazioni, relative al posizionamento spazio-temporale di persone, mezzi e merci; in questo ambito trovano applicazione i sistemi "cooperativi" di localizzazione, di posizionamento e di navigazione, sia autonoma che assistita. L'impatto economico potenziale di questi sistemi è vastissimo, coprendo gran parte degli aspetti del trasporto commerciale di ogni genere (rotaia, aereo, navale, di terra), gli aspetti relativi al movimento di persone su mezzi anche propri, gli aspetti relativi ai mezzi e ai sistemi di protezione ed intervento tanto per gli aspetti propriamente di Security che per quelli di safety (si pensi alla esigenza di localizzazione e coordinamento di squadre che operano in contrasto ad incendi boschivi o di altro tipo).
L'industria nazionale è in grado di intervenire con una propria offerta altamente competitiva in molte aree applicative, ma le condizioni di competitività esasperata di questo mercato impongono un miglioramento costante della capability disponibile.
Si parla in generale di sistemi "collaborativi" RTLS (*Real Time Locating Systems*), ovvero di quei sistemi che forniscono all'utente remoto la posizione degli oggetti monitorati, permettendo quindi di cercare e/o dirigere il movimento di beni e risorse. Questi sistemi sono gestiti da un server che elabora i dati provenienti da nodi fissi o mobili che operano in aree tipicamente ben definite e confinate. I dati trattati sono relativi a misurazioni di distanze, di angoli o di entrambe. In funzione della tipologia dei sensori impiegati,questi sistemi richiedono alcuni vincoli, come un'illuminazione comune delle zone rilevate e/o la vista diretta tra i nodi fissi e mobili del sistema. Nel settore della sicurezza del traffico aereo e di quello marittimo, i sistemi di posizionamento, navigazione di bordo assistita o autonoma, sono fortemente integrati tra loro e sono componenti stessi del sistema di controllo sia aereo (ATM) che marittimo (VTMS); si tratta di sistemi presenti nei contesti in cui sono necessarie informazioni relative alla posizione di persone e mezzi con precisioni di pochi metri. Attualmente il sistema più usato per la navigazione sia navale che aerea è quello INS/GPS, in cui la navigazione inerziale (INS-*Inertial Navigation System*) è assistita dal *Global Position System*, (sistema di posizionamento su base satellitare a copertura globale e continua costituito dalla rete satellitare, da un centro di calcolo, dalle stazioni di tracciamento e di soccorrimento ed dal ricevitore GPS). Aspetti mirati all'incremento di competitività dell'offerta nazionale attraverso azioni di ricerca e sviluppo mirate riguardano lo sviluppo e la regolamentazione di servizi di utilità pubblica, il miglioramento della precisione dei dati d'interesse (fino a decine di cm), l'integrità dei dati migliorando la resistenza a disturbi EM ambientali, la ricezione in sicurezza dei dati. L'offerta nazionale su questa capability offre anche applicazioni finalizzate alla sicurezza dei confini. In ambito marittimo, si punta allo sviluppo di sistemi automatici di identificazione (AIS) sempre più performanti**:** si tratta di sistemi anti-collisione composti di un ricetrasmettitore VHF e di ricevitore GPS, insieme ad altri sensori elettronici di navigazione, in grado di trasmettere automaticamente,ad imbarcazioni vicine e a stazioni VTMS presenti a terra ,informazioni relative a posizione, velocità e condizioni di navigazione. Altre ricadute interessanti che richiederanno significativi sforzi di R&D possono riguardano gli aspetti di impiego di altri sistemi di navigazione GNSS (quali Galileo) e gli aspetti legati all'ampliamento della portata dei *transponders* (attualmente intorno ai 70Km) per possibili integrazioni alla rete satellitare (*Space Based* AIS).

Technology relevance:

1. Algoritmi di navigazione e di geo-localizzazione [205-1; 205-2]
2. Simulazione e *modelling* [114-5]
3. Tecniche di sincronizzazione ultrastabili [113-13]
4. Sorgenti ad alta stabilità. (205-10 / 205-13)
5. Integrazione di sistemi di navigazione Galileo PRS [113-4; 306A-2; 205-2; 401-2]
6. Sistemi LBS (*Location Based Service*) [306A-2]
7. Sistemi di *Tracking and Tracing* [200-17; 113-4]
8. ADS-B (*Automatic Dependant Surveillance – Broadcast) for aircraft surveillance* [301B-3; 306A-2; 205-2; 401-2]
9. NAVCOM *Laboratory* per l'elaborazione e la caratterizzazione dei segnali [306A-2]

Settori Guida di riferimento: 6,8

TA1.7 Sistemi di sorveglianza perimetrale

I sistemi di sorveglianza perimetrale proteggono le infrastrutture critiche contro l'intrusione non autorizzata di persone e mezzi. Alcuni esempi di infrastrutture rilevanti sono gli aeroporti, le linee ferroviarie, le grandi centrali di produzione dell'energia, impianti industriali e depositi.

La sorveglianza e protezione perimetrale, ad oggi, si può realizzare con semplici recinzioni e videocamere dotate di Video Analisi, oppure con le stesse recinzioni associate a sensori antintrusione. In alcuni ambiti è necessario sorvegliare anche le aree esterne adiacenti l'infrastruttura, o ampie aree a cielo aperto interne al perimetro. L'abbinamento dei sistemi fornisce risultati abbastanza validi ma costituisce un costo molto oneroso da sostenere per il cliente finale. I sistemi di recinzione presenti sul mercato sono le recinzioni metalliche passive e le recinzioni "integrate attive". Queste ultime sono recinzioni associate a sensori antintrusione che, in generale, hanno il difetto di generare un elevato numero di falsi allarmi.

L'obiettivo della ricerca è di individuare e sviluppare sistemi con le seguenti caratteristiche:

- Rilevamento automatico dell'intento d'intrusione
- Un basso FAR (frequenza di falsi allarmi)
- Totale immunità a fattori meteorologici, vibrazioni, o interferenze radioelettriche
- Rilevamento in caso di intenzione di sabotaggio
- Facile installazione
- Controllo centralizzato in un sito considerevolmente grande.

In particolare, si richiedono soluzioni di sorveglianza per la protezione perimetrale sufficientemente affidabili, che forniscano un basso FAR, anche senza necessitare dell'abbinamento con sistemi TVCC e di video analisi.

In ambito ferroviario, sono in via di sperimentazione sistemi in fibra ottica installati al di sotto dei binari, utili a rilevare il passaggio in prossimità dell'armamento ferroviario e quindi ogni potenziale intrusione. Per gli aeroporti, si deve verso mirare ad un sistema per la gestione integrata della sicurezza nel sedime aeroportuale, del quale i sistemi di sorveglianza perimetrale sono una componente, estendendo le capacità degli attuali sistemi di gestione della movimentazione di superficie. Inoltre, vanno considerate anche le possibili intrusioni aeree, sviluppando tecniche e sistemi di sorveglianza di aeromobili non cooperativi a bassa quota (piccoli, lenti, *manned* ed *unmanned*).

Per alcune applicazioni si renderà necessario realizzare, anche attraverso installazioni di prova, una approfondita analisi delle caratteristiche geografiche che possono interferire con il regolare funzionamento del sistema, per definire con maggior precisione i limiti della sua applicazione:

- Su ponti e viadotti
- In zone ad elevato rischio sismico
- In zone desertiche

Technology relevance:

1. Recinzioni "Integrate attive" e tecnologie di gestione dei falsi allarmi [113-4; 117-8]
2. Sistemi antintrusione "smart" [117-8]
3. Sviluppo di nuovi sensori specificamente perimetrali ad alta stabilità e basso costo [117-8; 307B-2]
4. Sistema integrato per la gestione della sicurezza nel sedime aeroportuale [301B-7; 301B-8; 200-17; 306A-1; 306A-2]
5. Tecniche e sistemi di sorveglianza di aeromobili non cooperativi a bassa quota [200-17; 113-4; 306A-1; 306A-2]
6. Protezione da *jamming* dei sistemi ATC di sorveglianza e navigazione, in particolare quelli basati su GPS (ADS, GBAS, GRAS, etc.) [113-10]

Settori Guida di riferimento: 1,2,7

TA1.8 Piattaforme di sorveglianza marittima, terrestre e aerea

La sorveglianza, particolarmente se svolta su siti ed infrastrutture critiche o per la protezione di tratti di confine, può un'opzione assai costosa, specie se applicata ad ampie zone da controllare. L'impiego di mezzi di tipo terrestre, e/o marino con uomini a bordo in operazione continua, è generalmente inaccettabile e lo sviluppo di soluzioni *unmanned* e delle relative piattaforme operative sta diventando quindi una soluzione desiderabile.

La capability deve essere in realtà suddivisa per i suoi diversi obiettivi, dato che le tecnologie sensoriali, di comunicazione e di locomozione per le tre aree che devono essere controllate, implicano sviluppi di tipo differente. Vi sono molte caratteristiche comuni che suggeriscono di vedere le tre aree tecnologiche congiunte in un'unica Capability, tra queste gli aspetti di controllo, di intelligenza, di network e di percezione. Gli sviluppi sulla percezione costituiscono ovviamente un elemento distinto da quelli sulla sensorialità propriamente detta, coinvolgendo aspetti di integrazione, più che di struttura, del sensore stesso. Circa la rilevanza dell'impiego di piattaforme autonome, a parte gli argomenti già menzionati nelle generalità, è importante tener conto che l'esclusione dell'uomo dall'interno del veicolo, implica vantaggi che vanno al di là del risparmio sull'impiego dell'operatore, come la migliorata resistenza ad ambienti ostili, superiori caratteristiche di tipo operativo, ridotte dimensioni, minore energia richiesta e quindi maggiore autonomia.

L'industria nazionale vede la realizzazione di piattaforme autonome come uno dei propri punti di forza nella competizione internazionale, e tuttavia minacce sempre più serie a questa posizione sono in arrivo soprattutto da Paesi extra-europei, con la conseguente generazione di una forte richiesta di supporto per le attività di ricerca e sviluppo (richiesta che comprende anche l'accesso ad operatori non industriali come centri di ricerca e Università). Per l'impiego di questi sistemi in condizioni operative reali, uno sforzo particolare deve essere rivolto allo studio ed alla valutazione di procedure di certificazione ed alle metodologie che permettano di rilasciare autorizzazioni e permessi di transito. Tali aspetti sono infatti direttamente legati alle dimensioni di mercato e risultano quindi di estremo interesse per un elevato impatto industriale.

Gli obiettivi specifici per il sostegno e lo sviluppo di questa Capability comprendono:

- La tecnologia per gestire missioni, sia con o senza, la supervisione di un operatore umano in remoto; entrambe le opzioni sono attualmente una sfida tecnologica e non adeguatamente supportate;
- La capacità di intervenire su aree e di eseguire task, attualmente eccessivamente costosi per poter essere adeguatamente eseguiti a partire dalle tecnologie e dalle infrastrutture disponibili;
- Le tecnologie e le prestazioni satellitari, atte a fornire acquisizioni con risoluzioni spaziali e temporali adeguate alle attività di controllo e sorveglianza. Questo incentiverà anche la ricerca e lo sviluppo di metodologie e algoritmi ad-hoc per processare i dati acquisiti dalle nuove piattaforme

Technology relevance:

1. Sistemi di comunicazione ad alta protezione [117-18]
2. Reti di sensori avanzate [408-1]
3. Sistemi di sorveglianza multi-piattaforma coordinati [308A-1]
4. Calcolo distribuito [116-9; 116-10]
5. Architettura di sistemi autonomi [400-3 ; 402-9; 403-6]
6. Procedure di *clearance* per l'impiego di piattaforme autonome [500-3]
7. Sciami intelligenti e situation awareness cooperativa [113-11; 303B-5; 416-11]
8. Sensoristica satellitare di Osservazione della Terra per usi civili [215-6; 215-9]
9. Algortimi di processamento dati di Osservazione della Terra per prodotti e servizi a valore aggiunto [113-1]

Settori Guida di riferimento: 8

TA1.9 Strumenti di supporto alla sorveglianza mediante riconoscimento di scene e cross correlation di informazioni

Lo scopo finale della funzione di sorveglianza è quello di mantenere una rappresentazione aggiornata della situazione di interesse, in modo da supportare i sistemi e le persone preposte a gestire la situazione stessa, consentendo di prevederne anche l'evoluzione. La rappresentazione della situazione non deve per questo limitarsi ad una collezione di elementi, di oggetti (correttamente posizionati, identificati, classificati e corredati di informazioni addizionali) e di dati, ma deve evidenziare anche *pattern* di alto livello, condizioni, e scene rilevanti per i fini, i compiti e la missione dell'utilizzatore.

Automatizzare questa fase del processo richiede innanzitutto la rappresentazione (formale e completa) della porzione del mondo che interessa l'utilizzatore (ontologie di dominio). Gli elementi della situazione percepita vanno quindi correlati, aggregati e vanno individuati gli elementi di interesse effettivamente presenti. In generale, il processo coinvolge il trattamento di informazioni incomplete, la gestione dell'incertezza e della confidenza, l'estrazione di informazioni da grandi quantità di dati, la gestione di informazioni distribuite su più sistemi, anche di organizzazioni diverse.

E' auspicabile che le metodologie, i linguaggi e gli strumenti di base siano sviluppati dalla ricerca in campo ICT e che nell'ambito della sorveglianza per la sicurezza, la ricerca si concentri ,soprattutto, verso l'applicazione e la validazione nei settori guida interessati delle tecnologie ICT più innovative, tra cui:

- interoperabilità tra sistemi diversi (traduzione tra ontologie);
- supporto del processo cognitivo umano (presentazione dell'informazione), trasferimento della conoscenza acquisita tramite vocabolari condivisi);
- rilevamento precoce di situazioni critiche, con ridotto numero di falsi allarmi
- recupero di informazioni rilevanti da grandi basi dati non strutturate / multilingue (es. internet)
- gestione adattiva e dinamica dei sensori e delle piattaforme di sorveglianza verso un paradigma di sorveglianza proattiva;
- riduzione degli errori umani causati dalla mancanza o sovrabbondanza di informazioni;
- rapidità di decisione e capacità di suggerire azioni appropriate.
- tecniche di *data mining* per l'estrazione di informazioni da dati di Osservazione della Terra.

Technology relevance:

1. Modellazione dei domini e dei sistemi [114-5]
2. Ontologie formali, traduzione tra ontologie [116-4]
3. Correlazione di dati eterogenei [113-8, 114-3]
4. Modellazione delle interdipendenze [114-3]
5. Rappresentazione e gestione dell'incertezza/ Ragionamento simbolico e multi-criterio [114-1]
6. Sistemi multi-agente [116-11]
7. Metodi di *Learning Bayesiano* [114-3]
8. Reti neurali artificiali [114-2]
9. Algoritmi evolutivi [116-1]
10. Interfaccia ed interazione tra uomo e computer [308B-1; 308B-3]

Settori Guida di riferimento: 1

TA1.10 Sensori per la sorveglianza marittima e costiera, basati a terra o imbarcati

Monitorare quanto sta avvenendo nella fascia di mare e nello spazio aereo prossimo alla costa, è indispensabile per consentire lo svolgimento sicuro delle attività legali (commercio, turismo, pesca) e per contrastare invece quelle illegali (contrabbando, traffici illeciti, immigrazione clandestina). La situazione marittima si basa in primo luogo sui dati generati dai sensori; alcune limitazioni di questi ultimi, soprattutto in riferimento alla capacità di seguire e identificare ad adeguata distanza le piccole imbarcazioni, rendono più difficoltoso il contrasto delle attività illegali. I sistemi di sorveglianza marittima e costiera per la protezione dei confini utilizzano differenti tipi di sensori, basati a terra, imbarcati, subacquei, aerei o satellitari. I sensori basati a terra sono tipicamente quelli che garantiscono la sorveglianza continua della fascia di mare più prossima alle coste (svolgendo spesso sia funzioni di sicurezza, sia di controllo del traffico marittimo), mentre i sensori imbarcati sono lo strumento di sorveglianza più importante nelle fasi di pattugliamento e di intervento in mare. Queste tipologie di sensori includono radar attivi, telecamere ottiche e a infrarossi, sensori di sorveglianza passiva, sensori laser; i dati che essi generano, unitamente a quelli dei sistemi collaborativi (quali AIS, LRIT) e, quando disponibili, alle informazioni di sistemi aerei, formano la base di dati *real time* su cui strutturare la generazione della situazione marittima.

La detezione elettromagnetica (radar) ha, e continuerà ad avere, un ruolo centrale in virtù delle distanze raggiungibili e della possibilità di utilizzo in ogni condizione ambientale; i radar svolgono funzioni di sorveglianza di superficie (traffico marittimo) e di sorveglianza aerea (scoperta di velivoli a bassa quota). I miglioramenti prestazionali auspicabili riguardano la capacità di scoperta e tracciamento di bersagli piccoli, a distanze maggiori, da ottenere con sensori di costi relativamente contenuti. L'evoluzione tecnologica verterà sulle architetture delle antenne AESA (Active Electronically Scanned Array), sui nuovi componenti elettronici di potenza, sulle crescenti capacità di digitalizzazione e di elaborazione dei segnali, e sull'evoluzione dei sistemi di sorveglianza passiva.

Il successo dei sensori elettro-ottici è stato legato inizialmente alla loro capacità di detezione e di identificazione giorno-notte; il loro utilizzo si è quindi esteso a funzioni di sorveglianza, di inseguimento e di guida. Ai fini della sorveglianza marittima e costiera sono in particolare di interesse i possibili miglioramenti nelle capacità di identificazione a lunga distanza e di sorveglianza omnidirezionale con rilevamento automatico dei bersagli e delle minacce; si attende inoltre una maggior integrazione dei sensori elettroottici nella catena di sorveglianza.

Technology Relevance:

1. Architetture antenne attive per radar multifunzione [200-17; 201-9]
2. Componenti di potenza e tecnologie per moduli T/R [107-5]
3. Modi radar passivi e multi statici [103-1; 200-17; 217-5]
4. Architetture e algoritmi di *signal processing* [116-1]
5. *Inverse synthetic aperture* radar [200-17; 217-5]
6. Tecnologie elettro-ottiche per l'identificazione a lunga distanza e l'inseguimento automatico dei bersagli [108; 202-2; 202-3; 214-8]
7. Sistemi elettro-ottici di sorveglianza omnidirezionale con capacità autonome di individuazione dei "bersagli" [108; 202-2; 202-3; 214-8]
8. Tecnologie laser per la generazione di immagini 2D o 3D dei bersagli [200-22]
9. Modellazione e simulazione di architetture di sorveglianza integrata multi sensore per l'analisi delle prestazioni e l'ottimizzazione delle soluzioni [114-5]

Settori Guida di riferimento: 6

Area Tecnologica 2: Comunicazioni

Per ***Comunicazioni*** si intende l'insieme di *terminali, apparati, reti e infrastrutture* adibiti alla trasmissione di dati, di vario genere, insieme al *layer di tecnologie e applicazioni* a supporto dello scambio di informazioni.
L'esigenza è quella di soluzioni chiavi in mano sicure, integrate e interoperabili per la trasmissione di voce e dati, che mettano insieme tecnologie abilitanti differenti, tra cui gli standard radio digitali TETRA e DMR e l'ultima generazione di radio a banda larga wireless. In particolare è necessario costruire soluzioni di rete multi tecnologiche che assicurino all'utilizzatore una connettività trasparente in tutte le circostanze, e che migliorino l'efficienza di operazioni di pubblica sicurezza, servizi medici d'urgenza, di agenzie per la protezione civile e di applicazioni per la sicurezza nazionale.

In risposta alla domanda crescente di sicurezza debbono essere sviluppate aree tecnologiche pensate appositamente per rispondere alle esigenze specifiche del settore e accrescere efficienza, sicurezza, qualità e tempestività delle operazioni. Le soluzioni al problema della security dovranno essere affidabili, flessibili e solide, nonché per interfacciarsi con altre reti, sistemi e strumenti. Le applicazioni comprendono telemetria, localizzazione automatica del veicolo, trasferimento di video e accesso a banche dati.

La molteplicità degli scenari operativi fa si che i requisiti principali per le comunicazioni siano quelli di:

- Interoperabilità,estesa ai vari livelli (tra differenti gruppi di attori, in una operazione congiunta, di policies e practises, etc) ;
- Sicurezza delle Comunicazioni -dati scambiati in maniera tale da evitare perdita, danneggiamento o dispersione dell'informazione trasmessa-;
- Disponibilità -in termini di qualità del servizio di trasmissione dell'informazione, QoS-
- Resilienza, in termini di robustezza dell'infrastruttura di Comunicazione, che dovrà essere in grado di operare anche in situazioni critiche.

Le tecnologie per le Comunicazioni includono:

Terminali e apparati:

- Terminali di comunicazione :
  - radio analogiche (HF, VHF, UHF etc);
  - radio digitali (APCO);
  - terminali TETRA;
  - smartphone
- Apparati di routing e switching;
- Datalink per piattaforme Robotizzate;

Reti e Infratrutture di Comunicazione:

- Rete radio analogiche;
- Reti radio digitale;
- Rete TETRA;
- Reti di Comunicazioni WiFi (WLAN, MANET, Reti Mesh);
- WiMAX;
- Reti di Comunicazioni satellitari;
- Comunicazioni short-range(RFID, Bluetooth, UWB);
- Tecnologia IP-based;
- Reti di Comunicazione cellulare (GSM, UMTS);
- Reti integrate (ad esempio. Software Defined Radio integrata terrestre/satellitare);

Layer di Tecnologie e Applicazioni:

- Tecnologie per la trasmissione/compressione di dati (Disponibilità);
- Tecniche di diffusione dell'informazione anche in condizioni critiche e/o di emergenza (Disponibilità);
- *Middleware*, per integrazione di reti e sistemi esistenti in un unico substrato (Interoperabilità);
- Protezione da *jamming* (Sicurezza);
- Reconfigurabilità delle reti (Resilienza);

I diversi tipi di servizi e di applicazioni dovranno assicurare i requisiti di Interoperabilità, Resilienza, Disponibilità e Sicurezza necessari nel dominio delle Comunicazioni.

TA2.1 Sistemi di trasmissione dati da mezzi in movimento

La trasmissione di dati proveniente da/verso mezzi in movimento, necessariamente basata su tecnologie wireless, costituisce una rilevante sfida tecnologica a causa della variabilità e della distorsione delle trasmissioni in radiofrequenza, dovute al *multipath* e alla temporanea ostruzione fisica. Nel caso delle reti terrestri, tali effetti indesiderati possono essere alleviati grazie a una diffusione capillare sul territorio di punti di accesso alla rete. Tuttavia, questo approccio produce una maggiore frequenza di transizione di cella, con conseguente abbassamento del livello di qualità del servizio, dovuto alla necessità di effettuare le procedure di *handover* e autenticazione.

Per quanto riguarda il trasporto ferroviario, un numero molto ridotto di treni, in particolare solo quelli su linee compatibili con standard ETCS livello 2, è equipaggiato con un sistema di radiocomunicazione che mantiene costantemente il contatto con delle stazioni di terra tramite una rete dedicata GSM-R, che consente il riscontro dei dati telemetrici e una maggiore robustezza a sabotaggi e attacchi rispetto a quelli tradizionali. Per tutti gli altri, sarebbe auspicabile la definizione di una tecnologia che consenta l'equipaggiamento dei treni con un sistema di localizzazione geografica autonomo e il collegamento in radiocomunicazione, lungo tutto il percorso, con un centro di controllo remoto, per la referenziazione dei dati e l'invio/ricezione di comandi o allarmi non rilevabili altrimenti a causa di., manomissioni, emergenze etc. Relativamente al trasporto su strada e multimodale, un incremento significativo della sicurezza deriverebbe dalla diffusione su larga scala di sistemi cooperativi, finalizzati alla diffusione e condivisione di dati provenienti dai mezzi di trasporto. Tali dati devono essere fruibili in tempo reale per la realizzazione di servizi quali: la prevenzione di incidenti grazie a sistemi di guida assistiti (ad esempio, distanza di sicurezza, decelerazione automatica su ostacolo); la localizzazione dei mezzi e del contenuto trasportato; la gestione dinamica del traffico per favorire la rapidità di intervento in eventi a rischio, per l'incolumità di persone, beni o siti sensibili. I protocolli e le applicazioni che abilitano tali servizi devono essere sicuri, al fine di evitare un utilizzo improprio, da parte di soggetti intenzionati, a causare disagio o creare attacchi. Per aumentare la copertura su strada, è in corso di sperimentazione la tecnologia IEEE 802.11p/WAVE, che consente la comunicazione tra veicoli e stazioni a bordo strada: tale tecnologia può integrarsi con altre terrestri a maggiore raggio di copertura (ad esempio. reti cellulari/ WiMAX,/satellitari, oppure DVB-SH per la ricezione di dati in multiplexing da un centro di controllo).

Una particolare attenzione dovrà essere riservata alle tecnologie di comunicazione relative al segmento aeronautico in cui l'esigenza di security si combina con quella di Safety.

Technology relevance

1. Comunicazione autovetture a banda larga [413-4]
2. Broadband wireless access: [413-6]
3. Interoperabilità e *handover* verticale: [416-15]
4. Integrazione di tecnologie cellulari - 2G, 2.5GGSM, TETRA, GSM-R, GPRS, UMTS, TETRA2 - [413-2; 413-4]
5. Tecnologie cellulare: HSxPA, LTE [413-2]
6. Tecnologie comunicazione aeronautica: LDACS, VDL, AeroMACS [413-4]
7. Sistemi di navigazione satellitari: GPS, Galileo, EGNOS, PRS [205-5]
8. Tecnologie per trasmissione dati integrata satellitare/terrestre: DVB-SH [118-3]
9. Tecnologie per la trasmissione/compressione di dati per il monitoring "real-time" di immagini riprese a bordo di veicoli presso punti di controllo a terra. .[112-2;113-3]
10. Implementazione di carri merci provvisti di sistemi di intercomunicazione e di controllo remoto [501A-2]

Settori Guida di riferimento: 3,4,8

TA 2.2 Reti wireless ad-hoc e di sensori

Le reti *wireless ad-hoc* e le *sensors network* rappresentano un'area di enorme interesse grazie ai numerosi scenari applicativi identificati nei settori guida di SERIT, dai quali deriva la necessità di integrare nel progetto sia le tecnologie sia le diverse applicazioni di sicurezza.
I requisiti emergenti dai diversi contesti operativi implicano lo sviluppo di funzionalità di *sensing*, di elaborazione e riconoscimento dei segnali, di rilevazione eventi e generazione automatica di allarmi, di stima e controllo di fenomeni e/o processi distribuiti spazialmente, di trasporto dell'informazione in presenza di restrizioni energetiche, trasporto dell'informazione in condizione di assenza totale/ parziale di infrastrutture di rete dedicata, resilienza della rete a guasti e interruzioni di collegamento. Lo sviluppo dovrà avvenire secondo modalità di *design* di tipo *cross-layer*, con una considerazione congiunta delle tecniche di elaborazione dei dati e segnali in modalità distribuita, dei meccanismi di accesso al mezzo wireless, e infine dei protocolli di comunicazione, utilizzati sia a livello di rete che di trasporto. In particolare, è di specifico interesse nel contesto SERIT la progettazione e lo sviluppo di tecnologie, algoritmi, protocolli e soluzioni per reti di sensori e, più in generale, *reti ad hoc* (includendo reti tolleranti ai ritardi ed alle disconnessioni, VANET e *reti mesh*), sicure e resistenti agli attacchi ed agli incidenti, con capacità di auto-organizzazione ed auto-riparazione in caso di malfunzionamenti, e con funzionalità avanzate di protezione dell'integrità e della confidenzialità dell'informazione gestita, trasmessa, ed elaborata da sensori/attuatori.
E' inoltre centrale lo sviluppo di nuovi sistemi integrati di reti wireless, di sensori/attuatori per il monitoraggio affidabile delle condizioni di sicurezza ed integrità di strutture, ambienti e processi, e per la trasmissione, gestione, ed elaborazione di allarmi e controlli.

Technology relevance

1. Reti ad hoc: livelli fisici 802.11a/b/g/n/ac/ad e protocolli di routing; [200-30; 413-2]
2. Reti mesh: estensioni 802.11/s e protocolli di routing, [200-30; 413-2]]
3. Reti DTN: Protocolli Bundle, DTN, DTN2 [200-30; 413-2]
4. Reti di sensori: tecnologia 802.15.4, protocolli ZigBee e 6lowPAN, Bluetooth, [200-30; 413-2]
5. Reti di sensori e DTN: protocollo IETF ROLL, [200-30; 413-2]
6. Sicurezza integrata in reti di sensori e reti ad hoc: implementazioni efficienti per ECC, IBC, AES, etc, [200-30; 413-4]

Settori Guida di riferimento: 4,8,10

TA2.3 Sistemi per la diffusione delle informazioni in situazioni critiche

Nella realtà contemporanea, la confidenzialità delle informazioni assume sempre maggiore rilevanza non soltanto in ambito militare e del Segreto di Stato ma anche in condizioni quotidiane di vita civile. Basti pensare a:

- organismi di salvaguardia dell'Ordine Pubblico (come le forze di Polizia e Vigili del Fuoco) o di salvaguardia della popolazione e del territorio (Protezione Civile). In questo settore è sempre più rilevante la necessità di proteggere alcune delle informazioni raccolte e trattate da queste organizzazioni per il carattere vitale che tali informazioni possono avere rispetto al benessere della popolazione e alla preservazione dei servizi. Data l'integrazione sempre più stretta tra queste strutture, si pone altresì l'esigenza di permettere un flusso controllato di informazioni tra le differenti reti di dati impiegate.
- banche o altre aziende di servizi;anche in questo caso è indispensabile sia proteggere le informazioni da accessi indesiderati o potenzialmente pericolosi sia scambiarsi informazioni in modo controllato e sicuro per una migliore efficienza del sistema globale dei servizi.
- Infrastrutture critiche comunicanti quali i sistemi di distribuzione dell'energia;

Risulta pertanto sempre più utile applicare anche in ambito civile paradigmi già sperimentati con successo nella Sicurezza Militare, rafforzandoli attraverso l'adozione di tecnologie innovative.

In particolar modo è oggi possibile ipotizzare e realizzare architetture SW capaci di separare reti a diverso livello di confidenzialità garantendo, nel contempo, uno scambio controllato di informazioni. Tali architetture, tradizionalmente basate su server di perimetro, si possono oggi progettare utilizzando gli strumenti che i nuovi sistemi operativi multilivello mettono a disposizione. Si tratta di sistemi operativi che permettono la separazione delle informazioni a livello spaziale e temporale in modo completo e garantiscono (su una stessa macchina di dimensioni ridotte e di tipo consumer) la completa indipendenza dei flussi di dati appartenenti a reti di organizzazioni diverse.

Technology relevance

1. Architetture a livello multiplo di confidenzialità per garantire la separazione di reti di dati contenenti informazioni sensibili in ambito civile, [117-18; 413-3]
2. Creazione di applicativi in grado di presiedere alla comunicazione controllata tra tali reti, [117-18; 416-13]
3. Architetture SW capaci di permettere lo sviluppo di applicazioni e reti di dati operanti a diverso livello di confidenzialità [416-13; 116-1]
4. sistemi operativi partizionati e multilivello, [116-6]
5. applicativi di verifica e controllo del transito di informazioni tra reti a diverso livello di confidenzialità [117-18]

Settori Guida di riferimento: 6,13

TA2.4 Integrazione del segmento satellitare a supporto di applicazioni evolute

In diversi ambiti civili sta crescendo sempre di più l'esigenza di poter comunicare efficacemente scambiando dati acquisiti ed informazioni nelle condizioni più diverse, al fine di gestire situazioni di crisi o di sorvegliare il territorio in maniera più efficace, riducendo drasticamente sia il rischio per la vita umana che i costi. Tale esigenza può essere soddisfatta solo se si riesce a disporre di infrastrutture di telecomunicazioni particolari basate su accesso satellitare, da far operare in situazioni e contesti altrettanto critici, come una zona terremotata o geologicamente dissestata, oppure semplicemente per poter sorvegliare in maniera più continuativa uno specifico territorio esteso.

L'introduzione di veicoli aerei senza pilota - *Unmanned Aerial Vehicle (UAV)* - è stata la prima e significativa risposta all'esigenza sopra descritta. Già in ambito militare i velivoli senza pilota hanno conosciuto una sensibile evoluzione tecnologica che li rende oggi, in quanto a manovrabilità ed efficienza, simili ad aerei con pilota. L'Italia è tra quelle Nazioni che, con la propria industria aeronautica è in grado di proporre nuovi modelli di UAV per applicazioni sia militari che civili, mirate, quest'ultime, all'utilizzo da parte della Protezione Civile Nazionale o di altri Enti preposti alla gestione di crisi o a compiti di sorveglianza.

Gli UAV utilizzati per la sorveglianza, possono ospitare come carico utile diversi sensori quali radar ad apertura sintetica, telecamere operanti nel visibile e nell'infrarosso. L'attività che si propone è quella di definire un sistema di rete basato su accesso satellitare che realizza un'infrastruttura di telecomunicazioni utilizzando dei terminali installati a bordo di UAV, in grado di sorvolare aree di cui acquisire dati d'immagini (visibile, infrarosso, radar) e misure (campi elettromagnetici, dati meteorologici, etc.), facendoli convergere attraverso il satellite a centri di raccolta ed elaborazione, anche geograficamente remoti rispetto all'area di sorvolo, e garantendo flussi dati con prestazioni elevate (alto affidabile e *bitrate*). Tale rete d'accesso potrà, a sua volta, essere connessa con altre reti terrestri e/o satellitari tramite cui diffondere i dati acquisiti.

Technology relevance:

1. sistemi di comunicazione (anche satellitare) [217-1]
2. sistemi aerei senza pilota [UAV] estendendone le loro capacità operative grazie al satellite [403-6]
3. tecniche di trasmissione dati ad alta efficienza e qualità. [112-2; 113-3]
4. tecnologie per la trasmissione sicura dell'informazione [crittografia] di nuova concezione. [117-3]
5. Tecniche anti-jamming in ambito "connettività satellitare". [113-10]
6. Potenziamento delle infrastrutture di gestione crisi e sorveglianza grazie a tecniche combinate satellite-UAV. [411-2]
7. PRS, comunicazione e dati a supporto di applicazioni evolute [205-5]
8. Studio applicazione IPv6 su satellite [416-13; 413-4; 116-2]

Settori Guida di riferimento: 3,8

TA2.5 Architetture evolutive dei sistemi di comunicazione per first responders

Le architetture di comunicazione dedicate alla gestione delle emergenze richiedono un'infrastruttura di comunicazione cooperativa sicura che consenta la gestione delle comunicazioni voce e dati, ovvero lo scambio di informazioni tra sistemi di tecnologie differenti in scenari di crisi a supporto del personale operativo e specialistico chiamato a gestire le particolari condizioni di emergenza. Tali sistemi di comunicazioni devono poter operare anche in situazioni in cui le infrastrutture di rete pre-esistenti possono risultare parzialmente o completamente danneggiate dall'evento che ha causato l'emergenza.
La soluzione di Middleware insieme all'architettura di comunicazione deve garantire all'utente l'accesso a servizi ed applicazioni complesse, implementando l'integrazione di sistemi caratterizzati da specifiche funzionalità operative che utilizzano tecnologie di comunicazione differenti.
L'accesso alle comunicazioni ed ai relativi servizi dovrà, indipendentemente dalle tecnologie utilizzate, garantire una qualità del servizio adeguata alle specifiche applicazioni richieste.
In particolare, il *middleware* di comunicazione dovrà essere in grado di erogare comunicazioni di tipo Network Centric, utilizzando servizi di comunicazione sicuri, integrati ed interoperabili, basati su sistemi appartenenti a diversi enti governativi, civili e militari, tra cui i Sistemi di comunicazione:

- di tipo tattico e strategico;
- navali e avionici;
- PMR (Professional Mobile Radio);
- del traffico aereo (ATC/ATM).

La soluzione middleware consentirà di raccogliere dai sistemi di telecomunicazione wireless integrati, dati provenienti da diverse stazioni di monitoraggio, che potranno essere poi tempestivamente distribuiti sia ai centri di Comando e Controllo, sia agli enti competenti, in maniera indipendente dalla particolare tecnologia di accesso.
I *media router* consentiranno di realizzare una rete mesh utilizzando tutte le opportunità di comunicazione disponibili, ottimizzando la gestione della QoS dei diversi servizi di comunicazione. I servizi che la piattaforma metterà a disposizione sono:

- I servizi di comunicazione Unificati, che consentiranno la gestione delle comunicazioni tra gli utenti dei diversi domini;
- L'integrazione di dati relativi al monitoraggio e al controllo;
- Una piattaforma dedicata allo sviluppo di servizi che nasceranno da esigenze future legate all'interoperabilità
- Una specifica attenzione alle soluzioni e alle tecnologie a supporto della comunicazione e della localizzazione *indoor* da utilizzare in operazioni di *rescue*. In presenza di strutture sotterranee infatti, come metropolitane o gallerie, o qualora occorra comunque intervenire dall'interno ,le attuali tecnologie non sono in grado di garantire adeguatamente lo scambio di informazioni da e tra *first responding*.

Technology relevance (max 10)

1. Sistemi Wireless (p.e. da TETRA a TETRA2 o a nuovi standard) [416-2; 413-6]
2. Interoperabilità delle reti di emergenza reti unificate tipo E-112 [416-16]
3. Interoperabilità su IP di reti esistenti [416-13]
4. Sistemi di comunicazione indoor (deployment e deployable) per emergenza. [413-2]

Settori Guida di riferimento: 6

TA2.6 Middleware, architetture di rete e comunicazione (Network Centric Communication), per l'integrazione di reti e sistemi eterogenei

In scenari di gestione della crisi o di sorveglianza del territorio, i dati e le informazioni sensibili, di esclusiva pertinenza di un sistema, devono essere scambiati tra enti certificati, utilizzando un framework di autenticazione distribuita. Questo *framework* di integrazione metterà a disposizione alcuni servizi , indipendenti dalla tecnologia di comunicazione utilizzata, e consentirà un livello di astrazione, tramite l'esposizione su un livello di *middleware*,di servizi condivisibili da applicazioni dedicate, a supporto degli utenti e degli operatori coinvolti.
All'interno del *framework* saranno inoltre integrati i sistemi di comunicazione Wireless, in modo da consentire,alle applicazioni "terze parti" e agli utenti, la disponibilità dei servizi di comunicazione wireless in modo unificato. Tali servizi includeranno la messaggistica, le chiamate di gruppo e la localizzazione. I servizi potranno essere utilizzati da terze parti tramite o meccanismi di *publish/subscriber*, riservati ai soli sistemi ed utenti autenticati, oppure meccanismi di *request/replay* , riservati agli utenti che potranno richiedere informazioni puntuali e necessarie alla gestione delle emergenze.
Tale *framework* di comunicazione consente lo scambio di informazioni riservate per monitorare e gestire scenari di emergenza, tramite l'introduzione e lo sviluppo di servizi elementari che potranno essere utilizzati da una "centrale di coordinamento", che funge da interfaccia tra tutti i sistemi per la gestione degli scenari di emergenza.
L'impiego di architetture SOA e *Web Service* sono giustificate dal fatto che in tali scenari la centrale di coordinamento potrebbe essere ogni volta diversa e dipendente dal tipo di scenario di crisi. (es. Protezione Civile, Organismo NATO,…)

Technology relevance (max 10):

1. Framework dei servizi di comunicazione con tecnologia SOA a Web Service; [116-4; 116-6]
2. Sistemi di comunicazione wireless con tecnologia Tetra/TEDS/TETRA2 ;[416-3; 416-16]
3. Sistemi di comunicazione wireless con tecnologia DMR [416-3; 416-16]
4. Sistemi di comunicazione wireless con tecnologia WIMAX [416-2; 413-6]

Settori Guida di riferimento: 2,3,6

TA2.7 Studio architetture Software Defined Radio & Cognitive Radio per applicazioni di sicurezza

Le operazioni nelle quali gli operatori di Public Security generalmente operano possono ricondursi ad una delle seguenti aree:

- urbane o sub-urbane, dove le radio comunicazioni devono essere ristabilite solo localmente, ad una estensione massima equivalente al più a qualche cella GSM. In questa situazione, il backbone è ancora attivo e deve essere eseguita una adeguata gestione dello spettro (*spectrum sharing and policies adoption referred to primary and secondary users*);
- isolate, dove il ripristino delle radio comunicazioni richiede maggiori risorse e tempo, ma con minori vincoli di gestione dello spettro;
- zone di confine; se queste sono assimilabili ad uno (o entrambi) i casi precedenti, devono essere applicate specifiche regole (*policies*) per operazioni di cross-border.

Le predette situazioni richiedono l'interoperabilità tra mezzi di comunicazione e tra operatori. Ciò coinvolge i sistemi di comunicazione usati in questo contesto, dove in Europa sono diffusi gli standards TETRA e TETRAPOL (tra loro non interoperabili), nonché le procedure di intervento, la gestione delle informazioni ed il piano delle frequenze da utilizzare non ancora standardizzato per applicazioni *wideband* e *broadband*. Questi elementi giustificano pienamente l'opportunità di dotare gli operatori di dispositivi per le radio comunicazioni aventi capacità di riconfigurabilità tale da permetterne l'adattamento ai diversi standard europei nonchè internazionali (come. APCO P25) e l'adattamento di *policies* da usare nei specifici contesti. Per la realizzazione delle componenti di trasporto radio una rete di comunicazione, ossia i terminali *handheld* e le base-stations, è quindi necessario adottare architetture software e relativi componenti hardware che permettano di rendere allo stato dell'arte le capacità di riconfigurazione.

Technology relevance

1. Architetture SW capaci di permettere lo sviluppo delle componenti di applicazioni, servizi e *waveforms* non dipendente dalle componenti HW, al contrario favorendo la "*new technology insertion*" [116-2; 116-3; 116-4]
2. *Real Time Operative System* [116-5]
3. *Middleware* e *Application Program Interfaces*[116-1; 116-4]
4. *Programmable Processing Elements* [116-8]

Settori Guida di riferimento: 8

TA2.8 Protezione e disturbo del canale di trasmissione dati

I canali usati per la trasmissione dei dati/informazioni sono sempre più vulnerabili e soggetti a disturbi di interferenze sia involontarie che volontarie. In particolare le interferenze volontarie rappresentano una minaccia che rende l'infrastruttura di comunicazione sempre più vulnerabile. Il numero di incidenti dovuto a interferenze intenzionali continua a crescere soprattutto a causa della disponibilità di disturbatori facili da costruire, abbastanza economici o addirittura acquistabili via internet. Alcuni di questi, più sofisticati, adottano tecniche di inganno (*spoofing*, *meaconing*).

Tenendo presente l'uso sempre più massivo dei canali satellitari civili, che non rispondono agli stringenti requisiti di sicurezza come quelli militari, e che di conseguenza si stanno connotando come infrastruttura critica, nasce l'esigenza di sviluppare tecnologie a tutela di minacce di tipo intrusivo e a garanzia dei notevoli investimenti fatti sia in ambito Europeo (e.g. GALILEO e GMES) che in ambito commerciale. Ad esempio i servizi GNSS [1]sono diventati essenziali per il trasporto aereo, terrestre, e operazioni marittime nonche' per la salvaguardia della vita umana nelle operazioni di soccorso. I segnali sui canali radio GNSS sono estremamente deboli e le trasmissioni possono essere facilmente compromesse dalla presenza di disturbi, anche di bassa potenza, sia intenzionali che accidentali. Un disturbatore di bassa potenza (< 1 W) può inibire l'acquisizione dei segnali di navigazione entro un raggio di decine di chilometri

Per contrastare questa minaccia e' necessario irrobustire dove possibile i canali di trasmissione e, ove cio' non sia possibile come sui servizi civili, disporre di una rete di monitoraggio nazionale, in particolare a protezione dei servizi Galileo, basata su sensori e localizzatori distribuiti sul territorio in grado di rivelare emissioni da disturbatori di canale.

Altri servizi che stanno diventando parte del nostro sistema di protezione civile e in generale di sicurezza sono relativi ai sistemi di telecomunicazione e di osservazione e per i quali in Italia possiamo sfruttare l'*heritage* tecnologico di COSMO SkyMed (sistema duale di ultima generazione con elevatissimi livelli di sicurezza) e nell'ambito di questa capability si intende sviluppare un sistema di protezione completo ad uso civile a costi idonei ed in grado di soddisfare i requisiti di sicurezza più stringenti e le esigenze di sicurezza nazionale, focalizzandosi in particolare *sull'improvement* delle capabilities tecnologiche di base e design e *testing* di apparati terra / bordo implementanti funzionalità di sicurezza.

Technology relevance:

1. Tool software di simulazione [114-5]
2. Ricevitori per la rilevazione e localizzazione di segnali modulati con tecniche convenzionali, ad espansione di spettro, e con tecniche di inganno [201-7; 201-8]
3. Antenne *phased array* a controllo digitale [201-7; 201-8]
4. *Design* e *testing* apparati terra / bordo implementanti funzionalità di sicurezza
5. Tecniche di correlazione segnali ricevuti da più ricevitori per analisi, localizzazione, identificazione del disturbo.[113-3; 113-4]
6. Modelli evoluti di Analisi del Rischio applicati ai sistemi spaziali [412-3]
7. *Hardening* ed integrazione Algoritmi Cifratura [117-3; 117-4]

Settori Guida di riferimento: 8

[1] GNSS (*Global Navigation Satellite System* o GNSS) è l'espressione usata correntemente per descrivere i sistemi di navigazione che utilizzano satelliti artificiali che forniscono un servizio di posizionamento geo-spaziale a copertura globale basato su informazioni radio, quali GPS e Galileo.

TA2.9 Architetture di rete orientate al fast deployment

Diversi scenari applicativi rilevanti per il contesto della Security, richiedono la possibilità di dispiegare dei sistemi di comunicazione "*on demand*" in modo rapido ed affidabile.

Questi requisiti possono essere soddisfatti solo utilizzando architetture di rete di tipo *autonomic*, con funzionalità avanzate per l'identificazione delle risorse disponibili ai vari livelli della rete (ad es., collegamenti, apparati, servizi, etc.), e di auto-configurazione delle stesse. Il sistema di comunicazione dovrebbe inoltre essere dotato di soluzioni altamente flessibili ed adattabili, in modo da poter supportare diversi scenari d'uso, modalità operative e servizi, con la capacità di commutare automaticamente tra le varie modalità di funzionamento.

Questa flessibilità può essere ottenuta attraverso piattaforme *middleware* che utilizzano astrazioni di alto livello per descrivere lo stato delle risorse della rete ed i servizi da supportare, e che si appoggiano su un insieme di regole di preferenze e strategie per associare ciascuna delle astrazioni di alto livello all'insieme dei paradigmi di comunicazione disponibili. Questo approccio consentirà di realizzare un architettura di rete modulare, facilmente estendibile e adattabile a vari scopi.

Per quanto riguarda i paradigmi e le tecnologie di comunicazione, una rete orientata al *fast deployment* dovrà necessariamente minimizzare il ricorso a tecnologie di comunicazione cablate,per prediligere collegamenti wireless (sia di corto/medio raggio che di lungo raggio) e modelli di comunicazione di tipo auto-organizzante. Infatti, nelle reti auto-organizzanti, le comunicazioni possono avvenire anche senza il supporto di apparati di rete dedicati e server centralizzati, ma sfruttando comunicazioni *peer-to-peer* tra i dispositivi wireless.

Tuttavia, è necessario definire un substrato abilitante a supporto delle operazioni si integrazione delle varie piattaforme, partendo dalle reti *mesh* che garantiscono il trasporto dell'informazione su aree limitate (ad es. coperture cittadine) fino a piattaforme navali, aeree e satellitari per il trasporto dell'informazione su lunghe distanze.

Technology relevance:

1. Protocolli di *routing* adattativo [413-5]
2. Applicazione di concetti *Peer to Peer like, flooding* e di management autonomico [116-10; 411-6; 413-1; 413-5]
3. Tecnologie per l'interoperabilità del segmento terrestre/wireless con quello satellitare [301B-1; 416-3]
4. Tecnologie di interoperabilità ed accesso wireless basate su requisiti di *fast deployment* (ad esempio ponti radio auto-configuranti, sistemi No LOS/ BLOS); [416-2]
5. Reti self healing e mesh [416-10]

Settori Guida di riferimento: 6

TA2.10 Sicurezza di Rete

La crescente disponibilità di banda passante, unità ai sempre minori costi di connettività ed alla disponibilità sempre maggiore dei punti d'accesso, ha fatto delle moderne reti di comunicazione il vero e proprio sistema nervoso del pianeta. Eppure anche queste architetture hanno il problema della sicurezza.

Proprio perché "reti aperte", le reti digitali sono intrinsecamente insicure: esse non sono state progettate in modo da garantire autoprotezione e difesa contro eventuali abusi. Ne discende che esse sono particolarmente sensibili all'intercettazione ed all'alterazione dei dati trasmessi nonché alla violazione dei supporti informatici ad essa connessi.

Senza garanzie adeguate l'utente non avrà incentivi all'utilizzo di tali tecnologie che, sebbene siano più convenienti, sono anche più insicure.

Inoltre il desiderio dell'utente di garantire la propria riservatezza e anonimato mal si concilia con la necessità di imputabilità, cioè la possibilità effettiva di conoscere l'identità degli utenti e di ciò che stanno facendo.

Ideale sarebbe trovare un giusto bilanciamento fra queste diverse esigenze e tale compromesso dovrebbe essere attentamente protetto.

D'altra parte le cronache di tutti i giorni riportano con sempre maggiore frequenza notizie relative ad intrusioni perpetrate ai danni di sistemi informatici più o meno noti e non passa settimana in cui i principali bollettini di sicurezza non danno rilevanza alla scoperta di pericolosi bug od exploit destinati ad essere prontamente sfruttati per portare a compimento attacchi di vario genere.

Dalla combinazione di questi ed altri fattori possiamo trarre lo spunto per fare una semplice osservazione: acquisire visibilità sulla rete significa purtroppo accrescere le probabilità di vedere, prima o poi, il proprio server violato da qualcuno.

Sfortunatamente non esistono dei rimedi nè delle tecniche tali da poter rendere sicuro al 100% un sistema od una rete contro gli attacchi provenienti dall'esterno ma, ciò nonostante, si può ancora operare per tenere lontani molti problemi e vulnerabilità.

Per fare ciò occorre innanzitutto comprendere la natura e la portata dei pericoli ai quali ci si espone e successivamente adottare delle precauzioni di carattere generale dirette a circoscrivere i rischi suddetti entro limiti accettabili in relazione alla natura degli interessi da proteggere

Per questo è necessario sviluppare metodologie, tecnologie e sistemi per il monitoraggio di grandi architetture di rete (anche includendo reti per applicazioni dedicate – ad esempio reti per la trasmissione di energia) e di analisi e classificazione del traffico e delle applicazioni e comportamenti in rete, al fine di rilevare, diagnosticare, prevenire, e mitigare (anche in modo automatizzato per una maggiore reattività) intrusioni, attacchi, frodi, *maleware*, anomalie, incidenti.

Technology relevance

1. Modelli evoluti di Analisi del Rischio [412-3]
2. *Hardening* ed integrazione Algoritmi Cifratura [117-3; 117-4]
3. Design e *testing* apparati implementanti funzionalità di sicurezza [117-12; 117-13; 117-14]
4. Tool SW di simulazione [114-5; 115-6]
5. Tecnologie e soluzioni per Intrusion Detection, Intrusion Prevension, mitigazione [117-8]
6. Sonde di monitoraggio [117-8]
7. Protezione di rete mediante sistemi di difesa perimetrale e di controllo di accesso [117-3; 117-4]
8. Progettazione di algoritmi; protocolli, servizi ed architetture per la sicurezza delle reti e delle comunicazioni [117-3; 117-4]

Settori Guida di riferimento: 2,5

Area Tecnologica 3: Detection & Identification Systems

Nella loro accezione più comune, i termini “detection” e “identification”, pur appartenendo entrambi ad uno specifico contesto della sicurezza, hanno insistito generalmente fino ad oggi su settori applicativi differenti.

Mentre infatti la “detection”, in italiano “individuazione” o meglio “rilevazione”, potrebbe essere definita, nel contesto della sicurezza in oggetto come la determinazione e trasmissione da parte di un sistema che un evento si è verificato (dalla scoperta della presenza di oggetti pericolosi in un pacco a la rilevazione di un comportamento anomalo da parte di un essere umano), l’”*identification*”, in italiano “ identificazione” si pone più precisamente l’obiettivo di attribuire una identità ad un oggetto (ad esempio con l’uso di RFID) o ad una persona (ad esempio attraverso l’uso di tecnologie biometriche).

La stessa identificazione nel contesto della sicurezza ha un significato molto vasto che spazia dal generico campo dell’accreditamento all’accesso di luoghi o servizi fino ad arrivare alla specifica accezione nel contesto delle tecnologie biometriche che separa nettamente “identificazione” e “verifica di identità” dando alle due modalità operative specifiche molto differenti, sia dal punto di vista tecnico che delle implicazioni legali e sociali.

In termini generali, I sistemi di Detection e Identification consentono di:

- Rilevare anomalie in diversi contesti, grazie alla raccolta di dati da differenti fonti e alla successiva analisi
- Riconoscere persone ed asset, attraverso le tecnologie biometriche o documenti di identità elettronici per le persone e attraverso tecnologie eterogenee per gli asset;
- Individuare potenziali minacce, congiuntamente ai sistemi di Sorveglianza e Situation Awareness.

Con il sempre più stringente bisogno di sicurezza le tecniche basate sulla “detection” e “identification” stanno rapidamente trovando una serie di applicazioni in settori cruciali come lo screening di un container, i controlli automatici di frontiera o la evidenziazione di individui che hanno recentemente utilizzato armi da fuoco. “Detection” e “identifcation” possono altresì essere usati in maniera convergente, ad esempio nel contesto della sicurezza del trasporto pubblico. Un conducente di un mezzo di trasporto potrebbe essere inizialmente identificato con una tecnologia di tipo biometrico, per essere certi che abbia la titolarità alla guida e, allo stesso tempo, adeguati sistemi di detection potrebbero monitorare il suo stato di guida per prevenire le conseguenze di una diminuzione di attenzione o di uno scostamento significativo da parametri di “normalità” che, ad esempio, potrebbe essere l’indicatore di una guida sotto minaccia.

Una classificazione applicativa delle tecnologie per la “detection” e “identification” le divide in:

Sistemi di detection e identification relativi al dominio “persone”:

- Sistemi di identity management;
- Sistemi per accreditamento e screening (in correlazione ai sistemi di sorveglianza e information management e per applicazioni di controllo di frontiera);
- Sistemi per il riconoscimento di caratteristiche biometriche (ad esempio impronte digitali, volto, iride, dinamica di apposizione della firma o voce);
- Sistemi per la verifica di documenti di identità elettronici;
- Body scanner;
- Sistemi per il riconoscimento di comportamenti “anomali” rispetto a un offset predeterminato.

Sistemi di detection e Identification relativi al dominio “oggetti”:

- Sistemi per la rivelazione di oggetti pericolosi o proibiti da specifiche normative di sicurezza
- Metal detectors;
- Radio Frequency Identifiers (RFID).

Sistemi ibridi di detection e identification, ad esempio:

- Sistemi per la validazione della titolarità agli accessi fisici o logici basati tecniche di identificazione biometrica e aggiornamento periodico delle credenziali sulla base di rilevazioni di caratteristiche comportamentali/biologiche allo scopo di prevenire possibili atti criminali o cali di attenzione del conducente.

TA3.1 Detection ed imaging di persone e oggetti attraverso gli ostacoli (fuoco, muri, smog, metalli e altro)

Questa area fa riferimento alle tecnologie in grado di rilevare la presenza di persone o di oggetti e, in presenza di ostacoli visivi, di identificarne la natura, sia in termini di proprietà fisiche (natura solida o gassosa) che morfologiche (estensione o forma). In particolare, le tecnologie impiegate sono basate sull'emissione di onde elettromagnetiche di differente lunghezza d'onda scelta in funzione della natura dell'ostacolo e del bersaglio. Per gli ostacoli solidi è usata una strumentazione in grado di emettere radiazioni in una porzione dello spettro elettromagnetico con una lunghezza d'onda compresa approssimativamente tra 10 nanometri (nm) e 1/1000 di nanometro (raggi X).

Questo tipo di irradiazione permette di penetrare varie sostanze solide come acciaio, legno, alluminio o fibra di vetro e il suo uso sta trovando interessanti applicazioni, oltre che nel settore militare, in quello dell'homeland security. Per tale banda di frequenze, l'obiettivo della ricerca riguarda lo sviluppo di strumentazioni portabili per la visualizzazione in tempo reale di sostanze e persone nascoste, possibilmente mediante basso dosaggio di radiazioni.

Per gli ostacoli di tipo gassoso invece viene generalmente usata una strumentazione che utilizza radiazioni nello spettro dell'infrarosso e, ad oggi, le applicazioni sono ancora dedicate per lo più al settore militare e a quello dell'aeronautica in condizioni di visibilità ridotta. Per tale tecnologia, l'obiettivo della ricerca mira allo sviluppo di videocamere all'infrarosso di basso costo, portabili e capaci di operare in uno scenario operativo.

Infine, va sottolineato come, allo stato attuale, le radiazioni non ionizzanti come onde radio e microonde risultano di rilevante interesse nel campo della visualizzazione oltre un ostacolo sia ai fini di operazioni di soccorso e recupero che di sorveglianza. In tale contesto operativo si possono distinguere due classi di sistemi: i primi sono basati sull'effetto Doppler e sono specializzati nel rilevamento e caratterizzazione di segni vitali di persone sepolte e/o oltre un ostacolo; i secondi sono orientati alla caratterizzazione della geometria dell'interno di edifici con conseguente rilevamento dei movimenti di persone mediante approcci basati su "*change-detection*" e modellistica elettromagnetica avanzata. Per tale tecnologia, gli obiettivi della ricerca riguardano l'adattamento delle soluzioni tecnologiche finora individuate, in termini hardware e di data processing, a scenari operativi caratterizzati da una notevole complessità sia dal punto di vista della diffusione elettromagnetica che della necessità operare in tempi rapidi con strumentazione portatile basata su un numero ridotto di sensori.

Technology relevance

1. Tecnologie basate sui raggi-X [110-02]
2. Tecnologie basate sui raggi Gamma [110-03]
3. Tecnologie basate su sensori a radiofrequenza [110-10]
4. Spettrografia all'infrarosso [110-05]
5. Sensori per tecniche di imaging e mapping [110-20]
6. Pattern recognition [113-02]
7. Tecnologie per la fusione di dati e informazioni [113-04]
8. Tecnologia di tipo Ultra-wideband (UWB) [200-01]
9. Apparecchiature con sensori di tipo radar [200-17]
10. Radars [217-05]

Settori Guida di riferimento: 1,3,4,6,7

TA3.2 Sviluppo dei sistemi di monitoraggio diretto (sensori,…) / indiretto (comandi primari/ secondari del veicolo) e monitoraggio in remoto dei parametri dello stato del guidatore

Lo sviluppo di nuove tecnologie ed algoritmi per l'elaborazione numerica dei segnali provenienti da sensori permette di ipotizzare applicazioni innovative anche nel settore automobilistico e del trasporto pubblico. Vari studi concordano che un considerevole numero di incidenti su strada (specie quelli che coinvolgono mezzi commerciali pesanti) è imputabile ad alterate condizioni psico-fisiche del guidatore causate, ad esempio, da assunzione di. alcool, stupefacenti o sostanze farmacologiche, in modo volontario o meno. È quindi opportuno implementare in maniera sempre più puntuale sistemi per la valutazione delle condizioni del guidatore, sia prima della partenza del veicolo che periodicamente durante la guida, allo scopo di registrare eventuali cali di attenzione e/o di abilità di guida e provvedere, all'occorrenza, eventualmente da postazione remota, ad eventuali correzioni di guida. L'esigenza di intervenire diventa indispensabile in presenza di particolari rischi per la sicurezza e l'incolumità dei cittadini derivanti, ad esempio, dal trasporto di sostanze tossiche, inquinanti, infiammabili che possono essere considerati strumenti potenzialmente vulnerabili ad atti di terrorismo o di criminalità. Il possibile verificarsi su mezzi pubblici e privati di atti violenti di matrice terroristica porta inoltre ad ipotizzare l'eventualità di una coercizione effettuata sul conducente tale da alterare i livelli di volontà e/o la capacità di condurre il mezzo appropriatamente. Lo stesso mezzo di trasporto necessita di un controllo periodico idoneo, sia sulle sue parti componenti che sulle caratteristiche di moto (traiettoria, velocità, accelerazione e/o stabilità). Un' alterazione significativa dei vari parametri rispetto a una condizione "standard" potrebbe infatti essere potenzialmente riconducibile non solo ad una guida non appropriata ma anche a malfunzionamenti o avarie del veicolo. Gli obiettivi della ricerca indirizzati da 3.2 sono quindi:

- Detection di stati anomali del conducente (affaticamento, reattività limitata od alterata, perdita di conoscenza del guidatore,…) attraverso la valutazione di parametri biologici;
- Sviluppo di sistemi attivi associati a quelli di detection orientati alla generazione di segnali di allerta per avvisare il conducente di anomalie di guida e/o provvedere ad un rapido intervento sui comandi primari del mezzo di trasporto (con possibilità di comunicare le anomalie ad un centro remoto);
- Detection di anomalie dell'ambiente esterno al mezzo;
- Sviluppo di sistemi attivi orientati alla generazione di segnali allerta per avvisare il conducente di anomalie sul percorso e consentire un rapido intervento sui comandi primari del mezzo di trasporto (con possibilità di comunicare le anomalie ad un centro remoto);
- Detection avanzata di avarie del veicolo;
- Sistemi di integrazione e convergenza dei diversi sistemi di detection per incrementare l'accuratezza nell' identificazione della reale causa-effetto dell'anomalia riscontrata, ridurre i falsi allarmi e individuare appropriate azioni correttive automatiche.

Technology relevance

1. Tecnologia basata su sensori acustici [110-14]
2. Tecnologie basate sull'elaborazione di segnali analogici [112-01]
3. Tecnologie basate sull'elaborazione numerica di segnali [112-02]
4. Tecnologie per la fusione di dati e informazioni [113-04]
5. Pattern *recognition* [113-02]
6. Apparecchi per la ripresa di immagini [200-02]
7. Riconoscimento biometrico del volto [203-01]
8. Informazioni sull'ambiente/luogo [205-13]
9. Radars [217-05]
10. Equipaggiamenti relazionati alle tecnologie biometriche [219-04]

Settori Guida di riferimento:

1,3,4,5,7

TA3.3 Individuazione di eventi anomali basata sull'analisi integrata di misure ambientali, comportamentali e fisiologiche, incluse le biometriche

I recenti approcci per il monitoraggio di aree ed ambienti "sensibili" si basano sempre più sulla integrazione di informazioni provenienti da sensori di tipo eterogeneo, che acquisiscono dati di natura diversa e complementari fra loro come immagini nello spettro del visibile e dell'infrarosso, segnali a radiofrequenza, informazioni audio o anche tracce di componenti chimici/biologici. L'analisi dei dati raccolti punta spesso all'individuazione di situazioni o eventi classificabili come "anomali" e la tecnologia "pivot" attorno alla quale ruota questa nuova visione del controllo del territorio è la videosorveglianza, strumento fortemente strategico in molteplici contesti. Più che di videosorveglianza oggi si parla di "video-analisi" con tipiche applicazioni nel controllo capillare di zone altamente sensibili quali ad esempio scali aeroportuali, stazioni e luoghi caratterizzati da un elevato flusso di persone. Le tecniche di video-analisi sono spesso usate per la rilevazione di situazioni di "anomalia" che potrebbero essere un indizio del possibile verificarsi eventi pericolosi per la collettività. Una delle maggiori difficoltà di questo tipo di approccio è rappresentato dalla corretta determinazione di "anomalia" e cioè del livello di deviazione rispetto ad una situazione standard tale da innescare un' allerta e porre in essere azioni di risposta. Se da una parte sono da considerare pressoché consolidate le tecnologie in grado di rilevare macro-anomalie (ad esempio la presenza di oggetti incustoditi in luoghi sensibili come aeroporti o stazioni o movimenti improvvisi di un agglomerato di persone), la determinazione dello scostamento dei parametri di normalità appare senz'altro più complessa nel caso di indizi meno evidenti ovvero di "micro-anomalie". Il concetto di anomalia può essere esteso anche a livello del singolo individuo e sempre più spesso un comportamento "anomalo" rilevato attraverso un'osservazione diretta o un'elaborazione dei dati, può essere estremamente importante ai fini della possibile rilevazione di una minaccia alla sicurezza collettiva. Così come in vari aeroporti si va diffondendo la figura del "Behavioral Officer", addetto alla sicurezza, particolarmente specializzato nella valutazione delle anomalie comportamentali dei passeggeri, così è prevedibile un sensibile aumento delle capabilities di sistemi automatici di rilevazione. Verranno proposte soluzioni basate sull'integrazione di dati provenienti da sensori complementari fra loro in grado di rilevare e localizzare eventi connessi ad urla, spari, vetrine infrante, incidenti automobilistici. La classe dei sensori potrà comprendere anche dispositivi di acquisizione in grado di evidenziare la presenza di individui che hanno recentemente utilizzato armi da fuoco. Gli obiettivi di ricerca di TA 3.3 sono quindi:

- Sviluppo di tecniche avanzate di video-analisi per l'individuazione di comportamenti consueti e quindi classificabili come "normali";
- Individuazione di eventi anomali anche in situazioni complesse;
- Sviluppo di tecniche analitiche "multi-media"
- Estrazione di informazioni di tipo "soft-biometrics" (fisiche, comportamentali e accessorie);
- Soluzioni di tracciamento in sistemi multi sensore basate sull'estrazione di features biometriche;
- Valutazione degli aspetti sociali e legali che caratterizzano le applicazioni di video-analisi e biometria.

Technology relevance

1. Tecnologia basate sull'elaborazione numerica di segnali [112-02]
2. Tecnologia per l'elaborazione di immagini e pattern [113-01]
3. Pattern recognition [113-02]
4. Detection di intenzioni [117-07]
5. Tecnologie per la detection di intrusioni [117-08]
6. Protocolli di comunicazione messi in sicurezza [117-18][
7. Apparecchi per la ripresa di immagini [200-02]
8. Riconoscimento biometrico del volto [203-01]
9. Riconoscimento biometrico dell'iride [203-04]
10. Informazioni sull'ambiente/luogo [205-13]

Settori Guida di riferimento: 1, 3, 5, 6, 7

TA3.4 Check-point biometrico del futuro con auto accreditamento passeggeri

La velocità e l'accuratezza dei controlli diventeranno due parametri sempre più importanti nel contesto globale della mobilità e del trasporti. In particolare, in Europa, dove il termine "mobilità" si coniuga al concetto di integrazione ed è un fattore critico dell'economia e della vita quotidiana dei cittadini, si assiste ad una forte convergenza fra la necessità di assicurare la sicurezza dei passeggeri attraverso verifiche di identità sempre più certe ed efficaci e il mantenimento di adeguati standard di comfort nell'espletamento delle varie procedure. I nuovi sistemi per l'attraversamento automatico di frontiera (ABC- *Automated Border Crossing*) in sperimentazione o in esercizio in molti scali aeroportuali stanno dimostrando la loro validità ed anticipano comunque una tendenza che coinvolgerà sempre più anche i confini marittimi e terrestri. I sistemi EES (*Entry/Exit Systems*) e RTP (*Registered Traveller Programmes*) sono la prova che le esigenze del controllo di frontiera stanno rapidamente evolvendo e stanno trovando una particolare applicabilità nel comparto aeroportuale. Tale scenario infatti, sia per il considerevole numero degli attraversamenti di frontiera che per le esigenze di rapidità delle transazioni, rappresenta probabilmente il contesto più interessante per i sistemi EES e RTP. I requisiti fondamentali di tali sistemi oggetto della ricerca nel contesto di TA 3.4 sono:

- Rispetto della privacy degli utenti durante la fase di *enrollment*, di verifica, di gestione dei dati della persona e di possibili successive verifiche di identità anche non specificatamente legate al controllo di frontiera. Tale concetto si esplicita nella possibilità di verificare l'identità degli utenti senza rilevare dati e informazioni relativi alla persona non strettamente indispensabili alla particolare procedura;
- Forte attenzione verso l'interoperabilità fra le diverse soluzioni adottate in ambito UE ai fini di una possibile futura integrazione;
- Possibilità di supportare diversi tipi di supporti e/o documenti elettronici, creando una convergenza anche rispetto ai futuri standard che caratterizzeranno i nuovi passaporti elettronici;
- Resistenza agli attacchi;
- Esplorazione di tecniche basate su più biometrie applicate in modo iterativo;
- Apertura verso possibili implementazioni orientate alla riconciliazione dei bagagli.

Le attività di ricerca dovranno mirare allo studio di sistemi in grado di:

- Aumentare l'affidabilità, la velocità e ridurre al minimo l'obsolescenza dei sistemi;
- Eliminare la necessità di particolare collaborazione da parte dell'utente finale nella verifica di identità;
- Permettere una ciclica verifica delle prestazioni in funzione delle alle variazioni delle caratteristiche biometriche del soggetto e proporre soluzioni migliorative;
- Rendere più veloci e sistematiche le verifiche dei rinnovi dei documenti di viaggio elettronici, la loro sospensione di validità etc..

Technology relevance:

1. Tecnologie nello spettro di frequenza dei Terahertz [110-08]
2. Tecnologie nello spettro delle microonde e delle onde millimetriche [110-11]
3. Tecnologia basata sull'elaborazione numerica di segnali [112-02]
4. Tecnologia per l'elaborazione numerica di immagini e pattern [113-01]
5. Pattern recognition [113-02]
6. Analisi dei dati [113-08]
7. Detection di intenzioni [117-07]
8. Apparecchi per la ripresa di immagini [200-02]
9. Riconoscimento biometrico del volto [203-01]
10. Equipaggiamenti relazionati alle tecnologie biometriche [219-04]

Settori Guida di riferimento: 1,3,5,6,7

TA3.5 Soluzioni che individuano minacce collegate ai conducenti di mezzi di trasporto pubblico

Il controllo della effettiva titolarità alla conduzione di un mezzo per evitarne il furto o un uso da persona non autorizzata o la presenza di una coercizione esercitata su un conducente in caso di sequestro del veicolo da parte di criminali si sta rapidamente estendendo da uno scenario prettamente militare ad un ambito molto più allargato.
E' sufficiente infatti considerare la minaccia per la collettività costituita dal sequestro di un veicolo pubblico, affollato di passeggeri, che si muove in un contesto cittadino, per avvalorare la tesi che vanno studiate contromisure sempre più efficaci per scongiurare o mitigare tali pericoli.
Le tecnologie che si stanno dimostrando decisive per questo tipo di applicazioni sono naturalmente quelle biometriche che, come noto, sono, tra l'altro, in grado di legare saldamente l'abilitazione all'espletamento di una qualsiasi azione da parte di un soggetto alla verifica di un suo attributo fisico o comportamentale.
La caratteristica biometrica potrebbe però essere presentata da un conducente di un mezzo di trasporto che è sotto minaccia e quindi può divenire estremamente importante effettuare anche altri controlli, ad esempio valutare variazioni di postura, movimenti del busto o anche analizzare se le caratteristiche di guida corrispondono a quelle, di riferimento, acquisite precedentemente.
Sulla base di quanto esposto, la ricerca di TA 3.5 dovrà quindi consistere in:

- Messa a punto di sistemi affidabili e di costo contenuto in grado di permettere la guida del mezzo solo a coloro in possesso delle credenziali biometriche permettendo allo stesso tempo un monitoraggio continuo e non solo alla "partenza" del mezzo, che rispetti la privacy. Tali sistemi dovranno essere caratterizzati da una bassissima vulnerabilità
- Studio di soluzioni innovative per contrastare l'identity theft (furto di identità)
- Realizzazione di tecniche robuste di analisi di immagini in tempo reale in grado di valutare particolari posture, espressioni movimenti del busto della persona che guida il mezzo, per evidenziare situazioni che possano essere l'indicatore di una minaccia esercitata su un conducente, minimizzando i falsi allarmi;
- Messa a punto e test di tecniche per il tracciamento dei comportamenti di guida tipici del conducente attraverso sensori associati alla rilevazione di altri parametri riferiti, ad esempio, al motore, ai vari comandi o allo sterzo per evidenziare variazioni significative che possono indicare una maggiore probabilità di una avvenuta sostituzione del conducente o di una guida sotto stress di minaccia.

Technology relevance

1. Tecnologie basate sull'uso di sensori acustici [110-14]
2. Tecnologia basate sull'elaborazione numerica di segnali [112-02]
3. Tecnologia per l'elaborazione numerica di immagini e pattern [113-01]
4. Analisi dei dati [113-08]
5. Tecnologie per la conversione da analogico a digitale [112-03]
6. Detection di intenzioni [117-07]
7. Analisi del comportamento [120-06]
8. Apparecchi per la ripresa di immagini [200-02]
9. Riconoscimento biometrico del volto [203-01]
10. Equipaggiamenti relazionati alle tecnologie biometriche [219-04]

Settori Guida di riferimento: 3,4,5

TA3.6 Soluzioni robuste e efficienti per interoperabilità tra sistemi di gestione dell'identità elettronica e dell'autenticazione multi-biometrica nel dominio sia fisico che logico

Le tecniche di riconoscimento biometrico per l'accesso logico e fisico stanno dimostrando le loro potenzialità in maniera sempre più convincente sia in termini di prestazioni che di affidabilità ed accettabilità da parte dell'utenza. Gli accessi si dividono in "logici" e "fisici", ove per "logico" s'intende quello relativo a risorse informatiche o servizi (ad esempio a transazioni in rete), mentre per "fisico" si intende quello a luoghi (ad esempio locali od aree). I due contesti applicativi sono stati considerati congiuntamente solo in alcune soluzioni recenti e le tecnologie biometriche potrebbero essere l'elemento fondamentale per una reale convergenza. In vari casi, infatti, vengono richieste credenziali biometriche sia per l'accesso logico che per quello fisico e uno degli obiettivi che si prefigge di analizzare TA 3.6 è lo studio della loro integrazione. La ricerca analizzerà inoltre vantaggi e criticità derivanti da una puntuale adozione delle tecnologie di tipo PET (Privacy Enhancing Technologies) che si stanno affermando in vari contesti pubblici e privati come robusto supporto alla tutela della privacy. L'uso delle tecniche biometriche può comunque implicare difficoltà legate alla complessità od anche impossibilità da parte di un utente, a causa di handicap congeniti o acquisiti, di esibire una caratteristica biometrica consona alla autenticazione. Uno strumento proposto per ovviare a tale punto di criticità può consistere nell'adozione di procedure di autenticazione basate sulla valutazione di più caratteristiche biometriche: tali sistemi vengono definiti come "multibiometrici" in funzionamento multimodale. Dal punto di vista tassonomico, oltre ai sistemi "moltimodali" si annoverano altri sistemi multibiometrici il cui scopo può essere orientato ad un incremento del livello di sicurezza o ad un miglioramento complessivo delle prestazioni, soprattutto per applicazioni su larga scala e in assenza di supervisore. Un ulteriore obiettivo della ricerca sarà quindi lo studio delle applicazioni multibiometriche sia dal punto di vista dell'accessibilità e usabilità, sia in termini di incremento delle prestazioni anche nell'ottica del rapporto costi/benefici e della possibilità di garantire, se necessario, l'anonimato. Le aree di ricerca di TA 3.6 sono quindi:

- Tecniche di Identity Management;
- Convergenza fra sistemi per il controllo dell'accesso fisico e logico;
- Integrazione di tecnologie biometriche con sensoristica di tipo RFID ed
- Integrazione fra basi di dati biometrici;
- Valutazione delle prestazioni di sistemi multibiometrici con particolare riferimento alla vulnerabilità;
- Tecnologie PET;
- Algoritmi per la "*liveness detection*";

L'interoperabilità fra sistemi di accesso fisico e logico potrà essere ottenuta attraverso:

- Convergenza fra sistemi di Identity Management, sistemi per l'accesso fisico e sistemi per l'accesso logico, includendo, laddove necessario, tecnologie RFID per la localizzazione;
- Interoperabilità fra archivi biometrici, Middleware, DB e DataWarehouses;
- Soluzioni innovative per la correlazioni, integrazione e ed interoperabilità fra tecniche di Datamining, documenti di identità elettronici, dispositivi e sistemi per le verifiche biometriche e PKIs

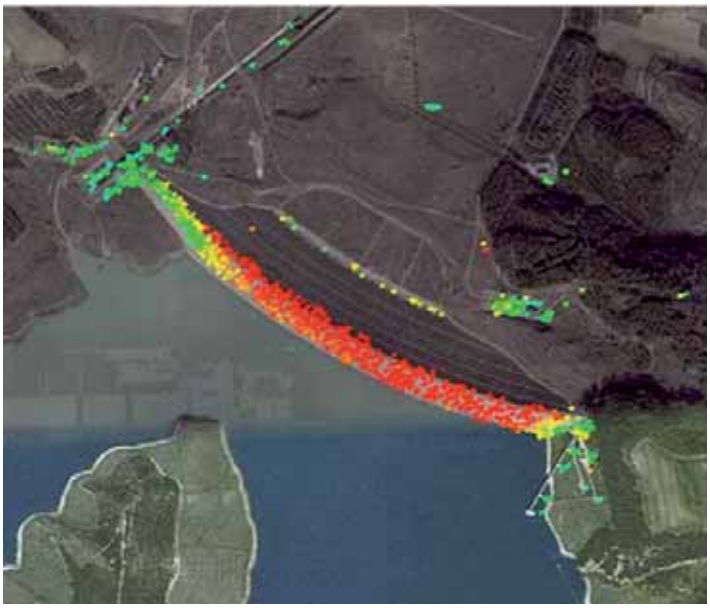
Technology relevance

1. Image / pattern processing technology [113-01]
2. Tecnologia basata sull'elaborazione numerica di segnali [112-02]
3. Raccolta, classificazione dei dati [113-03]
4. Tecnologie per la fusione di dati ed informazioni [113-04]
5. Detection di intenzioni [117-07]
6. Tecnologie di autenticazione IT [117-12]
7. Protocolli di comunicazione messi in sicurezza [117-18]
8. Riconoscimento biometrico del volto [203-01]
9. Apparecchi per la ripresa di immagini [200-02]
10. Equipaggiamenti relazionati alle tecnologie biometriche [219-04]

Settori Guida di riferimento: 5

Area Tecnologica 4: Tecnologie per Crisis Management & per la Protezione di Persone, Asset e Infrastrutture.

Gestire una crisi significa organizzare una tempestiva risposta efficiente ed efficace ad un evento di notevoli proporzioni, al fine di mitigare gli effetti negativi che possono danneggiare persone e cose.



È necessario dunque:

- Garantire l'interoperabilità tra i diversi sistemi cooperanti adottati per fronteggiare l'avvenimento;
- Implementare Centri di Comando e Controllo per la Gestione Operativa;
- Condividere informazioni tra gli enti cooperanti;
- Garantire l'accesso a dati e informazioni condivise in maniera sicura;
- Adattare e riconfigurare ,se necessario, i processi operativi al fine di ottimizzare la risposta alla crisi;
- Provvedere all'addestramento e all'equipaggiamento degli operatori e dei First Responders;

La tematica è principalmente rivolta a potenziare la capacità di intervento degli operatori durante una crisi, proteggendone al tempo stesso l'incolumità.
Le tecnologie del Crisis Management includono:

- Applicazioni robotiche per crisis management e operazioni search&rescue;
- Attuatori in risposta all'emergenza (e.g. veicoli equipaggiati) ;
- Tools & Equipaggiamento per specifiche funzionalità di S&R;
- Simulation & Training per gli operatori di Crisis Management;

Per **Protezione di Persone, Asset e Infrastrutture** si intende la capacità di mettere in sicurezza persone, strutture fisiche e diversi asset al fine di ridurne la vulnerabilità intrinseca e aumentarne la resilienza.

- Le tecnologie per la protezione includono:
  - Monitoraggio costante (raccolta e processing di dati e informazioni di vario genere):
    - Controllo accessi;
    - Gestione Allarmi locali;
    - Fusione/ elaborazione dati e informazioni di diverso genere (afferenti anche alle aree Sorveglianza, Detection & Identification)
  - Analisi *early warning (Forecasting* e analisi di dati precursori)
  - Sviluppo piani di sicurezza (per garantire un'efficace azione di *preparedness e prevention*);
  - Protezione tramite barriere fisica (*fences* attive e passive per il controllo degli accessi nelle aree protette).

La protezione di Persone, Asset e Infrastrutture è fortemente connessa all'azione di *Preparedness*, intesa come azione volta a mitigare gli effetti di possibili rischi. L'azione di *Preparedness* include le seguenti tecnologie:

- Analisi del rischio, studio della vulnerabilità e delle interdipendenze, mappe di vulnerabilità territoriali;
- Design for security;
- Applicazioni dedicate al Monitoraggio della rete fisica e degli edifici (rif. a sensori per sorveglianza)
- Strumenti e modelli di diagnostica;
- Modelling e Simulation dei possibili scenari e delle possibili soluzioni, inclusa la simulazione "multi-layer".

TA4.1 Sistemi innovativi di anti-intrusione

Negli ultimi anni il fenomeno legato a furti, intrusioni ed atti terroristici è divenuto progressivamente più grave a causa dell'aumento della frequenza del livello delle tecnologie impiegate. Per questo motivo, sta assumendo sempre maggiore importanza la necessità di evitare, e possibilmente prevenire, questi fenomeni e dissuadere gli artefici dal compierli al fine di salvaguardare l'incolumità delle persone e difendere beni materiali ed infrastrutture. La difesa dai furti è comunemente affidata a sistemi di controllo, dissuasione ed allarme che prevedono l'impiego di diverse tecniche che vanno dall'installazione di sistemi di controllo accessi all'uso di RFID. Ad oggi l'analisi dei sistemi di protezione ha sempre avuto come riferimento di partenza gli svariati tipi di obiettivi da difendere e ha messo a disposizione tecniche ed installazioni differenti proprio in dipendenza dalla natura di questi, e poca rilevanza è stata attribuita all'uniformità tecnologica. Un esempio di sistema innovativo è la tecnologia audio basata sulla post-elaborazione dei segnali audio di pressione acustica e velocità di vibrazione aerea ripresi in tempo reale con sonde intensimetriche 3D. In base a questa tecnologia ogni suono in un ambiente comunque complesso e riverberante viene rappresentato da 4 segnali risultanti dalle convoluzioni del segnale di sorgente con le 4 risposte all'impulso di pressione-velocità. Misurando queste ultime e sintetizzandole in grafici polari di intensità impulsiva si ottengono mappature delle riflessioni acustiche provenienti da ogni area da monitorare per ragioni di sicurezza. Tali mappature costituiscono il *template* per il riconoscimento di suoni o rumori sospetti provenienti dalle singole aree poste sotto sorveglianza.

L'obiettivo è individuare sistemi antifurto innovativi che possano essere applicati sia negli asset fisici fissi (Palazzi, uffici, locali tecnici, ecc) che negli asset fisici mobili (come mezzi di trasporto) o, in alternativa, metodi di integrazione tra tecnologie dedicate alle due differenti applicazioni. Gli atti terroristici sono notevolmente più difficili da prevedere, i potenziali obiettivi sono estremamente vari e differenti tra loro e mettono a repentaglio l'incolumità delle persone pressoché in qualsiasi luogo. E' tuttavia possibile e necessario studiare un sistema, completato da un assieme di procedure, atto a prevedere con il maggior anticipo possibile le situazioni potenzialmente pericolose e ad individuare nel minor intervallo di tempo attività criminali già in corso per evitare perdite umane e danni materiali.

Technology relevance:

1. Sistemi Controllo accessi [103-2; 219]
2. Sistemi Antintrusione [108-3; 110-19; 300A; 306B-1]
3. Sistemi di Videosorveglianza [118-4; 200-2; 307-A; 306B-1; 408]
4. Sistemi Biometrici [203-4; 203-6;407-1]
5. Sistemi a raggi X [110-2; 110-3; 200-13]
6. Sonde intensimetriche 3-D basate su tecnologia MEMS (anemometria a doppio filo caldo) [110-14; 110-20]
7. Sistema per calibrazione di precisione dei sensori pressione-velocità [304B-13]
8. Apparato di misura in-situ di risposte all'impulso quadrifonico [200-9; 300B-6]
9. Sistema di registrazione digitale del segnale quadrifonico [303B-20]
10. Software di analisi degli eventi sonori con discriminazione dell'allarme [116-1; 305B]

Settori Guida di riferimento: 1

TA4.2 Analisi della deformazione e dei danni dell'infrastruttura in seguito ad atti terroristici o eventi naturali e loro riabilitazione

Le infrastrutture, necessarie al funzionamento della società e dell'economia, sono vulnerabili sia nei confronti di minacce antropiche, che a seguito di eventi naturali. Partendo dalla Direttiva EU relativa all' "individuazione e alla designazione delle infrastrutture critiche europee e alla valutazione della necessità di migliorarne la protezione" 114/08/CE, la domanda di protezione delle infrastrutture critiche è aumentata e con essa è cresciuta l'esigenza di monitoraggio con tecnologie innovative.

Il monitoraggio di un'infrastruttura richiede l'utilizzo e, quasi sempre, l'integrazione di tecnologie di osservazione e misurazione innovative con caratteristiche complementari. Lo sviluppo dei nuovi sensori evidenzia la necessità di realizzare un sistema cooperativo di protezione delle infrastrutture in situazioni di emergenza finalizzato all'analisi dello stato dell'infrastruttura in presenza di eventi critici, sia a seguito di atti vandalici, sia per effetto di eventi naturali (persistenti o improvvisi) e che sia di supporto anche al corretto recupero.

Un sistema in grado di operare in condizioni di emergenza deve prevedere da un lato la gestione e il trattamento di informazioni multi-sorgente ai fini interpretativi, di analisi di precursori, di *quick assessment* dei danni, di gestione operativa e di *first response*, e dall'altro la possibilità di operare con una rosa di strumenti osservativi e misurativi che utilizzano sensori e tecnologie indipendenti di misura, non invasive, complementari in termini di parametri misurati e frequenza e scala di misurazione. In tal senso la possibilità di analizzare a livello di dettaglio le deformazioni costituisce un elemento di fondamentale importanza per l'analisi della stabilità delle infrastrutture, delle cause che conducono a situazioni di crisi e per la loro eventuale corretta riabilitazione.

Le tecnologie di *sensing* devono consentire la generazione di prodotti anche in near real time ed inoltre operare a distanze diverse per consentirne l'utilizzo in differenti scenari:

- *remote sensing* in cui si prevede l'impiego di sensori aviotrasportati e satellitari che consentono di analizzare l'infrastruttura ed il contesto nella quale essa insiste a differenti scale di analisi.
- *near sensing* con sensori osservativi *short range* con differente accessibilità per la misurazione di precisione ad elevata risoluzione.
- *proximity and integrated sensing* con sistemi di monitoraggio strutturale non distruttivo capaci di misurare le deformazioni con continuità spaziale e temporale.

Il sistema di gestione dati deve essere in grado di rappresentare le informazioni in modo da consentire analisi ed interpretazioni confrontando misurazioni e dati osservativi di diversa natura. Data la complessità delle infrastrutture e la differente scala, frequenza ed incertezza delle misure derivanti da differenti tecniche di sensing, un aspetto di importanza fondamentale del sistema deve riguardare l'integrazione e la *cross-validazione* dei risultati delle tecnologie.

Technology relevance

1. Sistemi informativi di gestione dati [113-4; 205-12]
2. Sistemi di supporto alle decisioni [114-4]
3. Sensori Radar ad Apertura Sintetica ad alta risoluzione e frequenza di rivisita ad esempio equipaggiati a bordi di costellazioni di satellitari (es COSMO-SKYMED e TERRASAR-X/TANDEM-X) [112-2; 200-18; 217-5; 401-3]
4. Sensori radar aviotrasportati consente un monitoraggio *on-demand* con frequenze anche di diverse acquisizioni al giorno [110-20; 217-5; 200-17]
5. Sistemi *Ground Based Synthetic Aperture Radar, sensori multispettrali ed iperspettrali,* Laser Scanner per misure ad alta risoluzione [200-18;110-10; 110-13; 110-12]
6. Sensori distribuiti in fibra ottica per il monitoraggio ad alta risoluzione e/o su long-range di deformazioni e vibrazioni [118-7]

Settori Guida di riferimento: 9,10

TA4.3 Sviluppo di componenti, tecniche e metodologie per lo studio e l'analisi dei rischi sugli edifici e sugli impianti (mappe di vulnerabilità delle aree fruibili, controllo di valori soglia, etc)

Lo sviluppo di componenti, metodologie e tecniche per l'analisi dei rischi di edifici ed impianti rappresenta un'esigenza dal significativo impatto sociale ed economico. Essa, infatti, non solo interessa diverse tipologie del costruito (tra cui infrastrutture di interesse pubblico, edifici storici, strutture civili, aree archeologiche.) ma assume un carattere ambivalente di interesse sia per la *Safety* (rischio legato ad eventi naturali e a difetti nei manufatti umani), che per la *Security* (eventi causati da comportamenti non leciti quali ad esempio quelli terroristici). Con riferimento agli edifici, la sicurezza va assicurata attraverso verifiche e controlli degli elementi strutturali per il mantenimento in efficienza, la prevenzione contro i rischi naturali (sismi, frane..) e antropici, la costruzione di modelli dinamici delle strutture, la gestione delle situazioni di crisi, conseguenza di attacchi terroristici e disastri naturali. Una risposta a queste necessità consiste nello sviluppo di sistemi per un monitoraggio che sia continuo nel tempo, multi-sensoriale, multi-scalare (visione globale della struttura e del territorio e diagnostica di dettaglio), multi-risoluzione, multi-profondità con carattere di bassa o nulla invasività. La messa a punto di un tale sistema richiede, da un lato, architetture avanzate basate su reti wireless e di sensori, e dall'altro, l'integrazione di tecniche di diagnostica non invasiva basata principalmente su *sensing* elettromagnetico e/o acustico.

In particolare, tale sistema di monitoraggio, oltre a "sorvegliare e monitorare" la struttura, deve mirare anche al monitoraggio del territorio circostante, con particolare attenzione alle deformazioni ed al comportamento dinamico del suolo (movimenti franosi, movimenti tellurici, etc).

Questi dati risultano decisivi ai fini dell'identificazione di modelli del comportamento delle strutture in relazione all'esposizione ai diversi tipi di rischio.

Inoltre, la diagnostica di dettaglio della struttura (ad alta risoluzione) risulta importante anche per la verifica della bontà e dell'efficacia delle operazioni di *reinforcement* e pone sfide interessanti, in termini di attività di ricerca, legate alla necessità di monitorare nuovi materiali utilizzati durante le operazioni di consolidamento.

Insieme al controllo e verifica degli elementi strutturali di un edificio, riveste analoga importanza il monitoraggio e la protezione degli impianti, al fine di evitarne danni e malfunzionamenti, anche conseguenti ad attacchi terroristici, e la possibilità di fornire un supporto alla gestione delle situazioni di crisi con particolare riferimento alle procedure di evacuazione nelle fasi immediatamente successive all'evento. In tale ambito, attività di sicuro interesse riguardano la classificazione dei rischi in relazione alle tipologie d'impianto e la definizione di contromisure attive e passive per riduzione effetti da scoppio su edifici/ impianti.

Technology relevance

1. Tecniche di monitoraggio via satellite (SAR a microonde, ottico) [110-10; 112-2; 110-20; 200-18; 200-17; 217-5; 401-3]
2. Tecniche di fusione ed integrazione dati multisorgente (e.g. dati SAR, foto aeree, immagini ottiche da satellite, carte topografiche di base, carte inventario aree in frana) [112-2]
3. Tecniche di posizionamento GNSS ad elevata accuratezza (controllo degli spostamenti delle infrastrutture e delle deformazioni del territorio) [306A-2]
4. Sensoristica in fibra ottica distribuita (scattering di Brillouin, reticoli di Bragg, reticoli a passo ,lungo), rilevamenti laser e sensori piezoelettrici e/o optoelettronici distribuiti [118-7]
5. Tecniche in situ per la diagnostica dell'interno della struttura e del sottosuolo (*Ground Penetrating Radar, Electrical resistivity Tomography*, spettroscopia iperspettrale, analisi termografiche ad infrarossi, sonic e ultrasonic sensors,…). Tecniche *Ground Based* SAR e laser per il controllo dei micro-movimenti della struttura [200-18]
6. Analisi e modellizzazione dei rischi sugli edifici e sugli impianti e classificazione dei rischi in relazione alle tipologie d'impianto. Sensori di pre-allarme, allarme e rilevamento [308A-1]
7. Componenti e tecniche per la protezione o assorbimento degli scoppi e contromisure attive e passive per la riduzione degli effetti da scoppio su edifici/ impianti [101-4]
8. Sistemi integrati di reti wireless e di sensori e reti di comunicazione tra sensori con capacità auto-organizzanti [413-5; 413-6]

Settori Guida di riferimento: 9

TA4.4 Sistemi robotici cooperativi (manned e unmanned) per la valutazione remota e preventiva dell'area interessata dall'evento e l'erogazione delle prime azioni di intervento (Robotic Rescue).

L'azione degli Operatori di Primo Soccorso (First Responders, FR) nella gestione di eventi critici (di origine sia naturale che umana) è condizionata da un insieme di fattori che possono essere causa di notevoli rischi per gli operatori stessi, riducendo nel contempo l'efficacia della loro azione.

Sebbene le condizioni operative siano in genere differenti per i diversi FR (Vigili del fuoco, Protezione Civile, Polizia), è possibile individuare un insieme di fattori critici comuni, come l'estrema imprevedibilità dell'evoluzione degli scenari di crisi e la sostanziale riduzione della percezione sensoriale. Si possono citare ad esempio le modifiche strutturali (crolli negli edifici), le contaminazioni chimiche/biologiche/radioattive, le elevate temperature, le perdite di gas tossici/esplosivi, la riduzione della percezione sensoriale dovuta a fumo/polvere/vapori/gas, il deterioramento delle comunicazioni.

In situazioni del genere una o più piattaforme robotiche, dotate della capacità di operare, in ambienti ostili, al posto di – o in collaborazione con – una squadra di FR, potrebbero ridurre sostanzialmente gli incidenti – anche mortali – fra gli operatori, aumentandone contemporaneamente le capacità e l'efficacia. Piattaforme di questo tipo, tuttavia, non sono attualmente impiegate dalle squadre di soccorritori, a causa di fattori quali la limitata mobilità in ambienti critici (macerie, scalini), il basso livello del controllo del robot (mancanza dell'autonomia necessaria ad affrontare situazioni impreviste e perdite di comunicazione), la bassa facilità d'uso (gestione troppo impegnativa per gli operatori). Tutti i temi citati meriterebbero un esteso lavoro di ricerca ivi inclusi gli aspetti di simulazione e predizione di eventi a tempistica modellabile Una delle soluzioni tecnologiche recentemente più studiate da ricercatori e esperti dell'industria è rappresentata dall'impiego di sciami di robot cooperanti. Tale soluzione prevede spesso l'impiego di più unita *unmanned* dello stesso tipo (principalmente terrestri o aeree), che agiscono seguendo uno schema operativo predefinito. Una possibile soluzione tecnologica innovativa rispetto a questo quadro di riferimento (soprattutto in termini di maggiore flessibilità ed adattabilità ai diversi scenari operativi e alla continua evoluzione dei target della missione) consiste nell'integrazione di una piattaforma *manned* con una o più *unmanned*. Potrà essere considerato, ad esempio, l'impiego di un veicolo equipaggiato con una rete di sensori eterogenei (video/radio/audio/IR) in grado di identificare e comprendere gli scenari da fronteggiare e di attivare uno o più UAVs in grado di decollare e/o atterrare sul tetto del veicolo stesso. L'obiettivo di un sistema di questo tipo è fornire una maggiore capacità di adattamento e di configurabilità rispetto ai continui cambiamenti strategici che caratterizzano le operazioni di *crisis management*, attraverso la valutazione congiunta dei dati provenienti da una piattaforma *unmanned* dotata di maggiore capacità esplorativa ad ampio raggio e di una *manned* dotata di maggiore capacità esplorativa a breve raggio. Il fine ultimo è l'erogazione delle prime azioni di intervento in modo efficace e tempestivo.

Technology relevance

1. Meccanica della piattaforma (riduzione di peso e dimensioni) [216-12; 402-5; 402-9];
2. Mobilità (su tutti I tipi di terreno, incluse macerie, scale, etc.) [205-4; 402-5; 402-9];
3. Comunicazioni (ambienti sotterranei, aree schermate, capacità autonoma di recupero comunicazione) [413-1;413-2; 413-4; 413-6; 416-*];
4. Sensori (fusione dati; miniaturizzazione; condivisione fra il robot e l'equipaggiamento indossato dai FR) [200-* ; 205-9; 216-3];
5. Comprensione della situazione [301°; 411-2; 411-3; 411-5] ;
6. Localizzazione, Navigazione (auto localizzazione, costruzione di mappe, navigazione in ambienti non strutturati, funzioni autonome come l'inseguimento del FR e il ritorno automatico in caso di perdita di comunicazione) [205-1; 205-2; 205-11; 205-12];
7. Interattività (HRI – Interfaccia uomo robot – progettata per ridurre l'impegno mentale del FR, inseguimento/anticipazione dell'azione umana) [205-6; 205-8; 216-1; 303B-14; 414-1; 414-4];
8. Coordinamento e Sciami (cooperazione di diversi robot, sia dello stesso tipo che di tipi differenti) [402-9];
9. Simulazione e predizione in scenari a tempistica monitorabile [115-1; 115-2; 416-1; 504B-2; 504B-3];
10. Tecniche di visione artificiale a bordo di robot [411-3];

Settori Guida di riferimento: 10

TA4.5 Sistemi di assistenza e/o cooperativi per i veicoli di soccorso e di intervento, finalizzati a garantire il tempestivo raggiungimento delle aree di crisi

L'efficacia delle operazioni di soccorso e di mitigazione delle conseguenze di un attacco o di un evento dovuto a calamità naturale è spesso strettamente correlata alla tempestività dell'intervento stesso. Il raggiungimento delle aeree di crisi può essere condizionato da molteplici fattori, ambientali o derivanti anche da effetti a catena scatenati dalla medesima situazione di emergenza, che possono rappresentare un significativo ostacolo per i mezzi di soccorso (come: visibilità compromessa da agenti atmosferici, da scarsa luminosità, da fumi o da vapori e gas, condizioni di viabilità bloccata per il crollo di edifici o di strade e ponti,… etc.).

In tale contesto lo sviluppo di tecnologie a supporto dei mezzi di intervento basati su sistemi di assistenza e/o cooperativi costituisce una soluzione efficace al problema, oltre a garantire la sicurezza degli stessi soccorritori.

Sistemi di gestione satellitare avanzata delle flotte dei veicoli, o di visione artificiale per aumentare la visibilità in condizioni critiche, o di assistenza alla manovre mediante l'impiego di sensori e tecniche di controllo rappresentano alcuni immediati esempi di soluzioni tecnologiche efficaci ad assicurare la sicurezza ed il pronto intervento (ad esempio. veicoli antincendio, etc).

Altre promettenti soluzioni tecnologiche sono costituite dai sistemi cooperativi, basati sulla comunicazione veicolo-veicolo (V2V) e veicolo-infrastruttura (V2I). Numerose iniziative di ricerca promosse e condotte negli ultimi anni dalla Commissione Europea hanno dimostrato i potenziali benefici dell'utilizzo di sistemi di comunicazione V2x nell'ambito della mobilità. L'estensione sensoriale fornita dalle tecnologie di comunicazione rende infatti possibile "estendere" l'orizzonte spaziale e temporale sotto controllo, reagire più prontamente alle situazioni critiche e a rispondere adeguatamente alle necessità di controllo delle condizioni di viabilità (per esempio, al fine di instradare e facilitare il percorso dei mezzi di soccorso, anche attraverso il controllo remoto dei flussi semaforici e di traffico, o per l'accurata localizzazione e gestione dell'intera flotta dei mezzi di intervento).

Lo sviluppo e la disponibilità di sistemi di assistenza e/o cooperativi per i veicoli di soccorso renderà possibile un aumento della rapidità, dell'efficacia e della sicurezza dell'intervento dei soccorsi nelle situazioni di critiche, con conseguente riduzione della portata e durata dell'emergenza. Allo stesso tempo, la disponibilità sul territorio nazionale di una rete per la cooperazione veicoli-infrastruttura, potrà consentire un sistema nazionale per l'erogazione di servizi di sicurezza stradale ai cittadini in movimento.

Gli sviluppi tecnologici in tale ambito dovranno includere anche gli aspetti di sicurezza delle reti e dei protocolli di comunicazione.

Technology relevance:

1. Piattaforme hardware e software per sistemi cooperativi (rif. standard, e.g. ETSI, e normative Europee in corso di definizione) [116; 413]
2. Reti veicolari di comunicazione e infrastruttura [311A; 413]
3. Protocolli di comunicazione e sicurezza [413; 416-16; 117-18; 118; 311A]
4. Tecnologie sensoristiche e di controllo per sistemi imbarcabili e per l'infrastruttura stradale [110-6; 110-11; 110-20; 113-1; 113-2; 113-3; 113-4; 113-8; 113-13; 114; 200-2; 200-15; 200-16; 200-17; 200-22; 200-25; 200-30; 216-3; 411-3];
5. Accurata localizzazione e navigazione dinamica [205; 307A]
6. Tecniche di ricostruzione dello scenario e di data fusion [301A; 308A; 411-3; 411-5]
7. Soluzioni per l'integrazione a bordo dei veicoli di sistemi di assistenza e/o cooperativi [402]

Settori Guida di riferimento: 4

TA4.6 Piattaforme e sistemi di comando e controllo, mono o multi - operatore, di vario livello (da C2 a C4I), con funzionalità di autoapprendimento, simulazione e training

Un sistema di Comando e Controllo (C2) è in grado di supportare, nell'esecuzione dei propri compiti, tutte le organizzazioni coinvolte, a vari livelli, nella prevenzione e gestione di incidenti e crisi.
Il modo in cui le varie organizzazioni sono strutturate e le procedure previste nei casi di intervento variano a seconda dell'organizzazione e della nazione di appartenenza, con conseguente diversificazione della struttura del sistema di C2, delle responsabilità assegnate ai vari livelli di comando (strategico o di coordinamento, tattico, esecutivo) e della loro dislocazione.
E' prevedibile che, ancora per diversi anni e nonostante numerosi tentativi di armonizzazione e standardizzazione, le diverse organizzazioni mantengano una propria struttura e continuino ad avvalersi degli strumenti di supporto attualmente disponibili (sistemi "*legacy*").
Risulta di conseguenza indispensabile avere la possibilità di rendere interoperabili i sistemi esistenti collegandoli tra di loro attraverso l'impiego di un sistema "ombrello" che possa raccogliere e distribuire tutte le informazioni disponibili (situazione condivisa) e fornire supporto per la collaborazione tra le diverse organizzazioni sia in fase di pianificazione degli interventi che nella fase attuativa (supporto decisionale).
Tale sistema può essere installato presso il comando di più alto livello nella gestione di un'operazione o crisi e collegarsi ai sistemi esistenti per rendere esecutive le decisioni prese congiuntamente dai responsabili delle organizzazioni coinvolte. E' importante che il sistema presenti un'interfaccia uomo-macchina uniforme e coerente per le funzionalità comuni ai diversi tipi di utenti, mentre applicazioni dedicate potranno essere disponibili per specifiche categorie di utenti.
Attraverso una rappresentazione geo-referenziata 2D/3D dell'area di interesse, che integrerà tutte le informazioni disponibili e rilevanti (caratteristiche del territorio, rappresentazione 3D di edifici, immagini da telecamere di Video Sorveglianza, contenuto di DB, documenti, etc), l'utente potrà individuare e selezionare gli elementi di interesse e visualizzare in modo semplice informazioni di sempre maggiore dettaglio, in modo completamente trasparente rispetto alle loro caratteristiche (sorgente, formato, modalità di accesso).
Specifici strumenti software supporteranno l'interpretazione, l'analisi e la gestione delle informazioni e il processo decisionale.

Technology relevance

1. Tecnologie per l'interoperabilità, fusione/conversione di [113-4; 301B-1]
2. Architetture orientate ai servizi [116-4; 213-1]
3. Tecniche avanzate di interfaccia uomo/macchina con filtraggio e controllo delle informazioni in base al ruolo/attività [303B-14; 408B-3; 217-15]
4. GIS e visualizzazione 2D/3D geo-referenziate; tool per generazione/aggiornamento rapido di mappe e modelli 3D [205-12]
5. Simulazione di scenario (evoluzione prevista, *what-if analysis* per supporto decisionale, addestramento) [114-5; 504B-2]
6. Strumenti per la collaborazione e il supporto decisionale in ambiente distribuito [308B-1; 411-6]

Settori Guida di riferimento: 1

TA4.7 Metodologie e strumenti per l'analisi del rischio e l'ottimizzazione costo/benefici basati su simulazione e modellistica analitica

L'analisi dei problemi reali porta alla definizione di modelli matematici per il trattamento di sistemi complessi. Il carattere di "complessità" di un sistema può derivare o dal gran numero delle variabili in gioco, di controllo o di decisione, o dalla presenza di fenomeni fortemente non lineari o aleatori.

Ciò rende necessario l'impiego di sofisticate tecniche per individuare i valori ottimali delle variabili di controllo, di decisione o di progetto; l'attività di ricerca si concentrerà su sistemi complessi in cui si analizzerà il rischio derivante dalla presenza di incertezza sui dati e l'ottimizzazione dei costi e dei benefici.

Si distinguono, inoltre, modelli statici e modelli dinamici.

I modelli statici esprimono un sistema complesso attraverso la soluzione di un problema di ottimizzazione in cui le decisioni ammissibili sono descritte attraverso variabili soggette ad un sistema di vincoli di disequazioni. Le decisioni sono valutate sulla base di una funzione obiettivo che esprime un ordinamento (rispetto alla valutazione del rischio, o del costo/beneficio); si vuole quindi determinare i valori per le variabili che soddisfino i vincoli e che minimizzino (o massimizzino) la funzione obiettivo.

La modellazione del sistema può avvenire tramite vincoli e funzioni obiettivo lineari o non lineari, variabili che assumono valori nel continuo o nel discreto, creando una gerarchia di difficoltà dei modelli e la necessità di differenti tecniche risolutive.

I modelli statici possono esprimere elementi di stocasticità attraverso la definizione di possibili scenari a cui sono associate delle probabilità di occorrenza (programmazione stocastica) con l'obiettivo di ottimizzare il valore medio della funzione obiettivo oppure attraverso la definizione di un insieme di possibili parametri incerti al fine di determinare la soluzione migliore in tutto l'intervallo di variabilità dei parametri (ottimizzazione robusta). L'ottimizzazione robusta porta all'ottimizzazione del caso pessimo come accade per la limitazione delle componenti di rischio.

I modelli dinamici esprimono un sistema complesso attraverso la soluzione di un sistema di equazioni differenziali (sistemi a tempo continuo) o di equazioni alle differenze finite (sistemi a tempo discreto) in cui vanno determinate le variabili di controllo al fine di ottenere desiderate evoluzioni del sistema. I modelli dinamici possono essere deterministici o stocastici. In particolare i modelli stocastici possono essere utilizzati per l'analisi di segnali e per il filtraggio del rumore con applicazioni nell'analisi di serie storiche per l'identificazione di un andamento costante e la determinazione della stima di valori futuri al fine di ridurre la probabilità di rischio.

Technology relevance:

1. Sviluppo di modelli matematici per l'ottimizzazione, la predizione stocastica, il calcolo combinatorio [114-3; 114-4; 114-5; 312A-2; 411-5; 508A-2; 509A-1; 509A-3]
2. Sviluppo di algoritmi di Teoria dei sistemi e del controllo e di Teoria della stima e filtraggio [304B-9; 311A1]
3. Analisi di dati Statistica e analisi di serie storiche [113-3; 113-8; 113-12;114-2]

Settori Guida di riferimento: 1,2,6,10,12

TA4.8 Sistemi di Situation Awareness per gestire localmente situazioni anomale con l'obiettivo di prevenire effetti domino e circoscrivere le conseguenze negative

Dopo l'11 Settembre la necessità di garantire in modo sempre più efficace la sicurezza dei cittadini e delle infrastrutture ha stimolato nuove attività di ricerca e sviluppo rivolte allo studio e alla implementazione di sistemi di sicurezza che fossero in grado di riconoscere e prevenire attacchi/minacce di matrice terroristica.
Tuttavia, un aspetto ancora non sufficientemente esplorato e in cui ulteriori sforzi, da parte degli attori del settore della sicurezza fisica, sono necessari è rappresentato dalla capacità di gestire e reagire di fronte a situazioni anomale, soprattutto verso l'obiettivo di prevenire effetti a cascata e conseguenze negative per l'incolumità delle persone.
Ad esempio, uno scenario di grande interesse può essere rappresentato da un ambiente caratterizzato da flussi continui di persone (e.g. aeroporto, stazione ferroviaria) o da un evento in grado di richiamare una folla di persone (e.g. concerti, visita del Papa, partite di calcio).
La necessità è quella di facilitare e migliorare la comprensione della situazione grazie a prestazioni di scoperta, risoluzione, tracciamento, identificazione sempre più efficaci e tempestive e di dimostrare la possibilità di generare e condividere una *Common Operational Picture* caratterizzata da affidabilità ed usabilità migliorate rispetto a quanto garantito dai sistemi attualmente in uso.
In questo quadro di riferimento, gli obiettivi sopra citati potranno essere raggiunti grazie all'impiego di reti di sensori intelligenti accoppiate allo sviluppo di algoritmi di Situation Awareness (SA) per la comprensione automatica, adattiva e dinamica dello scenario.
Gli strumenti su cui concentrare la ricerca nel campo della SA sono rappresentati dal punto di vista algortimico da tecniche di *Machine Learning* e dai modelli cognitivi e ad agenti (e.g. reti bayesiane).
La fusione dati rappresenta un'altra tecnologia chiave. Facendo riferimento al modello *Joint Directors of Laboratories* (JDL) appare cruciale concentrare l'attenzione sulle fasi di *Situation Refinement, Threat Refinement, Process Refinement* e *Cognitive Refinement.*
Infine, l'implementazione di simulatori di scenari in grado di fornire una elevata quantità di dati di training relativi ai comportamenti che si vuole etichettare sia come normali che come anomali rappresenta una soluzione per incrementare la capacità dei sistemi di rispondere efficacemente in fase di *testing* e di funzionamento on-line I simulatori di scenari debbono permettere la rappresentazione di diverse infrastrutture critiche interdipendenti, nell'ipotesi che siano soggette ad attacchi/minacce di matrice terroristica ma anche ad eventi naturali.

Technology relevance:

1. Sensors and networks of sensors modeling [408-1]
2. Data Fusion [113-4]
3. Learning and reinforced learning methodologies (e.g. *Bayesian Learning*) [114-1: 114-3]
4. Simulazione e *augmented reality tools for interdepency analysis* [114-5]

Settori Guida di riferimento: 2

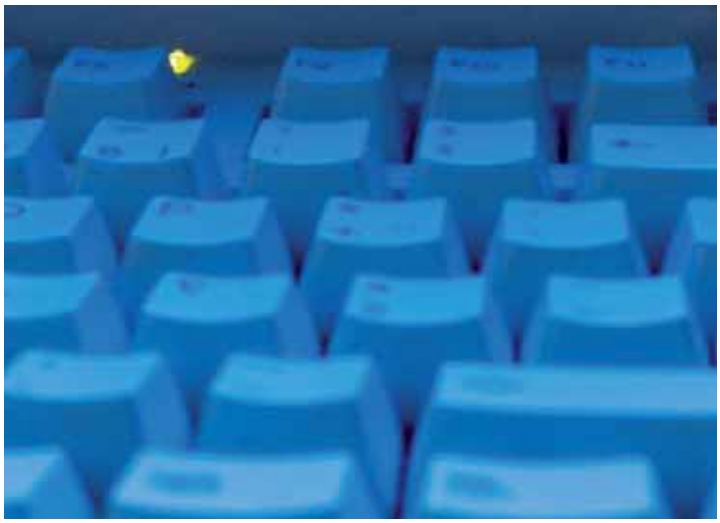
Area Tecnologica 5: Information Processing and Management

Per Information Processing e Management si intende la capacità di elaborare dati e informazioni eterogenee.
La tematica si esplicita in:

- Tecniche per l'elaborazione dei dati eterogenei;
- Tecniche di diffusione sicura dell'informazione;
- Piattaforme interoperabili, per l'accesso, lo scambio e la distribuzione delle informazioni richieste e necessarie;

Le tecnologie afferenti all'Information Processing e Management, a seconda degli scenari applicativi, includono:

- Tecnologie semantiche per la descrizione, classificazione ed identificazione delle informazioni rilevanti;
- Data Mining;
- Data Fusion;
- Engine Semantic Web – Ontologie, Reasoning, Spatial Mining;
- Attività di intelligence sui sistemi ICT;
- Tecniche di classificazione e riconoscimento applicate su fonti eterogenee di dati;
- Sicurezza dell'informazione scambiata (tecniche di crittografia);
- Sicurezza dei sistemi informativi, cybersecurity, anti-hackering;
- Strumenti logici per rendere le reti più resilienti anche verso effetti a cascata.



TA5.1 Fusione delle informazioni raccolte da diverse sorgenti al fine di aumentare e migliorare il contenuto informativo

I sistemi per la rilevazione di minacce ed intrusioni possono essere utilizzati per garantire la sicurezza di infrastrutture critiche o siti di interesse sociale o culturale o per controllare aree geografiche di diversa estensione (confini terrestri o marittimi, aree in cui si svolgono particolari eventi). Al fine di potere rilevare e riconoscere tutte le possibili situazioni di pericolo, tali sistemi devono essere in grado di raccogliere ed utilizzare informazioni e segnalazioni di eventi provenienti in modo asincrono da sorgenti e sistemi di monitoraggio operanti in diversi domini e a diversi livelli; tali informazioni, che costituiranno presumibilmente una vastissima collezione di dati eterogenei, devono essere raccolte ed elaborate in tempo reale per valutarne la rilevanza al fine di estrarre e riconoscere le situazioni di interesse. L'eterogeneità dei dati e la diversità delle sorgenti costituiscono fattori chiave per migliorare la capacità dei sistemi di rilevazione di individuare classi sempre più ampi di intrusioni generando il minor numero possibile di falsi allarmi.

L'obiettivo della ricerca è di sviluppare tecniche per la raccolta, l'analisi e la correlazione di informazioni provenienti da sistemi di monitoraggio eterogenei al fine di aumentare il contenuto informativo per l'identificazione di minacce ed intrusioni.

Tale obiettivo potrà essere raggiunto attraverso le seguenti attività:

- Realizzazione di strumenti adattabili per l'analisi in tempo reale di grandi quantità di dati rappresentati in formati eterogenei
- Estensione degli attuali sistemi per la rilevazione di minacce ed intrusioni al fine di renderli capaci di usare informazioni ed eventi provenienti da differenti domini e livelli
- Potenziamento delle capacità di valutazione dei sistemi per la rilevazione di minacce ed intrusioni attraverso l'introduzione di algoritmi e modelli per l'analisi, l'astrazione, il filtraggio e la correlazione di grandi moli di dati con requisiti di flessibilità ed accuratezza
- Miglioramento della affidabilità dei sistemi per la rilevazione di minacce ed intrusioni attraverso l'introduzione di meccanismi per il "*predictive security monitoring*"
- Miglioramento delle prestazioni e della *resilience* dei sistemi per la rilevazione di intrusioni attraverso lo sviluppo di tecniche innovative di "intelligenza computazionale"
- Sviluppo di una SDI (*Spatial Data Infrastructure*) con elevati standard di sicurezza

Technology relevance

1. Stream processing [113-8]
2. Security Information and Event Management (SIEM) [113-3; 117]
3. Complex Event Processing (CEP) [113-8; 116-8]
4. Data fusion [113-4]

Settori Guida di riferimento: 3,6

TA5.2 Sistemi ICT sicuri e resistenti agli attacchi (sicurezza del dato)

La complessità degli attuali sistemi ICT e l'eterogeneità dei componenti hardware e software in essi utilizzati rendono tali sistemi sempre più vulnerabili ad attacchi, capaci di modificare il loro comportamento nel tempo ed essere difficilmente rilevabili dai tradizionali sistemi di sicurezza.
Sorge, quindi, la necessità di progettare e sviluppare nuove tecniche, che, raccogliendo informazioni e dati da sorgenti differenti e combinando approcci diversi, siano in grado di prevenire le minacce e di rilevare le nuove tipologie di attacchi informatici. L'analisi e l'elaborazione delle informazioni raccolte da fonti eterogenee renderanno possibile l'esecuzione di una vera e propria attività diagnostica, che preveda non solo la rilevazione dell'attacco, ma anche l'individuazione dell'origine dell'attacco stesso e del componente o della parte del sistema ICT, che risultano essere maggiormente interessati dagli effetti dell'attacco. Al fine di incrementare le prestazioni e la "copertura", dell'attività diagnostica, in termini di classi di attacchi rilevabili, sono fondamentali lo sviluppo e l'integrazione di metodi innovativi per la rilevazione di anomalie. La attività di diagnosi costituisce una funzione chiave di un sistema di sicurezza, in quanto essa è chiamata a supportare, fornendo gli input necessari, i meccanismi e le azioni di riconfigurazione e reazione, il cui 'obiettivo è quello di rendere il sistema ICT capace di tollerare e sopravvivere ad un attacco. Alla luce di tali considerazioni, l'obiettivo della ricerca è di progettare e sviluppare sia tecniche che consentano di prevenire attacchi informatici che strumenti per rilevarli e mitigarli.
Tale obiettivo può essere raggiunto attraverso l'esecuzione delle seguenti attività:

- progettazione e sviluppo di tecniche per la diagnosi di attacchi informatici in grado di rilevare il tipo di attacco in corso, individuare la parte del sistema interessata dall'attacco ed, infine, valutare l'impatto dell'attacco rilevato sulle funzioni del sistema al fine di prevenire effetti a cascata
- definizione di tecniche per la gestione della rete e del traffico dati in grado di rendere la rete resiliente ad attacchi
- definizione di algoritmi per l'ingegneria del traffico dati in grado di fornire garanzie di qualità del servizio a flussi informativi critici in presenza di attacchi e/o fallimenti
- definizione di meccanismi di *'fingerprinting'* per i sistemi di calcolo critici per una rapida individuazione delle modifiche non autorizzate
- definizione di architetture per la protezione 'ring 0' dei sistemi iCT

Technology relevance

1. Adaptable Parsers [113-12]
2. Intrusion Detection Systems (IDSs) [117-8]
3. Network Monitoring Systems [416-10]

Settori Guida di riferimento: 2,5

TA5.3 Piattaforme, architetture ed algoritmi per l'analisi in tempo reale di grandi volumi di dati (high performance computing)

Il numero crescente di minacce alla sfera sociale, economica e finanziaria nel mondo moderno richiede un enorme utilizzo di tecnologie efficienti, scalabili, e facilmente programmabili per raccogliere, catalogare, processare ed analizzare grandi quantità di dati in tempo reale. Le minacce causate da un gruppo di attaccanti che si coordina per sferrare contemporaneamente un attacco massiccio contro un unico bersaglio (*0-day attack*), richiede la capacità di rilevare in breve tempo situazioni complesse e di trarne le dovute conseguenze (*decision making* in tempo reale).

E' necessario quindi lo studio ed lo sviluppo di nuove metodologie, architetture e strumenti software per la creazione, gestione e l'analisi automatizzata di basi/flussi di dati massive ed eterogenee.

Nuovi paradigmi quali il "*service oriented computing*", " *Infrastructure as a service*" (IaaS), "*Platform as a service*" (PaaS), permettono di acquisire una notevole capacità di calcolo e di gestione di piattaforme, in maniera semplice ed *on-demand*, potendo così essere allineate con le esigenze momentanee. In base alle informazioni trattate, diversi paradigmi di high performance computer possono essere necessari, quali *cluster computing, distributed and utility computing.*

E' necessario garantire che il processo dei dati sia fatto in maniera sicura ed affidabile, in particolare se sono utilizzate risorse ed infrastrutture fornite da terzi, e, se possibile, poter filtrare via dati non rilevanti per l'analisi in questione. Dal punto di vista degli algoritmi, e' necessario considerare tutte le problematiche relative alle tecniche di classificazione e riconoscimento di schemi, similarità ed anomalie su fonti eterogenee di dati.

La necessità di lavorare su flussi di dati in real-time, richiede nuove algoritmi rispetto a quelli esistenti.

Esistono inoltre molti problemi relativi all' indicizzazione di grandi basi di dati, utilizzando informazione semantica, così come la fusione ed aggregazione di informazione su basi/flussi di dati eterogenei. Parte integrante del processo di gestione della sicurezza è la capacità di supportare processi decisionali tempestivi ed efficaci, anche tramite il possibile riutilizzo di risorse informatiche già in produzione o in operazione.

Tra i vari campi applicativi che necessitano di architetture di *high performance computing*, da citare per la rapidità di acquisizione dei dati biometrici e di accesso ai dati preregistrati per la comparazione. La comparazione e' un processo per molti aspetti altamente "parallelizzabile".

Technology relevance:

1. Parallel Programming languages, Service oriented programming platforms [116-4]
2. Cloud/GRID/utility computing [116-10]
3. Data-mining, data fusion, similarity search, semantic search [113-4]
4. Secure and privacy-aware distributed computation [116-6]
5. Biometric data management [407-1]

Settori Guida di riferimento: 5

TA5.4 Metodologie e sistemi per il monitoraggio di grandi architetture di rete ICT al fine di detettare anomalie, tentativi di accesso non autorizzato, incidenti

Le evoluzioni delle tecnologie e l'esigenza di disporre di nuovi servizi IT stando cambiando le caratteristiche delle infrastrutture di rete ICT sia in termini di estensione che in termini di complessità. Cambiando le logiche architetturali anche le metodologie e i sistemi di monitoraggio devono adeguarsi al fine di preservare e garantire un livello di supervisione e controllo adeguato.

Le infrastrutture ICT rientrano infatti tra i settori individuati dalla UE come essenziali, quindi critici, per lo svolgimento di funzioni vitali della società.

Risulta quindi fondamentale la definizione e lo sviluppo di nuove metodologie, architetture e sistemi software per il monitoraggio, la rivelazione di anomalie, i tentativi di intrusione e gli incidenti di sicurezza che possano compromettere l'operatività delle grandi architetture di rete ICT.

Obiettivo della tematica è sviluppare metodologie e sistemi per il monitoraggio delle architetture di rete ICT che abbiano caratteristiche di scalabilità, robustezza, affidabilità e sicurezza. In particolare:

- definizione di modelli e metodi per la rilevazione di brecce e punti di debolezza nelle architetture che utilizzano reti ICT
- analisi delle caratteristiche di traffico per la prevenzione dei tentativi di attacco
- definizione e implementazione di modelli di trust tra reti ICT interconnesse
- architetture di reti resilienti
- gestione federata delle identità
- tecniche di *data-mining* e analisi *'wirespeed'* del traffico, al fine di individuare le anomalie in *real-time/near real-time*
- realizzazione di meccanismi di distribuzione e cooperazione geografica di sonde e collettori di informazioni di accounting per infrastrutture di larga scala ed alta capacità
- sicurezza logica delle reti (es. DNSSEC)
- effetti dei fenomeni naturali (sismici, vulcanici e climatici, etc) sulle infrastrutture ICT e relative contromisure per mitigarne gli effetti (ridondanza, resilienza, monitoraggio e previsione).

Technology relevance

1. IAM (Identity and Access Management) [306A-1]
2. AAA (Authentication, Authorization, Accounting) [117-12]
3. Public Key Infrastructure [117-6]
4. Network Management [416-10]
5. Trust Management [117-12]
6. SAML (*Security Assertion Markup Language*) e WS-Security (*Web Service Security*) [117-18]
7. High Availability [116-5]
8. ABAC (Attribute Based Access Control) security policies [117-12]
9. Wire-speed traffic analysis [113-8]
10. Data-mining [113-12]

Settori Guida di riferimento: 2, 5

TA5.5 Realizzazione di algoritmi e processi per l'estrazione automatica e l'elaborazione del contenuto informativo di immagini

L'impiego di immagini satellitari ad alta risoluzione è diventato sempre più comune nelle attività di monitoraggio di fenomeni ambientali su vasta scala e per rilevare situazioni di degrado di beni culturali. L'analisi di immagini ottenute in tempi successivi consente di valutare l'evoluzione temporale dei fenomeni e, tramite una modellazione accurata degli ecosistemi coinvolti ed un'analisi predittiva dei dati estrapolati, di prevederne le conseguenze a breve/medio termine, giungendo fino alla quantificazione, ove significativa, del danno ambientale ed economico. Inoltre tramite osservazione satellitare è possibile una mappatura dei dati a differenti scale spaziali e si può ovviare alle imprecisioni derivanti da specifiche caratteristiche del sito o dell'area di rilevazione.

L'obiettivo della ricerca è di sviluppare metodologie e servizi atti a fornire informazioni a supporto della riduzione di rischi ambientali e della prevenzione, attraverso:

- realizzazione di algoritmi e processi capaci di estrarre automaticamente da serie storica di dati telerilevati il contenuto informativo.
- realizzazione di algoritmi e processi automatici per l'elaborazione di immagini telerilevate ad alta risoluzione spaziale e spettrale.
- metodi per la valutazione di correlazioni spazio-temporali in stack di immagini.
- algoritmi di estrazione di mappe tematiche multiscala (spaziale e temporale) a partire da dati multi sorgente (piattaforma satellitare, piattaforma aerea, sensori di terra) ;realizzazione di modelli numerici capaci di assimilare dati telerilevati e rappresentare l'evoluzione multi-parametrica dei fenomeni ambientali e antropici.
- analisi di dati ad alta risoluzione spettrale per l'estrazione dell'informazione utile alla valutazione della connettività dei flussi tra aree vulnerabili e possibili sorgenti di rischio.
- data fusion di immagini aeree e satellitari per valutare lo stato di monumenti e siti e per monitorare evoluzioni di fenomeni e di interventi.

I risultati attesi di questa serie di attività porteranno un miglioramento in termini di:

- monitoraggio e rivelazione a grande scala di fenomeni locali;
- monitoraggio a scala locale attraverso la geo-localizzazione e la classificazione di immagini tele-rilevate ad alta risoluzione spaziale;
- analisi e studio delle interazioni esistenti tra le diverse scale spazio temporali, basati sull'assimilazione di dati satellitari, che permettano di descrivere i sistemi ambientali.
- Realizzazione di mappe sintetiche (GIS) che descrivono i flussi di connessione tra aree vulnerabili e sorgenti di rischio.

Technology relevance

1. Data mining [113-12]
2. Data fusion [113-4]
3. Change detection [113-1]
4. Tecniche di analisi multi/ iper-spettrali [113-1]
5. Interferometria SAR / PSI [217-5; 200-18]
6. Landscape / geo-hydrologic modelling [205-12; 114-5]

Settori Guida di riferimento: 10

.

TA5.6 Modelli architetturali e tecnologie per l'integrazione, l'elaborazione, la presentazione e la diffusione delle informazioni, considerando la molteplicità delle organizzazioni coinvolte, ognuna con specifici compiti istituzionali, e le esigenze di riservatezza dei dati

Gli strumenti informatici per l'elaborazione delle informazioni sono diventate le armi principali in dotazione alle organizzazioni impegnate nella lotta contro il crimine organizzato e il terrorismo. Il processo di globalizzazione e le caratteristiche di internazionalizzazione delle organizzazioni criminali e dei crimini stessi, come il traffico di esseri umani e l'immigrazione clandestina, il contrabbando di armi e droghe e le frodi finanziarie, rendono indispensabile la collaborazione tra le agenzie delle diverse nazioni coinvolte e gli organismi internazionali, quali EUROPOL e INTERPOL. Queste agenzie normalmente utilizzano strumenti informatici per acquisire informazioni dalle più diverse fonti ed estrarne elementi utili alle loro indagini o a prevedere situazioni di rischio per la sicurezza; le operazioni compiute comprendono il "*data-mining*", la correlazione e aggregazione delle informazioni e la "fusione" di nuove informazioni con le conoscenze già acquisite su organizzazioni, persone e modi di operare (profili). Naturalmente un'effettiva ed efficace cooperazione è possibile solo se i sistemi informatici utilizzati dalle varie agenzie possono essere resi interoperabili, in modo che le informazioni, le conoscenze acquisite e gli strumenti informatici possano essere facilmente condivisi (in un ambiente multinazionale, multilingua e multiculturale) e tenendo conto dell'esistenza di sistemi "*legacy*"; è però ugualmente necessario garantire il rispetto delle normative di sicurezza, della privacy e delle leggi vigenti nei diversi paesi nonché i requisiti di autonomia delle diverse organizzazioni coinvolte. L'approccio previsto è basato sullo sfruttamento di tecnologie mature o emergenti nel campo dell'ICT, quali SOA (*Service Oriented Architecture*), il Web Semantico, le ontologie. L'idea è di .consentire ad ogni agenzia di effettuare richieste verso altre agenzie cooperanti utilizzando *web services* semantici descritti in accordo ad un'ontologia comune, "scoperti", invocati e composti in modo automatico per soddisfare esigenze specifiche. Le richieste possono riguardare la disponibilità di informazioni, la condivisione di conoscenze o di strumenti avanzati per l'elaborazione o per il supporto decisionale.

Si può giungere in questo modo alla definizione di un'infrastruttura globale, basata su SOA per garantirne l'apertura, la scalabilità e la flessibilità, in cui siano disponibili una serie di servizi di base ("core") e di servizi funzionali per il supporto di attività specifiche di ogni categoria di utente. Sarà possibile in questo modo fornire servizi ad altre agenzie senza rendere pubblici ulteriori dettagli su basi di dati o strumenti di elaborazione.

Le attività di ricerca dovranno:

- definire l'architettura del sistema globale
- definire e descrivere i servizi richiesti
- definire un'ontologia comune nel settore della sicurezza ("*law-enforcement*")
- definire in dettaglio e sperimentare le soluzioni tecniche
- dimostrare l'utilità dell'infrastruttura ed illustrare i benefici ottenibili;
- fornire linee-guida per l'applicazione pratica su larga scala del concetto sviluppato, con particolare riferimento alle problematiche organizzative e agli aspetti legali.

Technology relevance:

1. Algoritmi per Information Management (*Data Fusion, Integration of behavioural and content analysis*) [113-4; 113-12]
2. Conversione/fusione di ontologie [113-7]
3. Gestione della sicurezza in ambiente distribuito (Standardisation of security information identification, Trust management, …) [412-4]
4. Modelli architetturali basati sulla combinazione dei modelli SOA e EDA (*Event Driven Architecture*) [116-4]

Settori Guida di riferimento: 6

Area Tecnologica 6: CBRNE

La minaccia CBRNE per sua natura potrebbe pesantemente impattare su una vasta scala di attività quotidiane legate alle attività dei cittadini. In generale la minaccia CBRNE si traduce in:

- Attacco con esplosivo;
- Attacco chimico- biologico (nelle acque, nel terreno e in atmosfera);
- Attacco radiologico;
- Agro-terrorismo (contaminazione batterica e radiologica della catena di distribuzione del cibo);
- Contraffazione dei medicinali

A tale scopo, le aree di ricerca per contrastare tale tipo di minaccia, possono essere classificate come:

- Detection e identification della minaccia di attacco chimico, nucleare e da attentato terroristico con esplosivi;
- Epidemia e gestione di emergenze sanitarie;
- Rapidità nella risposta per la Sicurezza (nucleare, batteri, virus ed esplosivi);
- Intercettazione manomissione container/ mezzi / persone etc per prevenire l'attacco CBRNE

Le tecnologie afferenti all'area CBRNE includono:

- Detection e identificazione della minaccia terroristica :
  - Sensori per la detezione di sostanze NBC
  - Sensori per la detezione di sostanze esplosive in tracce e/o di IED (Improvised Explosive Devices) nei siti sensibili, nelle stazioni e sui veicoli
  - Sistemi di monitoraggio stand-off
  - Sistemi per la rivelazione di armi e sistemi per innesco (detonatori) di ordigni
  - Sensori e sistemi di sensori con capacità embedded di analisi early warning;
- Epidemia e gestione di emergenze sanitarie;
  - Strutture di ricovero facilmente e rapidamente deployabili;
  - PPE- personnel protective equipment (equipaggiamenti per FiRe);
- Rapidità nella risposta per la Sicurezza;
  - Sensori in grado di supportare l'attività forense degli operatori in campo;
  - Pianificazione (prevenzione e preparedness) contro contaminazione su larga scala;
- Bio-detection e identification:
  - Piani per la prevenzione e il diffondersi di epidemie;
  - Laboratori mobili;
  - Centri sanitari mobili.

TA6.1 Sensori di elevata sensibilità per la rivelazione di composti in tracce (esplosivi, droghe, chimici, biologici, veleni, e loro precursori) per apparati fissi o mobili

La minaccia terroristica, ha come obiettivo quello di attaccare la società civile nelle sue attività quotidiane e nei suoi centri vitali. Vi è quindi una maggiore richiesta di disporre di sistemi da distribuire sul territorio in grado di rilevare precocemente esplosivi, droghe, agenti chimici tossici, agenti biologici per salvaguardare la comunità dall'eventuale loro uso a scopo terroristico.

Emerge così la necessità di dotarsi di sensori specifici, e possibilmente economici, per la rivelazione rapida di queste sostanze che abbiano una sensibilità elevata in modo tale da rilevare la loro presenza nell'ambiente in quantità minime (tracce) prima che esse possano causare danni ai cittadini.

Tra le sostanze da rilevare, rivestono un'importanza fondamentale gli esplosivi e gli inneschi, soprattutto quelli usati più recentemente, inclusi i loro precursori, in quanto sempre più spesso la minaccia proviene da esplosivi e inneschi fabbricati in casa (IE; Improvised Explosive). Di interesse per la sicurezza è la creazione di una sistema di raccolta dati anche per la tracciatura relativa alle informazioni chimiche e morfologiche di particelle potenzialmente collegate all'utilizzo di armi da fuoco e inneschi, in grado di discriminare gli osservabili utili a tale scopo da quelli fuorvianti di differente natura e origine e di identificare la provenienza degli esplosivi e degli inneschi (tracciabilità). Da segnalare poi le sostanze chimiche, che possono rappresentare un pericolo diretto per la salute delle persone o per l'ambiente. Infine è necessario considerare anche gli agenti biologici (batteri e virus) che rappresentano un ulteriore rischio di attacchi terroristici.

Gli agenti da rilevare possono essere in diverse forme: vapore, liquida, solida, aerosol. Occorre quindi sviluppare sensori ad altissima sensibilità che possano individuare precocemente tutte queste minacce, (per esempio identificando soggetti che hanno recentemente utilizzato esplosivi, inneschi o armi da fuoco), che dovranno essere utilizzati nei luoghi più critici (aeroporti, stazioni metro, installazioni critiche, etc.), operando in continuo, in postazioni che possono essere fisse o mobili.

Molti di questi sensori, grazie alle tecnologie utilizzate, hanno la possibilità di poter essere applicate con successo anche in altri campi, dimostrando così una loro multidisciplinarietà ed in particolare in tutti quei campi ove sia necessario rilevare sostanze pericolose in tracce.

Technology Relevance:

1. Sensori spettroscopici ad alta risoluzione nella banda UV VIS IR [100-5; 110-6; 110-7]
2. Sensori al Terahertz [110-8; 200-23]
3. Sensori a Radio Frequenza [110-10]
4. Sensori Acoustici [110-14]
5. Sensori Laser [109-1]
6. Spettrometri con componenti Nanomeccanici [110-15]
7. Spettroscopia atomica LIBS (*Laser Induced Breakdown Spectroscopy*) e Spettroscopia Raman [106; 110-6;110-12]
8. Microscopia elettronica a scansione ad elevata risoluzione (FESEM-EDS)[110-6; 110-12]
9. Dispositivi conduttometrici [100-13]
10. Sensori basati su materiali nano-strutturati [100-20; 110-15; 121-2]

Settori Guida di riferimento 6, 7, 12

TA6.2 Sensori per monitoraggio a distanza di pericoli chimici e biologici da postazione mobile o fissa

La capacità di rivelazione rapida e di identificazione di agenti chimici e biologici o di sostanze potenzialmente tossiche è un problema prioritario per tutelare la pubblica sicurezza, minacciata da attacchi terroristici.
Il rischio di attacchi di questo tipo è praticamente imprevedibile, essendo delocalizzato sul tutto il territorio, ed assume ancora maggiore rilevanza per l'imprevedibilità delle conseguenze del rilascio senza controllo nell'ambiente di agenti chimici e/o biologici. Nel caso di attacco con agenti particolarmente tossici e aggressivi, esiste il rischio che il rilascio coinvolga, oltre al bersaglio predestinato, anche un numero imprecisato di persone. La rilevazione precoce di nubi tossiche o più in generale del rilascio di sostanze pericolose nell'ambiente è un obiettivo che deve essere necessariamente perseguito per permettere la prevenzione dei danni alla popolazione causati da tali eventi. Lo sviluppo di sensori per il monitoraggio a distanza, capaci di seguire l'evoluzione di nubi tossiche, non solo contribuisce a mettere precocemente in allarme le amministrazioni responsabili della sicurezza dei cittadini, attivando le risposte opportune, ma permette inoltre di comprendere i fenomeni di diffusione e dispersione delle sostanze e quindi consente ai decisori preposti di attuare le contromisure necessarie ad evitare o mitigare gli effetti dannosi. Una nube tossica può espandersi e seguire percorsi influenzati dalla presenza di forze fisiche (venti, correnti, ecc.) o di ostacoli naturali. Data la difficoltà di discriminare queste sostanze nell'ambiente naturale o in zone a rischio confinate, questi sensori dovranno fornire delle informazioni in tempo reale circa la presenza di agenti chimici e/o biologici, la distanza a cui sono stati rilevati e possibilmente la loro distribuzione tridimensionale. Questi sensori dovranno essere realizzati in strutture rigide che possano essere facilmente installate su postazioni fisse o mobili e operare in modalità continua anche disattesa.

Nella scelta dei parametri tecnici, questi apparati dovranno rispettare le norme di sicurezza vigenti. Infine sarebbe auspicabile la realizzazione di almeno un tipo di unità centrale in grado di interpretare le informazioni provenienti da più sensori, così fornendo un numero di falsi allarmi il più contenuto possibile (*False Alarm Rate* -FAR-), ed una previsione dei fenomeni dinamici (espansione o propagazione). L'approccio multisensore è particolarmente adatto per realizzare procedure di monitoraggio a basso FAR: più sensori basati su differenti principi o differenti lunghezze d'onda dello spettro elettromagnetico possono fornire più informazioni analitiche, consentendo un'elevata selettività della procedura complessiva, basata sull'idonea interpretazione di tutti i dati raccolti.

Technology Relevance:

1. Radar [200-17110-8]
2. LIDAR [200-22]
3. LIBS [106; 110-6; 110-12]
4. Spettroscopia Raman [110-6110-12]
5. Spettroscopia terahertz [110-9]
6. Moduli di controllo di processo [112-1; 112-2; 112-3: 304B-9]
7. Moduli di raccolta ed elaborazione dei dati [116-9; 113-3; 113-8]

Settori Guida di riferimento: 7,13

TA6.3 Piattaforme multisensori intelligenti per la riduzione dei falsi allarmi nel monitoraggio di bio-hazard

La minaccia terroristica ricorre a diversi agenti tossici e nocivi con lo scopo di danneggiare direttamente infrastrutture o individui, ma spesso anche di compromettere l'economia di un paese o di una azienda. Tra gli agenti a disposizione sono di particolare rilevanza agenti biologici (biohazard), quali organismi viventi o componenti degli stessi, in grado di provocare malattie o decessi per l'essere umano oppure di infettare piante o animali destinati all'alimentazione umana.

Questa problematica è di particolare interesse anche nei sistemi di controllo della filiera agroalimentare ove occorre controllare le alterazioni indotte da un non corretto handling oppure causate da azioni di *tampering* con l'introduzione illegittima di sostante chimiche, biologiche o radiologiche nel cibo. Un vantaggio nella rilevazione di agenti *biohazard* in ambienti antropizzati o in ambienti naturali consiste nel fatto che ogni organismo vivente ha caratteristiche genetiche peculiari che possono essere sfruttate per l'identificazione. Gli studi di genomica e il sequenziamento di genomi di organismi di interesse ha fornito gli strumenti per lo sviluppo di tecnologie basate sulla analisi degli acidi nucleici in ambiente da elaborare poi con strumenti bioinformatica.

In particolari circostanze, tuttavia, le tracce molecolari degli organismi possono essere danneggiate o presentarsi in quantità ridotte ai limiti della rilevabilità. In simili casi diventa utile poter sfruttare simultaneamente più tecniche di identificazione, ricorrendo a piattaforme con sensori basati su principi diversi, per raccogliere il maggior numero di informazioni.

Le informazioni devono poi essere raccolte, analizzate e confrontate per giungere alla identificazione. Le tecnologie necessarie a tale scopo portano quindi a piattaforme multisensoristiche dotate di Intelligenza Artificiale per l'elaborazione dei dati. Il concetto di *data fusion* in particolare si riferisce alle procedure per unire insieme dati riferiti a parametri molto diversi, chimici, fisici, biologici. Molteplici sensori possono essere visti come componenti di tali piattaforme: da quelli basati sul riconoscimento di acidi nucleici e proteine, a quelli che rilevano molecole volatili o in soluzione, fino a sensori visivi che catturano immagini.

La miniaturizzazione dei sensori diventa rilevante nel momento in cui si vogliono installare più sensori nei punti critici di determinate infrastrutture o ambienti, facendo confluire tutti i dati in un unico punto centrale. Il ricorso alla nanotecnologie diventa significativo soprattutto in questo contesto.

Technology Relevance:

1. Intelligenza artificiale [114-1]
2. Trasmissione ed elaborazione di dati di provenienza diversa [113-7113-8]
3. RealTimePCR e DNA/immuno-array portatili [121-5; 203-7;121-9; 200-11; 200-28]
4. Reazioni immunochimiche con Surface Plasmon Resonance [101-12; 108-1; 121-5; 121-9; 200-28]
5. μTAS e Lab-on-a-chip [204-7; 200-28; 121-5; 121-9]
6. GC e HPLC portatili [121-9; 200-10]
7. Naso e lingue elettronici [110-15; 110-14; 200-9];
8. Sensori di gas e vapori [204-1; 110-14];
9. Visione artificiale sorveglianza con videocamera [217-3; 203-1; 200-2]
10. Sensori chimici con nanotubuli di carbonio e nanotecnologie [204-7; 110-15; 121-2]

Settori Guida di riferimento: 3,5,6,12

TA6.4 Tecnologie microfluidiche accoppiate a nanostrutture molecolari per la detezione di biohazard

La minaccia terroristica ricorre a diversi agenti tossici e nocivi con lo scopo di danneggiare direttamente infrastrutture o individui, ma spesso anche di compromettere l'economia di un paese o di una azienda. Tra gli agenti a disposizione sono di particolare rilevanza agenti biologici (*biohazard*), quali organismi viventi o componenti degli stessi, in grado di provocare malattie o decessi per l'essere umano oppure di infettare piante o animali destinati all'alimentazione umana.

Il riconoscimento di agenti biologici comporta solitamente l'identificazione del patogeno a livello medico, nel caso dell'uomo, con tecniche microbiologiche convenzionali, per poi risalire all'indietro e cercare la possibile causa di contaminazione lungo la filiera interessata. Tali approcci sono validati e sicuri ma richiedono tempi lunghi, che spesso riducono le probabilità di trovare l'agente causante. Innovazioni in questo campo hanno introdotto metodiche di analisi diretta di DNA o proteine rilevate nell'ambiente di interesse, fornendo così dati oggettivi su cui basare il riconoscimento del patogeno mediante i dati immagazzinati in banche dati di sequenze. Se queste tecniche rendono più veloce e sicuro il riconoscimento del patogeno, rendono anche possibile monitorare in tempo reale ambienti e punti critici prelevando campioni a tempi prefissati e agendo in maniera preventiva contro eventuali attacchi terroristici. Le analisi genetico-molecolari si basano su reazioni biochimiche che spesso coinvolgono poche molecole e che possono svolgersi in condizioni miniaturizzate. Le applicazioni microfluidiche volte alla miniaturizzazione di tecniche analitiche classiche, quali *Lab-on-a-chip*, sono nate proprio per scopi di difesa e lotta al terrorismo. La microfluidica è oggi applicata a molti tipi di sensori diversi, per la rilevazione di molecole volatili, di molecole in soluzione, di proteine, di acidi nucleici, arrivando addirittura alla amplificazione con rilevamento diretto di frammenti di DNA mediante *array* o piattaforme a e-DNA. Il comportamento peculiare delle nanostrutture, non ripetibile a livelli di scala maggiore, fornisce ulteriormente la possibilità di reazioni specifiche.

Technology Relevance:

1. μTAS e Lab-on-a-chip [200-28; 204-7; 121-5; 200-11]
2. GC e HPLC portatili e miniaturizzati [121-9; 200-10]
3. RealTimePCR portatile [203-7; 121-5; 200-11]
4. DNA/immunoarray portatili e miniaturizzati [203-7; 121-5; 200-11]
5. Analizzatore automatico per DNA ambientale: estrazione, purificazione, amplificazione per la rilevazione di patogeni [203-7; 204-7; 200-28 ;121-5 ;200-11]
6. Naso e lingua elettronici [110-15; 110-14; 200-9]
7. Sensori chimici a nanotubuli di carbonio e altre nanotecnologie [204-7; 110-15; 121-2]
8. Fluorescenza amplificata da metalli per sensori ottici [101-12; 108-1; 110-15]
9. Codici a barre con Quantum dots per marcatura di DNA [205-7; 203-7; 110-15; 200-11]
10. Piattaforme a DNA elettronico (E-DNA) [203-7; 200-3; 200-11]

Settori Guida di riferimento: 6, 12

TA6.5 Grandi portali di nuova generazione con attivazione neutronica o raggi X per la rivelazione di materiale nucleare o esplosivo dentro i container con l'impiego di rivelatori passivi che operano in ambiente ostile

La rilevazione di esplosivi o materiali nucleari è un campo di forte interesse politico, scientifico e industriale a livello mondiale, a causa dell'impatto della crescente minaccia di attentati terroristici. Vi è un crescente interesse nel campo della security per la difficoltà di esaminare con rigore grandi quantità di merci. Oggi circa il 90% delle merci nel mondo si muovono con container e l'ispezione di quelli che entrano in ogni paese via strada, ferrovia, nave o aereo è un compito arduo. L'elevato numero dei container è tale per cui il tempo disponibile per fare un controllo deve essere mantenuto breve.
Gli attuali mezzi di controllo, come quelli a raggi X sono molto carenti nel fornire informazioni che potrebbero non essere connessi con la presenza di esplosivi.
Le tecniche nucleari ordinarie con grandi sorgenti radioattive possono produrre l'attivazione radioattiva dei materiali testati e suoi dintorni; sono pericolosi in caso di esplosione del materiale testato e quindi possono divenire essi stessi bersaglio di un attentato terroristico. Con nuovi grandi portali forniti di generatori di neutroni, sarà possibile influenzare le procedure di sicurezza con soluzioni per la sorveglianza delle frontiere terrestri, aeree o marittime. Un generatore di neutroni adatto a questi scopi è, ad esempio, il Plasma Focus PF associato ad un moderatore, filtri, efficienti rivelatori gamma, moduli di rilevamento, moduli di raccolta dati e sensori. Il PF potrà essere impiegato in diverse applicazioni, grazie ad una ottimizzazione adeguata dei filtri.
Un apparato di filtraggio innovativo produce raggi X e neutroni veloci con spettri e assorbimenti diversi per ottenere misure da comparare e limitare il numero di falsi allarmi. Rilevatori permettono di individuare il picco Gamma prodotto quando l'elemento azoto nascosto (elemento chimico essenziale per esplosivi) è colpito dai neutroni termici (prodotti dal PF insieme ad un adeguato moderatore). Tali apparecchiature dovranno anche operare in un ambiente ostile per rilevare esplosivi o materiale nucleare all'interno di container. Armi chimiche, potenzialmente presenti nei cargo, possono essere accompagnate da vapori chimici distintivi consentendo la loro individuazione. Tra i componenti di armi nucleari il Pu239 ha emissioni radioattive deboli ma rilevabili. D'altra parte, l'U235 in forma di "uranio altamente arricchito" (HEU) presenta deboli emissioni di raggi gamma ed emissioni trascurabili di neutroni.
Per questi motivi un nuovo concetto di indagine mediante neutroni rallentati e raggi gamma, con rilevatori ad alta efficienza, è proposta per l'identificazione di armi chimiche, materiale fissile e oggetti non schermati come esplosivi.

Technology relevance:

1. Neutron generators [110-1]
2. Plasma Focus neutron generators [106; 110-1];
3. FASt and thermal neutrons [110-1]
4. X-rays [110-2]
5. Gamma rays [110-3]
6. Moderator [110-1]
7. Filters [110-1]
8. performing gamma-ray detectors [110-3]
9. detection processing module [112-2]
10. data collection modules and sensors [113-3]

Settori Guida di riferimento: 3, 11

TA6.6 Tecnologie di scansione rapida, da onde millimetriche a raggi X, per la ricostruzione di immagini e rivelare pericoli da postazione fissa al fine di rilevare esplosivi ed altri materiali pericolosi

Tecnologie efficaci per la rilevazione di armi ed esplosivi sono indispensabili per contrastare le minacce CBRN in luoghi che necessitano di elevata sicurezza, come aeroporti e stazioni.
Requisiti analoghi devono essere soddisfatti per tutti gli aspetti di sicurezza del territorio e per qualsiasi infrastruttura critica il cui degrado di servizio può facilmente estendersi ad altre infrastrutture, secondo l'effetto domino, aumentandone l'impatto.
Persone o mezzi che trasportano armi o esplosivi nascosti, o chiunque altro abbia attacchi terroristici in mente, devono essere individuati in qualsiasi circostanza.
I sensori utilizzati per fini di sicurezza devono essere in grado di effettuare un controllo non invasivo delle persone, dei bagagli e dei mezzi, con l'obiettivo di individuare armi, anche se di ceramica o plastica, esplosivi liquidi o al plastico, e sostanze chimiche o biologiche.
Tali sensori devono inoltre adattarsi ed essere efficienti in qualsiasi condizione ambientale.
Tecnologie valide ai fini della sicurezza e in grado di gestire queste tipologie di minacce sono i sistemi per ricostruzione delle immagini.
Questi sistemi si basano sulla capacità di "guardare" attraverso i materiali, e sulla possibilità di garantire una sufficiente risoluzione geometrica all'interno di un area stabilita.
Particolarmente interessanti sono le tecnologie che permettono di identificare il tipo di materiale e di distinguere tra materiali con caratteristiche fisiche simili.
I sistemi per la ricostruzione di immagini, grazie alla capacità di rivelare sostanze pericolose nascoste da postazione fissa a distanza, saranno il cuore di tutti i sistemi di sicurezza nei gateway delle infrastrutture critiche e potranno notevolmente migliorare il rivelamento delle potenziali minacce in situazioni rischiose con elevato affollamento.

Technology relevance:

1. Sistemi attivi e passive ad onda millimetrica per la ricostruzione di immagini; [110-11; 200-19]
2. Sistemi attivi tridimensionali ad onda millimetrica per la ricostruzione tridimensionale delle immagini; [113-1; 110-11; 200-19]
3. Sistemi ad onda sub-millimetrica per la ricostruzione di immagini [118-2; 110-11; 200-19];
4. Sensori THz per la ricostruzione di immagini [200-23; 110-8];
5. Antenne con diagramma di radiazione riconfigurabile [108-3];
6. Antenne riconfigurabili con tecnologia microelettromeccanica (MEMS) [108-3; 110-21];
7. Focal Plane Array Antenna (FPA) [108-3];
8. Spettroscopia a raggi X [110-2; 200-13];
9. Sensori a conteggio di fotoni per rivelazione X diretta e riflessa [200-13; 108];

Settori Guida di riferimento: 7

TA6.7 Nanotecnolgie per sistemi in spettrometria di massa: applicazioni nella rivelazione di esplosivi, droghe (metaboliti e impurezze).

Le droghe naturali e sintetiche costituiscono un'enorme fonte di lucro per la criminalità organizzata, e le vie del narcotraffico spesso si incrociano con altri tipi di attività illegali, tra cui il terrorismo. D'altra parte le sostanze esplosive hanno spesso tensioni di vapore talmente basse da essere difficilmente rilevabili soprattutto da remoto e quindi richiedono sofisticati sistemi di rivelazione spesso anche complessi anche in termini di preparativa.

La richiesta di tecnologie idonee ad evidenziare e caratterizzare la presenza, anche in tracce, di sostanze tossiche e/o pericolose (i.e. droghe , esplosivi ed inneschi) è quindi pressante:. considerata la gran mole di analisi che i laboratori devono effettuare, è estremamente importante sviluppare metodi analitici affidabili, veloci, economici e a basso impatto ambientale.

Questi sistemi dovranno rispondere inoltre a ulteriori richieste come un basso consumi, alta efficienza e selettività, tempi di analisi ridotti e un facile accoppiamento con altri sistemi di indagine analitici.

È da sottolineare inoltre che per argomentazioni anche forensi, la richiesta più rilevante riguarda la necessità di analizzare piccolissimi volumi di campione garantendo altresì elevatissime selettività e un notevole incremento della sensibilità (fino a poche parti per trilione) anche grazie a metodi di pre-concentrazione.

Un impulso notevole può venire dallo sviluppo di sistemi portatili basati su nanotecnologie che permettano la realizzazione di rivelatori altamente efficienti e che utilizzino materiali innovativi (quali polimeri, nanostrutture a base carbonio, silicio, carburo di silicio, magnetiche, molecolari etc.), che saranno validi strumenti per l'analisi immediata dei composti di interesse sia in fase gassosa che liquida.

Technology relevance:

1. Colonne capillari impaccate e monolitiche [110-15; 200-10; 200-11]
2. Sistemi di pompaggio miniaturizzati [304B-16; 200-10; 200-11]
3. Sistemi per cromatografia nano bidimensionale [200-10; 200-11]
4. Detector UV VIS on column [110-6; 100-7]
5. Spettrometro di Massa Ion Trap, triplo-quadrupolo, Time of Flight (TOF) [110-4; 200-10; 200-11]
6. Spettrometrie di massa a reazione di trasferimento di protoni (PTR-MS) [110-4; 200-10; 200-11]
7. Interfacce nano-ESI e nano-MALDI (commerciali e non) [110-15; 200-10; 200-11]
8. Micro e nano bilance in Si e SiC funzionalizzate in tecnologia MEMS-NEMS, Nanosistemi e Bio-MEMS [110-21]

Settori Guida di riferimento: 6, 7, 12

TA6.8 Strumenti compatti ed efficienti per la rivelazione di parti metalliche di armi e munizioni o detonatori

I grandi eventi richiamano una notevole quantitàdi persone, e accade purtroppo di frequente, che a queste circostanze si associno atti di violenza, come quelli negli stadi, di grande richiamo anche per possibili azioni terroristiche: si rende pertantonecessaria l'introduzione di misure di sicurezza ,a vario livello, all'ingresso di questi siti e, in generale, di altre strutture sensibili.
Questi presidi di sicurezza devono essere utilizzati in ambienti ad altissima affluenza ai quali le persone arrivano in tempi molto ridotti e con tempi operativi limitati. In questi contesti, l'efficienza degli apparati di controllo costituisce un elemento importante per l'efficacia dell'azione e perciò per la salvaguardia delle persone e degli operatori stessi.
I rivelatori di parti metalliche di armi, munizioni, mine o detonatori (*metal detectors*) hanno quindi un ruolo fondamentale per la sicurezza dei cittadini. Per questo motivo le normative sui metal detector stanno diventando sempre più stringenti. Esistono diverse tipologie di *metal detector*, manuali o portali, per l'ispezione di persone in transito e le procedure che utilizzano tali strumenti richiedono apparati di altissime prestazioni operative e funzionali.
I *metal detector* sono utilizzati a protezione degli accessi di edifici o mezzi di comunicazione (aerei, treni) e sono adibiti all'ispezione delle persone in transito. Attualmente sta emergendo la necessità di individuare oggetti metallici sempre più piccoli, a causa della minaccia rappresentata da ordigni improvvisati *(Improvised Explosive Device,* IED) le cui componenti metalliche si stanno sempre più riducendo. Tale esigenza si scontra con il problema di discriminare un'elevata quantità di oggetti metallici di impiego comune sulle persone ispezionate, che causa allarmi inutili ed inutili perdite di tempo.
La nuova sfida in questo campo è la rivelazione dei detonatori che sono la parte più piccola di un ordigno ma quella indispensabile per il suo funzionamento.
Questi sistemi devono poter operare nelle diverse condizioni anche sott'acqua per la ricerca di ordigni.

Technology Relevance:

1. Conduttori magnetici ad elevata efficienza [100-13]
2. Rivelatori di campo elettromagnetici compatti ed efficienti a differenti bande spettrali [110-13; 200-24]
3. Magnetometri efficienti [200-5]
4. Generatori di impulsi ad alta tensione modulabili a singolo o doppio impulsi [112-1]

Settori Guida di riferimento: 7

TA6.9 Strumentazione portatile attiva o passiva per il monitoraggio di materiale radioattivo in discariche o in container commerciali

La minaccia terroristica può concretizzarsi nell'uso delle cosiddette "bombe sporche" costituite da materiale radioattivo proveniente da centrali nucleari o da attività ospedaliere. Tali bombe non sono di per sé armi nucleari, ma provocano danni alla popolazione in quanto diffondono materiale radioattivo.
All'attività tipicamente terroristica si può talvolta sommare l'attività di smaltimento illegale di materiale radioattivo che provoca la contaminazione di discariche pubbliche con gravissime conseguenze per la salute dei cittadini e l'integrità del territorio circostante.
Inoltre, come già accaduto nel recente passato, vi è la possibilità di tentativi di commercio di derrate alimentari, o comunque più in generale merci, che presentano un'elevata radioattività in quanto provenienti da zone fortemente contaminate.
Da qui la necessità di monitoraggio delle merci nei caratteristici luoghi di transito e all'ingresso delle discariche per individuare ed identificare, al fine del successivo corretto smaltimento e del riconoscimento della probabile origine, eventuali carichi di materiale radioattivo.
Essendo circa il 90 % dei beni oggetto di commercio trasportato via mare con oltre 72 milioni di container, il controllo nelle strutture portuali assumerà un'importanza rilevante.
Inoltre, il materiale radioattivo è tipicamente trasportato insieme a merci legali e quindi in qualche modo nascosto da queste, quindi gli strumenti di rivelazione devono presentare elevata sensibilità.
A causa della diversa tipologia delle situazioni in cui le verifiche possono essere condotte (ferrovie, porti, aeroporti, dogane in genere, discariche) sembra essere necessario lo sviluppo anche di sistemi portatili al fine di permettere un adeguato contrasto al fenomeno.
I sistemi attivi, più costosi e complessi, garantiscono tuttavia una migliore affidabilità nella detezione, e, irradiando il sistema con neutroni o elettroni ad alta energia, permettono ai rilevatori di identificare anche le sostanze nascoste in contenitori.

Technology Relevance:

1. Spectroscopic gamma ray detectors [110-3; 200-14]
2. Passive millimetre wave imaging [110-11; 200-19]
3. Active millimetre wave imaging [110-11; 200-19]
4. Fast and thermal neutrons [110-1]
5. Terahertz technologies [110-8; 200-23]
6. Data processing and data fusion [113-4]

Settori Guida di riferimento: 8; 11

Referenti dei Settori Guida e dei TA

1. Sicurezza ferroviaria	Antonio Ruggieri
2. Protezione dell'approvvigionamento, della generazione e della distribuzione di energia elettrica	Sandro Bologna
3. Sicurezza del trasporto multimodale	Ileana D'angelo
4. Sicurezza del trasporto su strada	Maurizio Miglietta
5. ICT per la Sicurezza	Luigi Romano
6. Sicurezza dei confini	Dino Giuli
7. Sicurezza aeroportuale	Stefano Pasquariello
8. Tecnologie satellitari per il controllo del territorio e dell'ambiente	Paolo Bellofiore
9. Sicurezza nel costruito	Francesco Soldovieri
10. Sicurezza integrata nei beni culturali	Laura Moltedo
11. Sicurezza nucleare	Enrico Mainardi
12. Sicurezza agroalimentare	Raffaello Prugger
13. Sicurezza & Salute	Claudio De Lazzari

Chair dei TA

TA1	Claudio Moriconi
	Carlo Asperti
TA2	Angeloluca Barba
	Paolo Proietti
TA3	Mario Savastano
	Alberto Bianchi
TA4	Paolo Fichera
	Gianfranco Fornaro
TA5	Fabio Martinelli
	Daniele Cecchi
TA6	Antonio Palucci
	Nelson Marmiroli

Lista dei Partecipanti

Consiglio Nazionale delle Ricerche ICT	**Consiglio Nazionale delle Ricerche Dipartimento Tecnologie dell'Informazione e delle Comunicazioni (ICT)** • Sandro Massa • Luca Papi
FINMECCANICA	**Finmeccanica S.p.A.** • Cristina Leone • Michela Alunno Corbucci • Luca Giannicchi

AleniaAeronautica	**Alenia Aeronautica S.p.A** • Giulio Bertino
AnsaldoEnergia A Finmeccanica Company	**Ansaldo Energia S.p.A.** • Claudio Ravera • Carla Penno • Carlo Bima
AnsaldoNucleare Una Società Finmeccanica	**Ansaldo Nucleare S.p.a..** • Enrico Mainardi
AnsaldoSTS A Finmeccanica Company	**Ansaldo STS** • Nadia Mazzino • Concetta Pragliola • Antonio Ruggieri • Wellington Toapanta
CRF CENTRO RICERCHE FIAT	**Centro Ricerche FIAT** • Alberto Maria Merlo • Maurizio Miglietta
CONFAPI	**CONFAPI - Confederazione italiana della piccola e media industria privata** • Armando Occhipinti • Maria Teresa Ruffo

Consiglio Nazionale delle Ricerche	**Consiglio Nazionale delle Ricerche** **Dipartimento Energia e Trasport i** • **Roberto Caldon** • **Vincenzo Delle Site**
Consiglio Nazionale delle Ricerche	**Consiglio Nazionale delle Ricerche** **Dipartimento di Medicina** • **Claudio De Lazzari**
Consiglio Nazionale delle Ricerche	**Consiglio Nazionale delle Ricerche** **Dipartimento Patrimonio Culturale** • **Laura Moltedo**
Consiglio Nazionale delle Ricerche	**Consiglio Nazionale delle Ricerche** **Istituto di Analisi dei Sistemi ed In-formatica "Antonio Ruberti"** • **Elaheh Pourabbas** • **Claudio Gentile** • **Carlo Gaibisso** • **Alberto Gandolfi** • **Paolo Ventura** • **Fabio Guglietta** • **Maurizio Proietti** • **Andrea De Gaetano**
Consiglio Nazionale delle Ricerche	**Consiglio Nazionale delle Ricerche** **Istituto di Elettronica ed Ingegner-ia dell'informazione e delle teleco-municazioni** • **Maurizio Aiello**
Consiglio Nazionale delle Ricerche	**Consiglio Nazionale delle Ricerche** **Istituto di Informatica e Telematica** • **Raffaele Bruno** • **Fabio Martinelli**
Consiglio Nazionale delle Ricerche	**Consiglio Nazionale delle Ricerche** **Istituto di Metodologie per l'Analisi Ambientale** • **Vincenzo Cuomo** • **Nicola Pergola** • **Stefano Pignatti**

Consiglio Nazionale delle Ricerche Imc Istituto di Metodologie Chimiche	**Consiglio Nazionale delle Ricerche** **Istituto di Metodologie Chimiche** • **Salvatore Fanali** • **Zeineb Aturki**
Consiglio Nazionale delle Ricerche	**Consiglio Nazionale delle Ricerche** **Istituto di Scienze delle Produzioni Alimentari** • **Angelo Visconti** • **Palmiro Poltronieri**
Consiglio Nazionale delle Ricerche	**Consiglio Nazionale delle Ricerche** **Istituto di Scienze e Tecnologie della Cognizione** • **Amedeo Cesta**
Consiglio Nazionale delle Ricerche	**Consiglio Nazionale delle Ricerche** **Istituto di Studi sui Sistemi Intelligenti per l'Automazione** • **Arcangelo Distante** • **Nicola Veneziani** • **Guido Pasquariello** • **Ettore Stella** • **Gianni Attolico** • **Massimo Ianigro** • **Grazia Cicirelli** • **Marco Leo** • **Tiziana D'Orazio**
Consiglio Nazionale delle Ricerche	**Consiglio Nazionale delle Ricerche** **Istituto per il Rilevamento Elettromagnetico dell'Ambiente** • **Gianfranco Fornaro** • **Francesco Soldovieri**
Consiglio Nazionale delle Ricerche	**Consiglio Nazionale delle Ricerche** **Istituto per lo Studio dei Materiali Nanostrutturati** • **Giuseppina Padeletti** • **Gabriel Maria Ingo** • **Maria Pia Casaletto**
cini Consorzio Interuniversitario Nazionale per l'Informatica	**Consorzio Interuniversitario Nazionale per l'Informatica** • **Luigi Romano** • **Salvatore D'Antonio**

cnit consorzio nazionale interuniversitario per le telecomunicazioni	**Consorzio Nazionale Interuniversitario per le Telecomunicazioni** • **Federica Paganelli** • **Fabrizio Cuccoli** • **Franco Davoli** • **Giuseppe Bianchi**
ELSAG DATAMAT A Finmeccanica Company	**ElsagDatamat S.p.A.** • **Alberto Bianchi** • **Franco Borasi** • **Roberto Carattoli** • **Franco Cavagnaro** • **Anna Maria Colla** • **Bruno Conterno** • **Angela Maria Ileana D'Angelo** • **Mario D'Intino** • **Giovanni Garibotto** • **Giuseppe Martufi** • **Marina Settembre**
ENAV S.p.A. SOCIETÀ NAZIONALE PER L'ASSISTENZA AL VOLO	**ENAV S.p.A.** • **Francesco Di Maio** • **Bruno Carbone**
ENEA	**ENEA Agenzia nazionale per le nuove tecnologie, l'energia e lo sviluppo economico sostenibile** • **Claudio Moriconi** • **Paolo Antonio Fichera** • **Sandro Bologna** • **Antonio Palucci**
FEDERALIMENTARE Federazione Italiana dell'Industria Alimentare	**FEDERALIMENTARE** • **Daniele Rossi**
GILARDONI	**Gilardoni S.p.a.** • **Andrea Ascani Orsini**
intecs the Brainware Company	**INTECS Informatica e Tecnologie del Software S.p.a.** • **Cesare Dionisio** • **Paolo Coppola**

	**Kee Square** • **Stefano Tubaro**
	**Planetek Italia s.r.l.** • **Daniela Drimaco** • **Paolo Manunta**
	**“Sapienza” Università di Roma** • **Francesco Delli Priscoli** • **Donato Macone** • **Guido Oddi** • **Marco Castrucci** • **Francesco Saverio Romolo**
	**Selex Communications S.p.a.** • **Angeloluca Barba** • **Antonio Potenza** • **Fabrizio Vergari** • **Aldo Matricardi** • **Lorenzo De Benedictis**
	**Selex Galileo S.p.a.** • **Michele Genisio** • **Giovanni Cocca**
	**Selex Sistemi Integrati S.p.A.** • **Carlo Asperti** • **Daniele Cecchi** • **Stefano Pasquariello** • **Maurizio Calori** • **Agostino Longo** • **Paolo Proietti**
	**Semeion Centro Ricerche di Scienze della Comunicazione** • **Massimo Buscema** • **Guido Maurelli** • **Giulia Massini** • **Marco Intraligi** • **Massimiliano Capriotti**
	**Technoaware s.r.l** • **Simone De Titta**

	**Tecnoalimenti S.C.p.A.** • Raffaello Prugger • Ethel De Paoli • Marco De Vito
	**Telespazio S.p.A.** • Antonio Saitto • Paolo Bellofiore • Eusebi Borzelli Gianluca • Damiano Valletta • Alissa Ioannone • Antonella Catucci • Marco Grasso
	**Thales Group S.p.A.** • Rossano Marchesani • Ivan Baldi • Roberto Rossi • Antonio Toaiari
	**Thales Alenia Space Italia S.p.A.** • Mauro Leonardi • Giovanni Guarino • Corrado Farina • Daniele Frasca • Vincenzo Schena • Annamaria Nassisi • Massimo C. Comparini
	**Università CAMPUS BioMedico di Roma** • Roberto Setola • Marcella Trombetta
	**Università degli Studi di Genova Dipartimento di Ingegneria Biofisica ed Elettronica** • Carlo Regazzoni • Lorenzo Ciardelli

	Università degli Studi di Parma • **Nelson Marmiroli** • **Elena Maestri** • **Marta Marmiroli** • **Gianluigi Ferrari**
	Università di Cagliari Dipartimento di Ingegneria Elettrica ed Elettronica • **Luca Didaci** • **Gian Luca Marcialis** • **Fabio Roli**
Università degli Studi di Firenze Dipartimento di Elettronica e Telecomunicazioni DET	**Università di Firenze Dipartimento di Elettronica e Telecomunicazioni** • **Dino Giuli** • **Monica Gherardelli** • **Luca Facheris**
	Università di Salerno Dipartimento di Ingegneria Elettronica e Ingegneria Informatica (DIEII) • **Mario Vento** • **Gennaro Percannella** • **Pasquale Foggia** • **Donatello Conte**
UNIVERSITA' degli STUDI di ROMA TOR VERGATA *Facoltà di Ingegneria*	**Università di Tor Vergata** • **Angelo Spena** • **Franco Giannini**
VITROCISET	**Vitrociset S.p.a** • **Walter Matta** • **Antonio Romano**

Tassonomia STACCATO

I. Technologies-Components

100	**Structural materials and technologies and structural effects analysis**
100-1	Ceramics and glass technology
100-2	Ceramic composites
100-3	Composites materials technology
100-4	Powder metallurgy
100-5	Dense alloys
100-6	Organic composites
100-7	Metal metric composits
100-8	Carbone carbone composits
100-9	Polymeric materials
100-10	Synthetics fluids and lubricants
100-11	EM radiations absorbers
100-12	Magnetic metals
100-13	Superconductile conductors
100-14	New metallic alloys
100-15	Metallic composites
100-16	New concretes
100-17	Concretes resistant
100-18	Anti blast glasses
100-19	Materials for thermal control
100-20	Nano components and structures (tubes, ceramics, ...)
101	**Light and strong materials, surface treatments.**
101-1	Light materials for human protection
101-2	Light materials for site protection
101-3	Armor and anti-armor materials
101-4	Self-protective and explosive resistant material technology
101-5	Special fonction materials
101-6	Structural & Smart Materials
101-7	Surfaces treatments for improvement of mechanical properties
101-8	Surfaces treatments for improvement of life duration, corrosion reduction
101-9	Paints (without CoVs...)
101-10	Replacement of Cd, Hg, Cr
101-11	Simulation for surfaces treatment
101-12	Nano surfaces
101-13	Smart textiles
102	**Materials for deterrence**
102-1	Fissile materials enrichment
102-2	Nuclear materials processing
102-3	Nuclear-related materials
102-4	Fission reactor
102-5	Inertial confinement fusion (electrostatic, ...)
103	**Stealth materials and Technologies**
103-1	Radar passive absorbing materials
103-2	IR passive materials
103-3	Multifonctionnal stealth materials
103-4	Coatings and absorbing materials for laser signature reduction
103-5	Passive materials for acoustic reduction
103-6	Obscurants materials/equipments
104	**Survivability and hardening**
104-1	Underground nuclear weapons effects testing
104-2	Blast and shock effects
104-3	Structures vulnerability prediction after explosures and structural solutions
104-4	Thermal radiation effects
104-5	Transient radiation effects in electronics (TREE) and Systems-generated electromagnetic pulse (SGEMP) effects
104-6	Nuclear effects on electromagnetic signal propagation
104-7	High altitude electromagnetic pulse (HEMP) effects including dispersed EMP (DEMP)
104-8	Source region electromagnetic pulse (SREMP) effects
104-9	Pulsed-power driven nuclear weapons effects simulation sources
104-10	Hardening against natural environment lighting
104-11	EMC evaluation and hardening
104-12	Strong fields and MFP hardening
104-13	Damage reduction techniques
105	**Energetic materials**
105-1	Propellants
105-2	Conventional fuels and lubricants
105-3	Explosives
105-4	Pyrotechnics
105-5	(Micro-) pyrotechnology
106	**Plasma technology**
107	**Energy generation storage & distribution**
107-1	Electrical generators
107-2	Electrical batteries
107-3	Electrical fuel cells
107-4	Solar cells
107-5	RF power sources and devices
107-6	Acoustic power sources and devices
107-7	Other electric power sources and devices
107-8	Inertial / gravitational devices (flywheels, ...)
107-9	Other Energy storage & conditioning
107-10	Energy distribution
108	**Photonic/Optical Materials and Device Technology**
108-1	Optical surfaces.
108-2	Passive materials.
108-3	Active and adaptive optical systems (material, sensors, actuators,...).
108-4	Optical busses
108-5	Sights
108-6	Optical fibre material technology
109	**Opto-electronics: Laser, optics and related devices**
109-1	Lasers based power systems (lasers, optics, fibres, amplifiers, collimating, ...)
109-2	High density conventional systems
109-3	Pulsed and high power systems
109-4	Laser matter interaction
109-5	Short pulses laser propagation
109-6	Flame spectometry technologies
109-7	Laser induced fluorescence
109-8	Quantum Cascade Lasers
109-9	Blooming simulation for components and optronic subsystems
110	**Sensor Technology and Components**
110-1	Neutronic detection technologies (neutron tubes, ...)
110-2	X-ray technologies
110-3	Gamma technologies

110-4	Ion Mobility Spectrometry technologies
110-5	IR Spectroscopy
110-6	UV/Visible wave sensor technologies
110-7	UV VIS Spectroscopy
110-8	Terahertz technologies
110-9	Terahertz Spectroscopy
110-10	RFsensor technologies
110-11	Micro- and Millimeter Wave sensor technologies
110-12	Hyperspectral technologies
110-13	Multispectral technologies
110-14	Accoustic sensor technologies
110-15	Nanotechnologies for sensors
110-16	NAI detectors
110-17	BGO detectors
110-18	CZT detectors
110-19	Techniques for discrete surveillance
110-20	Sensor related imaging and mapping techniques
110-21	Microelectromechanical Systems (MEMS)
111	**Electronic components**
111-1	Silicon-based Materials
111-2	III-V Compounds
111-3	Other Semiconducting Matrials (AsGa, GaN, ...)
111-4	Insulating & Dielectric Materials
111-5	Carbon-based Materials
111-6	Superconductiong Materials
111-7	Magnetic Materials
111-8	Device Concepts and Fabrication
111-9	Device Packaging
111-10	Device Integration/Reliability
111-11	COTs assessment and obsolesence management
112	**Signal processing technologies**
112-1	Analog Signal Processing Technology
112-2	Digital signal processing technology
112-3	Analog/digital conversion technologies
112-4	High precision time measurament
113	**Information technologies**
113-1	Image / pattern processing technology
113-2	Pattern recognition
113-3	Data collection, data classification
113-4	Data and Information fusion technologies
113-5	Speech processing technology
113-6	Natural language processing technology
113-7	Data and information management technology (DB, ...)
113-8	Data analysis
113-9	Contextual search techniques
113-10	Jamming and anti-jamming technologies
113-11	Web intelligence
113-12	Text-mining / data-mining
113-13	Time synchronization
114	**Artificial Intelligence & Decision support**
114-1	IKBS/AI/Expert techniques
114-2	Neural network techniques
114-3	Mathematical modelling development
114-4	Optimisation and decision support technology
114-5	Modelling and simulation
114-6	Operational Analysis tools and techniques
114-7	Knowledge Management
114-8	War gaming techniques
114-9	Actionable intelligence
114-10	Decisionnal software
115	**Simulation tools and technologies**
115-1	Virtual and augmented reality
115-2	Synthetic environments
115-3	Synthetic environments - synthetic force generation
115-4	Synthetic environments - natural environment generation
115-5	Synthetic environments - management systems
115-6	Equipment simulation techniques
116	**Computing Technologies**
116-1	Software engineering
116-2	Protocol technology
116-3	COTS software assessment
116-4	SW Architectures
116-5	High integrity and safety critical computing
116-6	Secure computing techniques
116-7	Software verification and accreditation techniques
116-8	Hybrid computing
116-9	High performance computing
116-10	Grid computing
116-11	Software agents
117	**Information Security Technologies**
117-1	Content filtering
117-2	Cryptoanalysis
117-3	Cryptography algorithms (including quantum cryptography)
117-4	Cryptography implementation (including quantum cryptography)
117-5	Cyber attack technologies
117-6	Key management
117-7	Intention detection
117-8	Intrusion detection technologies
117-10	Integrity protection
117-11	Intrusion prevention technologies
117-12	IT Authentication technologies
117-13	OS hardening
117-14	Hardware protection technologies (tamper-evidence or tamper-protection)
117-15	Protocol Filtering
117-16	Retro engineering protection
117-17	Secure development
117-18	Secured communication protocols
117-19	Source code Static Analysis (Source code vulnerability analysis)
117-20	Virtual Private Nteworks (VPN) technologies
118	**Communication technologies**
118-1	Below microwave frequencies
118-2	Micro- and millimeter wave
118-3	Ultrawide band
118-4	IR / Visible / UV laser
118-6	Accoustic communication, including underwater.
118-7	Optical fibre
118-8	Cable technoligies
119	**Physiology Science & Medical technologies**
119-1	Medical products and materials

119-2	Surgical techniques and medical procedures
119-3	Human survivability, protection and stress effects
119-4	Human health physics
119-5	Neurosciences
119-6	Genome Engineering
119-7	Biomedical technologies
119-8	Rapid diagnosis of infectious disease
119-9	Telemedicine (diagnosis and surgery)
119-10	Novel antiviral, antibiotics, vaccines, and drug development
119-11	C & B knowledge and related data bases
120	**Human sciences, including researcha and studies**
120-1	Security / Military human resources management technologies
120-2	Human performance enhancement in crisis situations
120-6	Behavioural analyses
120-8	Psychology of workplaces and in emergency situations
120-10	Social analyses of teams and groups
120-13	Crisis Communication
120-14	Human behaviour models
120-25	Human factors in computers security
120-28	User friendliness technologies
120-29	Knowledge management
408B-3	R&D on user friendly technologies , Man-Machine-Interface
408B-4	Anthropometric studies for security systems
408B-5	Special Studies about the automation of human tasks in security related environment
121	**Biotechnology**
121-1	Biological technologies
121-2	Biomaterials and nanofabrication
121-3	Bio-compatible materials
121-4	Bio sensitive materials
121-5	Rapid analysis of biological agents and of human susceptibility to diseases and toxicants
121-6	Agro/food-biotechnologies
121-7	Contamination and intoxication of agriculture (water beddings, rivers, soil, air, ...)
121-8	Crop and animal viruses
121-9	Food testing and control techniques
121-10	Water testing and purification techniques
121-11	Decontamination techniques

II. Equipments and sub systems

200	**Sensor Equipments**
200-1	Non-acoustic sensors - UW
200-2	Cameras
200-3	Electrical and electro-chemical sensors
200-4	Explosive detection sensors
200-5	Magnetometers and magnetic gradiometers
200-6	Gravity meters and gravity gradiometers
200-7	Marine active sonar
200-8	Marine passive sonar
200-9	Acoustic and seismic sensors
200-10	Chemical and illicit substances detection
200-11	Biological substances detectors
200-12	Radiological and nuclear detectors
200-13	X-ray sensors
200-14	Gamma sensors
200-15	Active IR sensor equipments
200-16	Passive IR sensors equipments
200-17	Radar sensors equipments
200-18	SAR / ISAR equipment
200-19	Mm-wave sensors equipments
200-20	Micro-sensor systems for active control of structures
200-21	Motion sensor systems
200-22	LADARs, LIDARs equipments
200-23	Terahertz sensors
200-24	Magnetic sensors
200-25	Ultrasonic sensors
200-26	Autonomous small sensors
200-27	Smart dust technologies
200-28	Sensors on a chip
200-29	Sensors sitting
200-30	Mobile sensors networks info collection
201	**Signal Protection**
201-1	Effective defensive and offensive EW/IW techniques, measures and CM
201-2	Electronic protection
201-3	Optical counter measures: DIRCM
201-4	Optical counter measures: decoys and flares
201-5	Early detection techniques
201-6	Communication analysis
201-7	ELINT equipment
201-8	COMINT equipment
201-9	Radar active materials
201-10	IR active materials
201-11	Active materials (smart) for acoustic reduction
202	**Identification equipment**
202-1	IFF equipment
202-2	Non-co-operative IFF systems and techniques
202-3	Non-Co-operative Target Recognition equipment
203	**Biometric equipment**

203-1	Facial recognition
203-2	Fingerprints recognition (digital fingerprints)
203-3	Vein identification
203-4	Iris recognition
203-5	Hand shape recognition
203-6	Retinal patterns recognition
203-7	DNA analysis
203-8	Gait recognition
203-9	Voice recognition
203-10	Signature recognition
203-11	Ear shape recognition
204	**Chemical, Biological, Radiological and Nuclear (CBRN) protection and decontamination equipment**
204-1	Chemical agent defence, precursors and related materials
204-2	Biological agent defence, precursors and related materials
204-3	Mid-spectrum agent defence
204-4	chemical and biological defense systems
204-5	CB & RN Protection systems - Physical
204-6	CB Countermeasures - Medical
204-7	Biotechnology-based systems
204-8	Infrastructure and goods decontamination
205	**Navigation, guidance, control and tracking**
205-1	Inertial Navigation Systems (INS) and related components
205-2	Radio navigation, direction finding and map guidance
205-3	Vehicle and flight control equipment
205-4	Tracking equipment (electronic and mechanical seals)
205-5	Satellite navigation based receivers (miniaturization)
205-6	RFID based tracing device
205-7	Bar code based tracing device
205-8	Wi-fi based tracking device
205-9	Sense and avoid equipments
205-10	Unassisted landing systems
205-11	Digitisation of the environment/site
205-12	Geographic Information systems (GIS)
205-13	Environment/site information
206	**Directed energy systems technology**
206-1	Dazzle lasers against surveillance equipment (low power)
206-2	Deceive and dazzle lasers against missile seekers (low power)
206-3	Laser systems for sensor damage (medium power)
206-4	High energy laser (HEL), structural damage
206-5	High Power Microwave (HPM) (car stopping, antipersonnel, ...)
206-6	Particle beam (PB) systems
206-7	Supporting technologies for directed Energy Weapons
206-8	Low Power Electronic attack
207	**Munitions devices and energetic contents**
207-1	Gun propulsion
207-2	Mines, countermines, demolition systems, and EOD
207-3	Saving, arming, and futzing
207-4	Conventional munitions survivability
207-5	Ammunition hand and machine guns (small and medium calibre)
207-6	Ammunition large calibre guns
207-7	Kinetic energy (KE) subsystems
207-8	Weapons effects and countermeasures FTA
207-9	Induced shock waves from penetrating weapons
208	**Non lethal weapons**
208-1	Mechanical/kinetic anti-personnel
208-2	Mechanical/kinetic anti-materiel
208-3	Electromagnetic anti-personnel
208-4	Electromagnetic anti-materiel
208-5	Acoustical anti-personnel
208-6	Chemical anti-personnel
208-7	Chemical anti-materiel.
209	**Weapon systems (other than missiles and NLW)**
209-1	Small- and Medium-Calibre Weapons
209-2	Guns, Artillery, and Other Launch platforms
209-3	Torpedoes
210	**Explosives removal**
210-1	Explosive Ordnance Disposal
210-2	Explosives detection equipment
210-3	Mine detection and clearance
210-4	Counter Improvised Explosive Device equipment
210-5	Databases for IED components identification
210-6	High Power Microwave (HPM) for CIED (Counter Improvised Explosive Devise)
211	**Survivability and hardening equipment for persons**
211-1	Smart clothes and equipments
211-2	Exo Skeleton
211-3	Survivability of the embedded Personal Area Network
212	**Forensic technologies, others**
212-1	Drugs analysis
212-2	Fire arms and projectiles identification
212-3	Explosion investigations
212-4	Ballistics
213	**Buildings platforms**
213-1	Critical buildings specific architectures
214	**Marine equipments subsystems**
214-1	Propulsors and Propulsion Systems
214-2	Ocean salvage and deep sea implants
214-3	Signature Control and Survivability
214-4	Advanced Hull Forms
214-5	Human Systems Integration
214-6	Acoustic Sensors, Marine, Passive Sonar
214-7	Acoustic Sensors, Marine Platform
214-8	Electro-Optical Sensors for marine applications
214-9	Sea and Littoral Region Mine Countermeasures
214-10	Composite marine structures and substructures
215	**Space equipments subsystems**
215-1	Space Based Lasers
215-2	Structures for Space
215-3	Electronics and computers hardened for space environment

215-5	Propulsion for Space Systems
215-6	Space Systems sensors payloads
215-7	Space Avionics
215-8	Power and Thermal Management
215-9	Space Systems sensors payloads
215-10	Survivability in Space
215-11	Hot structures for launchers
215-12	Thermal protection
215-13	Integration and Qualification
215-14	Space Autonomy
216	**Ground equipments subsystems**
216-1	Human Systems Interfaces for Ground Systems
216-2	Hybrid-Electric Propulsion Systems
216-3	Sensors for Ground Systems
216-4	Vetronics
216-5	Advanced Diesel Engines
216-6	Land Mine Countermeasures
216-7	Defensive Aids Suites for vehicles
216-8	Structures for transport vehicles
216-9	Structures for tanks
216-10	Structures for other fighting land vehicles
216-11	Light armoured structures
216-12	Ground based robotic structures and subsystems
217	**Air equipments subsystems**
217-1	Advanced Air Data Systems
217-2	Energy-Management-Systems (EMSs)
217-3	Advanced External Vision
217-4	Health" Monitoring and Diagnostics
217-5	Radars
217-6	Optoelectronical sensors
217-7	Human Systems Integration
217-8	Signature Control and Survivability
217-9	Avionics subsystems
217-10	Defensive Aids Suites for air platforms
217-11	Aeronautical propulsion
217-12	Airframe
217-13	Helicopters structures
217-14	Helicopters mechanical parts
217-15	Man-machine interface
217-16	Flight Control System
217-17	UAVs structures and subsystems
218	**Missiles Equipments Subsystems**
218-1	Optoelectronical seekers
218-2	EM seekers
218-3	Hybrid seekers
218-4	Other navigation tools
218-5	Communication equipments
218-6	Divert altitude control systems
218-7	Ground or sea launchers for missiles
218-8	Retargeting
218-9	Warheads
218-10	Missiles structures
218-11	Subsonic propulsion of missiles
218-12	Supersonic combustion Ramjet (Scramjet) Propulsion
218-13	Kinetic Energy Missile (KEM) Propulsion
218-14	Terminal Guidance
218-15	Fuses
219	**Physical access control and Electronic Authentication Equipment**
219-1	Smart cards
219-2	Electronic tagging systems
219-3	Hardware tokens
219-4	Related biometric equipments
220	**Human Resources**
220-1	Computer adaptive testing (CAT) technology (for assessment of personnel and selection)
220-2	Facilities for Recruitment and selection of Personnel

IIIA. Systems-Services Functions

300A	**Risks assessment, modelling and impact reduction**
301A	**Risks and vulnerabilities assessment**
302A	**Risk reduction**
303A	**Protection**
303A-1	Civil first responders protection
303A-2	Armed forces protections
303A-3	Population protection
303A-4	Doctrine and operation
303A-5	Training and exercises
304A	**Exercise and simulation, training**
304A-1	Detection, identification and authentication
305A	**Search and detection**
306A	**Identification**
306A-1	Identity management
306A-2	Positioning and localization
307A	**Localization**
307A-1	Situation awareness & assessment (surveillance)
308A	**Surveillance**
308A-1	Environmental monitoring systems
309A	**Intelligence**
309A-1	Information management
309A-2	Intervention and Neutralization
310A	**Neutralization**
310A-1	Communication
311A	**Interoperable secured communications (Security systems architecture**
311A1	Command and Control
312A	**Crisis Operations / Management – C3I**
312A-1	Population warning systems
312A-2	Optimisation, Planning & Decision Support systems
312A-3	Infrastructure to Support Information Management & Dissemination
312A-4	Incident Response
313A	**Search and Rescue and evacuation**
314A	**Decontamination and de-pollution**
315A	**Personnel outfit systems**
315A-1	Subsurface systems
315A-2	Ground systems technology
315A-3	Air systems technology
316A	**Psychological and Social aspects**

IIIB. Design-Manufacturing

300B	**Operating Environment Knowledge & Modelling Technology**
300B-1	Oceanography
300B-2	Terrain science
300B-3	Meteorology
300B-4	Upper atmosphere and space environment
300B-5	lower atmosphere environment
300B-6	Acoustic propagation in air and water
300B-7	Electromagnetic propagation in air and water
300B-8	Pollutants and chemical propagation in atmosphere
300B-9	Chaos theories
301B	**Systems Engineering and Design Management**
301B-1	Interoperability
301B-2	COTS/MOTS/GOTS system based integration
301B-3	Safety Verification
301B-4	Cost Engineering
301B-5	Concurrent Engineering and Reduced Design Cycle
301B-6	Project Management and Control
301B-7	Reliability and maintainability of systems
301B-8	Integrated systems testing & evaluation
302B	**Systems Certification and Failure Investigation**
302B-1	Systems certification
302B-2	Failure Investigation
303B	**Systems Engineering and Integrated Systems Design**
303B-1	Aerodynamics
303B-2	Hydrodynamics
303B-3	Aeronautical Design and Systems Integration
303B-4	Radiation and EMV Hardening
303B-5	Robotics / automation in operational systems
303B-6	Security metrics
303B-7	System repair technology
303B-8	Electro-magnetic compatibility
303B-9	Digital power
303B-10	In-service data capture systems
303B-11	Fault tolerance and reconfiguration system
303B-12	Structural Vulnerability of systems
303B-13	Power management of systems
303B-14	Man Machine Interface / Man System Interface
303B-15	Design for Improved Reliability & Maintainability
303B-16	Advanced Prototyping
303B-17	Knowledge-based Engineering
303B-18	Health monitoring systems
303B-19	Signature Control for Ground Systems
303B-20	Acoustic design
303B-21	Stealth design
303B-23	Buildings design
304B	**Manufacturing and fabrication technology**
304B-1	Automation of industrial processes
304B-2	Metal working and industrial production

304B-3	Advanced fabrication and processing
304B-4	Bearing
304B-5	Metrology
304B-6	Non-destructive inspection and evaluation
304B-7	Techniques and Systems for Production Manufacturing
304B-8	Lean Manufacturing
304B-9	Process Control Technology
304B-10	Environmentally Friendly Factory Processes
304B-11	Production equipment
304B-12	Robotics
304B-13	Optical coating
304B-14	Dimensional metrology
304B-15	Precision bearings
304B-16	Micromechanical devices
304B-17	Mechanical, Thermal and Fluid-Related
305B	**Software design validation and maintenance**
305B-1	Software quality insurance
305B-2	Integrated Development Environment (IDE)
305B-3	Computer-aided software engineering (CASE)
305B-4	secure software engineering
305B-5	Design Pattern
305B-6	Agile software development
305B-7	Model Driven Software Development
305B-8	Component-Based Software Development
305B-9	Version Control System
305B-10	Code reuse
305B-11	Debugging tool
305B-12	Software testing processes and tools
306B	**Simulation and design tools**
306B-1	Sensor simulation
306B-2	Network centric simulation
306B-3	Hardware-in-the-loop-testing
306B-4	Manufacturing Process Simulation
306B-5	Computer aided design
306B-6	Computer aided manufacturing
306B-7	Vehicle Design and Synthesis Tools
306B-8	Digital vehicle
306B-9	Virtual reality centre (digital makeup of an architecture network, ...)
307B	**Installations and Facilities**
307B-1	Ground stations
307B-2	Site engineering
307B-3	Site sanitizing
307B-4	Wind tunnels
307B-5	Hydrodynamic test facilities
308B	**Ergonomic and Human factors**
308B-1	Methods, tools and processes to support the integration of people in security systems
308B-2	Analysis of user needs and user requirements for security systems
308B-3	Ergonomic Displays and Presentations.
308B-4	Human factors in error-tolerant systems

IV. Integrated platforms and systems and HFs

400	**Marine platforms**
400-1	Combat sea surface platforms
400-2	Logistic and support sea surface platforms
400-3	Unmanned surface vessels
400-4	Manned Submarines and deep submergence vessels
400-5	Unmanned Subsurface and deep submergence vessels
400-6	Mini and micro marine platforms
401	**Space platforms**
401-1	Communication satellites
401-2	Navigation satellites
401-3	Earth surveillance satellites
401-4	Meteo satellites
401-5	Manned space platforms
401-6	Unmanned scientific space platforms
402	**Ground platforms**
402-1	Ambulances
402-2	Fire engines
402-3	Tanks and armoured fighting vehicles
402-4	Transport vehicles
402-5	C2 and surveillance-vehicles
402-6	Others
402-7	Systems Integration for Ground Systems
402-8	Ground platforms survivability
402-9	Unmanned ground vehicles
403	**Air platforms**
403-1	Combat aircraft
403-2	Transport aircraft
403-3	Surveillance/C2 aircraft
403-4	Combat helicopters
403-5	Transport helicopters
403-6	Unmanned aerial vehicles
403-7	Lighter-than-air platforms
404	**Missiles platforms**
404-1	Missiles for space applications
404-2	Ballistic surface-to-surface missiles
404-3	Surface-to-surface missiles
404-4	Surface-to-air missiles
404-5	Air-to-surface missiles
404-6	Air-to-air missiles
405	**Simulators, Trainers**
405-1	Skills training systems
405-2	Tactical / crew training systems
405-3	Command and staff training systems
406	**Deterrence systems**
407	**Identity management systems**
407-1	biometrics solutions

407-2	token management
407-3	secure database management
408	**Integrated Surveillance Systems**
408-1	Forest / network of sensors
408-2	Wide-scale long-range multi-sensor surveillance
408-3	Site sensors networks
409	**Stealth management : Signature Control and Signature Reduction**
409-1	Radar signatures
409-2	Micro- and Millimetre wave radar signatures
409-3	Laser signatures
409-4	IR signatures
409-5	Visible/UV signatures
409-6	Acoustic signatures
409-7	Electrical and electrochemical signatures
409-8	Magnetic signatures
409-9	Theory theoretical models technique
409-10	Signature reduction
409-11	Signature control and survivability
410	**Stealth Technologies**
410-1	low signature apertures
410-2	Conception of stealthy airframes, ships and vehicles
410-3	Stealth management
411	**C2, Information and intelligence systems**
411-1	Intelligence integration (linking surveillance systems with databases)
411-2	Communication Command Control Information systems
411-3	Intelligence systems
411-4	Information exchanges and interoperable databases
411-5	Optimisation, Planning & Decision Support systems
411-6	Infrastructure to Support Information Management & Dissemination
412	**Networks and information security systems**
412-1	Cyber security policy management tools
412-2	Cyber attack systems
412-3	Cyber protection systems and architectures
412-4	Network security and data integrity between distributed sensors
413	**Communication Systems**
413-1	Rapidly Deployable Communication Infrastructure
413-2	Mobile Communications Infrastructure
413-3	Rescue Services Mobile Communication Systems
413-4	Secure Mobile Communication Systems
413-5	Self configuring Networks
413-6	Secured, wireless broadband systems
414	**HFs Services to Security**
414-1	Human Factors Integration (a.k.a. Human system integration, Human Factors engineering) into the design of systems
414-2	Human Factors in Threat Analysis
414-3	Human Error Analysis (a.k.a soft risk analysis)
414-4	Performance and behaviour improvement on the job of security personnel.
414-5	Human Factors aspects of site protection and access control
414-6	Human Factors aspects in background security checks
414-7	Contribution to crisis management including Lessons Learnt.
414-8	Psycho-social treatment of victims.
415	**Equipped Personnel**
415-1	Equipped soldier ('soldier system')
415-2	Equipped fire fighter
415-3	Equipped medics
415-4	Health and well-being monitoring systems
416	**Integrated systems of systems**
416-1	simulation and representation of complexity
416-2	Broadband access to mobile users in dynamic situations / EM difficult scenarios
416-3	Communications systems - below microwave frequencies
416-4	Communications systems - micro- and millimeter wave
416-5	Communications systems - IR / Visible / UV laser
416-6	Communications systems - Acoustic
416-7	Communications systems - Underwater acoustic
416-8	Communications & CIS Security systems
416-9	Communications switching: in level II communication subsystems, with antennas, front end, etc...
416-10	Communications network management and control
416-11	Command & Information Systems Integration
416-12	Information security
416-13	Network and protocol independent secured communications
416-14	Multi-mode secured communications
416-15	Re-configurable communications
416-16	Mobile secured communications
416-17	Protection of communication networks against harsh environment

VA. Mission Capabilities

500A	**Preserve the functionning of the State**
500A-1	Safeguard secured liaisons
500A-2	Protection of Installations and buildings of vital importance
500A-3	Protection of Authorities
501A	**Ensure Identification and control of goods and people**
501A-1	Ensure management and control of identities and rights
501A-2	Control and track cross border goods and materials
501A-3	Control and track cross border information
502A	**Ensure and Maintaining Law and Order**
502A-1	Fight against trafficking
502A-2	Fight against criminality
502A-3	Fight against delinquency and insecurity
502A-4	Manage intervention and neutralisation
502A-5	Manage judicial police operations
503A	**Ensure Economic Security**
503A-1	Ensure Intelligence (economic intelligence)
503A-2	Use appropriate instruments
503A-3	Ensure continuity of economic activity
504A	**Protection of citizens (goods and people)**
504A-1	Protect each individual citizen (included protecting fo material and immaterial goods)
504A-2	Secure public area
504A-3	Rescue of people (see rescue,...)
504A-4	Control of environment
504A-5	Secure food chain and wealth products
504A-6	Ensure collective protection (included secure public area)
505A	**Avert and foreseen Catastrophes**
505A-1	Decrease technological and industrial risks
505A-2	Surveillance of environment in order to alert
505A-3	Ensure Epidemiological Surveillance
505A-4	Surveillance of zones under humanitarian risk (migratory flow, drought,...)
506A	**Avert and prepare themselves against aggression**
506A-1	Manage intelligence and surveillance actions
506A-2	Evaluation of treats and vulnerabilities
506A-3	Reduction of criminology qualities
506A-4	Take protection measures (proactive and reactive ones)
506A-5	Manage preventative operations
506A-6	Surveillance of environment (control, detection CBRN, abnormal behaviours,...)
506A-7	Ensure Communication and alerts
507A	**Control and surveillance of areas**
507A-1	Air surveillance
507A-2	Maritime surrounding areas surveillance
507A-3	Costs and boundaries surveillance
507A-4	Surveillance of information flows and illegal content
507A-5	Detection and neutralisation of non authorised people or mobiles (before crisis)

508A	**Protection of areas and infrastructures**
508A-1	Protection of partially opened sites (ports, airports, hospitals,...)
508A-2	Protection of closed areas (sensitive installations)
508A-3	Protection of open areas (shopping centres,...)
508A-4	Protection of sites where events take place (G8, concerts in open areas,...)
509A	**Protection of networks**
509A-1	Transport systems
509A-2	Water and power distribution
509A-3	Communication network
509A-4	Information systems
509A-5	Bank Systems
510A	**Protection of environment (before, during and after)**
510A-1	Fight against pollution
510A-2	Fight against treats to the Environment
510A-3	Monitor the respect of agreements
511A	**Security of transport**
511A-1	Transport of dangerous materials
511A-2	Surveillance of traffic areas
511A-3	Ensure the continuity of flows
511A-4	Restore security of flows
512A	**Crisis management**
512A-1	Crisis management operations
512A-2	Manage and lead complex operations
512A-3	Rescue of people
512A-4	Protection of order and rescue forces
512A-5	Protection of chain of evidence
513A	**Ensure restoration and reparation**
514A	**Security of nationals abroad**
514A-1	Protection of traffic areas
514A-2	Collection of local data
514A-3	Lead evacuation operations
515A	**Lead operation for external security**
515A-1	Humanitarian Operations
515A-2	Evacuation Operations
515A-3	Conflict prevention/Peace keeping
516A	**Control of disarmament/ fight against proliferation**
516A-1	Ensure intelligence
516A-2	Area Surveillance
516A-3	Control and track of flows, substances and materials

VB. Policy and Support

500B	Security Analysis
500-1	Policy, force development and balance of investment studies
500-2	Combined operational effectiveness and investment appraisals
500-3	Platform and system concept studies
500-4	Scenario generation
500-5	Other effectiveness and performance studies
500-6	Political & Cultural, ethical and religious analysis
500-7	Crisis management and Conflict Simulation
500-8	Legal & Ethical constraints
500-9	Multinational and Inter-organisation analysis and planning and operation
501B	**Miscellaneous Security Functions and Policy**
501B-1	International Security & Counter Insurgency
501B-2	Non-proliferation
501B-3	Hazard assessment
501B-4	Distribution Logistics (e.g. maintaining distribution logistics in cases of severe crises)
502B	**Human resources (HR) management for security personnel**
502B-1	Recruitment of personnel
502B-2	Selection of personnel (e. g. Baggage and cargo screener selection)
502B-3	Licensing and Certification
502B-4	Working practices, procedures and rules of engagement
502B-5	Staff management and working practices
502B-7	Team (Crew) Resource Management
502B-9	Knowledge management applied to Security issues
503B	**Training**
503B-1	Operator training
503B-2	Population training
503B-3	Leadership/managers training
503B-4	Training Centres/facilities, e.g. airport training centres
503B-5	Training Development and evaluation
503B-6	Event specific training, e.g. hostage taking hijacking, mine-awareness.
503B-7	Job and task specific training, e.g. Baggage and Cargo screener training .
503B-8	Media training
504B	**Scenario and decision simulation**
504B-1	Human behaviour modelling and simulation
504B-2	Simulation for decision making (real time simulation)
504B-3	Mission simulation
504B-4	Evacuation and consequence management techniques
504B-5	Impact analysis concepts and impact reduction
504B-6	Structures vulnerability prediction
504B-7	Space Operations monitoring
504B-8	Quick Launch
504B-9	Single-Stage-To-Orbit (SSTO) Reusable Launch Vehicle (RLV)
504B-10	Launch Vehicles for Space Systems
505B	**Long term health hazard prevention in security related situations**
505B-1	System safety of security systems
505B-2	Fatigue and stress observation, analysis and coping
505B-3	Occupational health services for security personnel (methods, facilities, evaluation)
505B-4	Plans and concepts for disaster medicine and relevant health services

Note

Note

CONSIGLIO NAZIONALE DELLE RICERCHE

FINMECCANICA

Note

Note

CONSIGLIO NAZIONALE DELLE RICERCHE

FINMECCANICA

Note

Finito di stampare nel mese di Marzo 2011
dalla Tipolitografia Grifo - Perugia