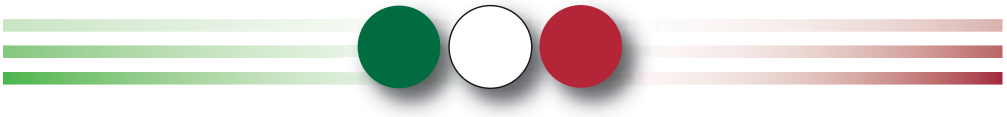


Security Research in Italy 2012

volume n. 2

Il vol. 2 di SEcurity Research in ITaly è stato parzialmente finanziato dal progetto:

Prefazione

L'evolversi del complesso scenario relativo ai diversi aspetti di Sicurezza si riflette nell'attenzione e nell'interesse che una platea sempre più vasta di rappresentanti del mondo accademico ed industriale rivolge verso la Piattaforma **SERIT (SEcurity Research in ITaly),** che vede ad oggi coinvolte oltre 250 organizzazioni e un numero sempre più elevato di esperti che partecipano nelle attività.

Nello scorso 2011, la piattaforma SERIT è stata formalmente riconosciuta dal Ministero dell'Istruzione, dell'Università e della Ricerca (MIUR) come la Piattaforma Tecnologica Italiana che si occupa dei temi legati alla Security sul territorio nazionale, e pertanto investita ufficialmente del ruolo di aggregatore di competenze, in risposta ai mutevoli bisogni di Sicurezza del paese, nonché di facilitatore per la messa a punto di nuove strategie, al fine di conseguire lo sviluppo tecnologico necessario a livello di sistema paese nei temi di interesse.

La piattaforma svolge inoltre un ruolo essenziale di catalizzatore per lo sviluppo tecnologico in materia di Security, che si estende anche oltre il confine nazionale, promuovendo la partecipazione congiunta dei membri ai bandi di ricerca Europei (*7° Framework Programme*), con lo scopo di reperire finanziamenti utili e indispensabili a perseguire gli obiettivi della ricerca.

In linea con gli obiettivi e i futuri temi Europei, la piattaforma si è inoltre dotata di una struttura maggiormente afferente alle tematiche lanciate dall' Europa per il prossimo programma quadro, Horizon 2020 (per il periodo 2014-2020), proponendo sia una nuova mappatura e un' opportuna aggregazione dei settori guida, sia una definizione di nuove aree tecnologiche conformi con quelli che sono i principali *drivers* europei, senza però perdere la declinazione originale nei domini applicativi che rispecchino le esigenze nazionali in termini di della sicurezza.

Lo scopo di questa pubblicazione infine è quello di descrivere e condividere la *roadmap* concepita dagli stakeholder e dagli esperti che hanno rilevato e descritto lo stato dell'arte del settore nel Paese e hanno definito, in primo luogo, le priorità in termini di capacità tecnologiche da sviluppare, e successivamente quantificato l'impegno necessario e gli investimenti indispensabili per implementare tali attività di ricerca.

La piattaforma SERIT si propone come strumento per supportare la pianificazione nazionale delle attività di ricerca in ambito sicurezza.

Un sentito ringraziamento a tutti coloro che hanno lavorato per rendere possibile questo importante passo in avanti per raggiungere l'eccellenza tecnologica in materia di Sicurezza del nostro paese.

Cristina Leone e Fabio Martinelli

Sommario

Introduzione

La Piattaforma SERIT si è data la missione di sviluppare un' agenda di ricerca e innovazione in ambito sicurezza per l'Italia: una roadmap strategica per la ricerca sulla sicurezza.
In particolare SERIT si propone di:

- Studiare le prospettive nazionali di sicurezza a medio termine e a lungo termine confrontandosi con gli scenari europei e mondiali
- Avvicinare la domanda e l'offerta, concentrarsi sui requisiti per la ricerca,
- Analizzare gli aspetti sociali e tecnologici della ricerca sulla sicurezza,
- Promuovere l'innovazione

I membri di SERIT si incontrano più volte all'anno per discutere le linee guida del lavoro ed analizzare i risultati. Il lavoro dettagliato è effettuata dai gruppi di lavoro (**Settori Guida - SG e Aree Tecnologiche - TA**). Essi operano in parallelo sotto la guida dei coordinatori dei gruppi, che ne assicurano la coerenza di approccio e nei risultati.
La Piattaforma SERIT è strutturata in maniera matriciale, dove i Settori Guida rappresentano le missioni prioritarie del Paese e le Aree tecnologiche descrivono le capacità chiave e le tecnologie da sviluppare, in particolare potremmo elencare:

- ***TA 1 - Sorveglianza & Situation Awareness;***
- ***TA2 - Comunicazioni;***
- ***TA3 - Detection & Identification Systems;***
- ***TA4 - Tecnologie per Crisis Management e per la Protezione di Persone, Asset e Infrastrutture;***
- ***TA5 - Information Processing and Management;***
- ***TA6 - CBRNE.***

1. Ristrutturazione dei Settori Guida

L'approccio di SERIT ha permesso di identificare in maniera puntuale un gran numero di settori, che data la trasversalità delle applicazioni, si è ritenuto opportuno di classificare in 7 Settori Guida, a loro volta articolati in sottosettori:

- ***Sicurezza dei trasporti;***
- ***Sicurezza del sistema energetico;***
- ***Sicurezza dei confini;***
- ***Cyber security;***
- ***Sicurezza agroalimentare;***
- ***Sicurezza e Salute;***
- ***Sicurezza integrata nei beni culturali e nel costruito.***

Il confronto con le priorità di *Horizon 2020*, mette in evidenza le similarità con il prossimo Programma Europeo di ricerca ed innovazione e le specificità del sistema Italia.
Le priorità in *Horizon 2020* sono di seguito riportate:

- **Lotta contro la criminalità e il terrorismo**, le cui capacità vengono analizzate da SERIT all'interno dei Settori Guida Sicurezza dei trasporti, Sicurezza del sistema energetico, Sicurezza agroalimentare e Sicurezza e Salute
- **Potenziare la sicurezza mediante la gestione delle frontiere**, che coincide con il Settore Guida Sicurezza dei confini
- **Garantire la sicurezza informatica**, che corrisponde al Settore Guida Cyber security
- **Migliorare la capacità di reazione dell'Europa di fronte alle crisi e alle calamità**, che SERIT copre nell'Area Tecnologica "Tecnologie per Crisis Management e per la protezione di persone, asset e infrastrutture"
- **Garantire la tutela della vita privata e della libertà su Internet e rafforzare la dimensione sociale della sicurezza**, trattata nell'Area Tecnologica: Aspetti etici e legali per la Sicurezza
- **Il Settore guida "Sicurezza integrata nei beni culturali e nel costruito"** è una specificità di ricerca italiana che si ritiene di mantenere invariato in quanto priorità nazionale.

1.1 Sicurezza dei Trasporti

La protezione dei sistemi di trasporto nazionali assicura libertà di movimento alle persone ed alle merci e crea, pertanto, un ambiente in grado di sostenere lo sviluppo dei commerci e, più in generale, l'economia del Paese.
L'adozione di misure che prevengono o rilevano l'ingresso, la presenza e gli spostamenti di persone, merci e mezzi non autorizzati e quelle che evidenziano loro comportamenti atipici consente una diminuzione dei rischi che incidono su un elemento determinante della catena del valore quale la logistica.
La sicurezza del trasporto su rotaia, su strada e via mare e la possibilità di operare spostamenti che combinino diverse modalità di trasporto (multi modalità / intermodalità), richiedono lo sviluppo di strumenti tali da consentire sia una visione di insieme dell'intero settore del trasporto sia una visione di dettaglio della modalità stessa.
Il Settore Guida Sicurezza dei Trasporti riunisce i sottosettori Sicurezza Ferroviaria, Sicurezza Trasporto Multimodale, Sicurezza Trasporto su Strada, Sicurezza Marittima, con l'intento di raccogliere le esigenze comuni e di far emergere quelle peculiarità che, confinate in ambiti specializzati, rischierebbe di non poter essere percepite. Nel seguito verranno illustrati più nel dettaglio i seguenti sottosettori guida:

- Sicurezza Ferroviaria;
- Sicurezza Trasporto Multimodale;
- Sicurezza Trasporto su Strada;
- Sicurezza Marittima;

1.1.1 Sottosettore guida: Sicurezza Ferroviaria

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.

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.

1.1.2 Sottosettore guida: Trasporto Multimodale

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 lo sviluppo di 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 di merci e persone.
Le sottotematiche di ricerca che richiedono maggiori attenzione sono:

- Sviluppo di sistemi innovativi, elettronici, fisici e ICT per aumentare l'affidabilità e la cooperazione dei sistemi di trasporto multimodale;
- Trasporto multimodale merci, incluse le merci pericolose;
- Sensori anti-Intrusione e per la tracciabilità dei container;
- Raccolta dati del trasporto merci/persone per centro operativo integrato.

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.

Raccolta dati del trasporto merci/persone per centro operativo integrato

La disponibilità e la combinazione di dati provenienti dai sistemi informativi che governano la mobilità di merci e persone in ambito urbano ed extraurbano consentono lo sviluppo di altri servizi/ applicazioni a supporto degli enti che governano la sicurezza, la gestione di grandi eventi e calamità naturali. La raccolta di informazioni relative ai piani di trasporto nel contesto urbano di merci e persone offre la potenzialità di predisporre il territorio all'accoglienza, alla gestione e all'eventuale dirottamento di tali flussi oltre a rendere disponibili strumenti che analizzando dati (e relative informazioni) disponibili potranno favorire ulteriori sviluppi quali ad esempio le investigazioni per prevenire o bloccare atti criminosi o scambi commerciali illeciti.

1.1.3 Sottosettore guida: Trasporto su Strada

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.

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 al trasporto su strada, riducendo i rischi di potenziali scenari sensibili e le conseguenti situazioni di emergenza;
- garantire mezzi per un intervento tempestivo ed efficace 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 settore riguarda trasversalmente diversi domini di applicazione in ambito sicurezza e protezione civile, per la prevenzione di attacchi terroristici e/o la mitigazione e gestione di eventuali situazioni di 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 degli 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 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.

1.1.4 Sottosettore guida: Trasporto Marittimo

Il miglioramento della sicurezza nel Trasporto Marittimo richiede interventi riguardanti l'insieme delle misure atte a monitorare il traffico navale, a tracciare quello delle merci e idonee e a controllare il trasporto passeggeri.
Soluzioni innovative finalizzate a salvaguardare la vita umana in mare, a tutelare l'ambiente marino e costiero nonché a prevenire azioni illecite contro navi ed infrastrutture portuali, potranno garantire la sicurezza della navigazione e, al tempo stesso, il miglioramento della gestione delle linee di traffico.
Queste azioni hanno lo scopo di rendere più efficienti le cosiddette "autostrade del mare", ovvero quei canali di trasporto che, per la quantità dei volumi movimentati, assumono un valore strategico nazionale.
Per il conseguimento di questi obiettivi occorre, tra l'altro, sviluppare e potenziare le capacità di monitoraggio delle navi (sistema VTMIS – Vessel Traffic Monitoring/Management Information Sistem), di tracciamento delle merci della filiera marittima, e infine di interoperabilità funzionale dei 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:

- il supporto alla multimodalità, nell'accezione di integrabilità con nodi intermodali esistenti;
- l'adozione di metodologie e soluzioni architetturali orientate ai servizi;
- il monitoraggio del traffico marittimo;
- la rilevazione di situazioni di rischio e la tempestiva comunicazione di allarmi tra gli operatori

(centri di controllo di terra, operatori di bordo e operatori marittimi);

In questo contesto assumono particolare rilievo gli sviluppi connessi ad un monitoraggio marittimo che abbia come obiettivo principale la determinazione della presenza, nelle aree di interesse, di unità non cooperative.

Gli obiettivi della ricerca, riassumibili nel miglioramento delle capacità di rilevamento e di cooperazione e collaborazione tra sistemi, tra amministrazioni e tra Stati, conducono all'individuazioni delle seguenti sottotematiche:

- Elaborazione dei dati;
- Sensori per la rilevazione dei dati;
- Automazione di procedure;
- Sistemi per la cooperazione.

Sottotematica Elaborazione dei dati

La sicurezza non può prescindere dalla sorveglianza, e quest'ultima non può essere condotta che attraverso la valutazione di informazioni e dell'analisi dei dati disponibili. In particolare, i sistemi di elaborazione dei dati potranno offrire strumenti di fusione dei dati ed innovare le modalità di presentazione dell'informazione. In quest'ultimo ambito assumono un'applicazione pratica diretta tutte quelle innovazioni che arricchiscono la rappresentazione mediante cartografia elettronica, incrementando notevolmente il numero di informazioni accessibili.

Sottotematica Sensori per la rilevazione dei dati

Le informazioni disponibili e quelle emergenti dall'analisi dei dati, possono beneficiare di ogni tipo di sviluppo in grado di aumentare la quantità e la qualità dei dati raccolti e delle stesse informazioni disponibili. Il miglioramento atteso riguarda la realizzazione di sensoristica con più elevato potere risolutivo e l'adozione di soluzioni in grado di ampliare le aree osservate.

Sottotematica Automazione di procedure

Lo sviluppo di capacità operative semi-automatiche sarà abilitante nell'innovare aspetti procedurali e tecnici che, a loro volta, necessitano di un continuo adeguamento alla crescente mole di dati ed informazioni a diposizione degli attori del settore. L'automatizzazione consentirà di completare la catena dato - informazione - conoscenza e di conseguire una Maritime Domain Awareness.

Sottotematica Sistemi per la cooperazione

L'incremento dell'interoperabilità tra le diverse piattaforme adibite al controllo del traffico marittimo dovrà rendere disponibili quei strumenti di scambio di informazioni utili per :

- consentire la collaborazione tra sistemi
- agevolare la cooperazione tra amministrazioni nazionali
- garantire la cooperazione transazionale e la continuità delle operazioni
- condividere informazioni al fine di elaborare uno scenario utile ed efficace per la gestione congiunta delle emergenze.

1.2 Sicurezza Infrastrutture Energetiche

Le Infrastrutture Energetiche, nelle sue componenti di sistema elettrico, sistema olio e sistema gas, hanno l'obiettivo di assicurare alla nazione uno sviluppo sostenibile in un mercato competitivo globale. L'indisponibilità di parti importanti delle Infrastrutture Energetiche nazionali 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 (produzione e distribuzione) è divenuto sempre più complesso, e di conseguenza vulnerabile a diversi tipi di minacce, dagli atti di terrorismo deliberati ai disastri naturali. In aggiunta, la penetrazione sempre più forte delle tecnologie ICT, necessarie alla gestione del Sistema in un'ottica di *Smart Grid*, rende il sistema stesso sempre più vulnerabile alle nuove minacce informatiche. È dunque importante garantire lo sviluppo di tecnologie ICT adeguate a garantire la flessibilità, la sicurezza del Sistema e/o di parti di esso, nonché la resilienza, intesa come la capacità del Sistema elettrico di continuare a fornire il servizio atteso anche in presenza di eventi avversi multipli.
Il servizio di trasporto nazionale del gas viene effettuato grazie a una complessa infrastruttura formata da circa 32.000 chilometri di metanodotti, tubazioni di grande diametro con funzione di trasferire grandi quantità di gas dai punti d'ingresso del sistema ai punti di interconnessione con le reti di trasporto regionali e con le strutture di stoccaggio, un centro di Dispacciamento e 11 centrali di compressione. Un possibile punto d'ingresso del sistema gas è il rigassificatore**,** un impianto industriale estremamente complesso e classificato a elevato rischio, in grado di trasformare il gas naturale dallo stato liquido allo stato gassoso. L'installazione di un rigassificatore comporta di norma elevati requisiti di *security*.
Il sistema dei "Porto Petroli" per lo sbarco, l'imbarco e il trasferimento di petroli greggio, prodotti petroliferi e petrolchimici dalle navi trasporto alle raffinerie e gli impianti di stoccaggio dei prodotti petroliferi è composto da molteplici Infrastrutture Energetiche con elevati requisiti di *security*, trattandosi di impianti soggetti ad un sistema di gestione della sicurezza conforme alla Seveso Bis.
Le Infrastrutture per il trattamento di rifiuti radioattivi sono al momento le sole Infrastrutture di interesse nazionali per quanto riguarda la *nuclear security*.
Nel caso di un deposito di rifiuti radioattivi, il rischio maggiormente ipotizzabile è il sabotaggio con conseguente dispersione di materiale nucleare e altro materiale radioattivo.
La protezione fisica del materiale si basa sull'integrità delle barriere, sia del deposito sia dei contenitori dei rifiuti. La minaccia all'integrità delle barriere è variegata e va dall'attacco terroristico (interno o esterno), ai disastri provocati dall'uomo (es. aerei) o naturali.
Il massimo sforzo dovrà essere rivolto ad individuare metodi per prevenire, o almeno rilevare tempestivamente, possibili indebolimenti delle barriere. Un monitoraggio continuo per una tempestiva diagnosi si presenta come un metodo efficace sia per evidenziare eventuali incidenti o sabotaggi sia per ridurne le conseguenze.
Molte delle Infrastrutture Energetiche sono inoltre soggette al Decreto Legislativo 11 Aprile 2011, n.61, di adozione da parte dell'Italia delle "*Direttiva Europea relativa all'individuazione e alla designazione delle infrastrutture critiche europee e alla valutazione della necessità di migliorarne la protezione*".
Alla luce di quanto sopra menzionato, il Sistema delle Infrastrutture Energetiche nazionali necessita di una molteplicità di strumenti concettuali e tecnologici atti a sostenere un approccio globale alla *security*.
A tale scopo, il Settore Guida "Sicurezza Infrastrutture Energetiche" necessita di:

- sviluppare metodologie per la predisposizione di piani per sistemi di sicurezza integrata e lo sviluppo di soluzioni tecnologiche per la protezione fisica e logica di tutti gli *asset* delle Infrastrutture Energetiche nazionali;
- sviluppare metodologie e piattaforme di simulazione per studiare la complessità delle interazioni e le vulnerabilità dovute alle interdipendenze tra diverse Infrastrutture Energetiche;
- sviluppare metodologie e soluzioni tecnologiche per un miglior monitoraggio della sicurezza fisica e logica delle diverse Infrastrutture Energetiche, anche allo scopo di prevenire gli effetti di caduta a cascata;
- sviluppare metodologie e soluzioni tecnologiche per affrontare il problema della *cyber security* delle Smart Grid.

Sistemi di sicurezza integrata per la protezione degli asset delle Infrastrutture Energetiche

È necessario perseguire lo sviluppo e la predisposizione di adeguati piani di sicurezza integrata, comprendenti la sicurezza fisica, logica e procedurale, per tutti gli *asset* delle diverse Infrastrutture Energetiche e con particolare riferimento alle centrali di produzione di energia, al fine di garantire la continuità di esercizio. Il tutto si attua in una visione di crescente penetrazione delle tecnologie ICT nei sistemi di controllo e gestione (SCADA) delle Infrastrutture Energetiche e la conseguente necessità di essere progettati, installati, operati e mantenuti per resistere a un intenzionale *cyber assault* senza perdere alcuna funzione vitale.

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

È necessario aumentare la conoscenza delle vulnerabilità delle diverse Infrastrutture Energetiche (sia fisiche che *cyber)*, studiare gli effetti a cascata indotti dalla caduta di una Infrastruttura 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 delle Infrastrutture e prevenzione degli effetti di caduta a cascata

Data la natura distribuita delle Infrastrutture Energetiche, il monitoraggio della rete assume un ruolo importante soprattutto per il sistema elettrico. Il monitoraggio della rete consiste in tutte quelle azioni utili ad analizzare in continuo gli impianti di generazione, di trasmissione e di distribuzione dei fluidi energetici al fine di assicurarne la funzionalità essenziale anche in condizioni di emergenza, ad esempio a seguito di eventi catastrofici o di atti di sabotaggio. È necessario sviluppare strumenti concettuali e tecnologici per portare i rischi connessi ad eventi critici ad un livello di accettabilità sociale, combinando azioni di prevenzione, rilevazione, diagnosi e mitigazione. Risultano fondamentali, per il raggiungimento di tale obiettivo, quelle attività di ricerca focalizzate allo sviluppo di metodi e strumenti atti alla corretta analisi dello stato delle reti di trasporto dei fluidi energetici, alla rilevazione di eventuali situazioni anomale e all'individuazione di quella parte del sistema afflitta da danno al fine di isolarla ed impedire effetti-domino.

Cyber Security delle Smart Grid

Per affrontare il problema della *cyber security* delle Smart Grid occorre in primo luogo identificare quelle che sono le mutue dipendenze tra le tecnologie ICT e di telecomunicazione necessarie per il governo di una Smart Grid e quelli che sono gli *asset* rilevanti per il problema della *cyber security*. Ad oggi quando si parla di Smart Grid quasi sempre si intende l'uso estensivo

degli *smart meter* (contatori intelligenti) di cui l'Italia vanta un primato europeo nella sua introduzione. Ma per un reale sviluppo delle Smart Grid bisogna affrontare il problema di come garantire un adeguato livello di *security* dei sistemi ICS (Industrial Control System) integrati con reti per la trasmissione dati IP-based, entrambi necessarie per il governo delle Smart Grid. In buona sostanza, come garantire integrità e correttezza delle informazioni necessarie al governo delle Smart Grid sviluppando tecnologie di *intrusion detection* e architetture mirate a garantire la *resilience* (continuità del servizio) delle Reti, cercando di affrontare il problema al giusto livello di astrazione: dallo *smart meter* alla Smart Grid.

1.3 Sicurezza dei Confini

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, ma anche in spazi contigui internazionali (marittimi e aerei), sia per i rischi di diretto interesse nazionale per i trasporti, sia per i rischi anticipabili relativi all'ingresso all'interno dei 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.
Le tematiche di maggiore interesse saranno oggetto di approfondimento nei seguenti Sottosettori Guida:

- Sicurezza Aeroportuale
- Sorveglianza dei Confini

1.3.1 Sicurezza Aeroportuale

L'obiettivo di questo Sottosettore 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 diverse necessità di ricerca per affrontare, in un quadro coerente, tutti gli 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 rivolta 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.
Le sottotematiche di ricerca più rilevanti sono le seguenti:

- Controllo dei bagagli e delle persone, inclusi sistemi biometrici.
- Acquisizione e gestione dei dati biometrici.
- Sicurezza ATM
- Protezione piazzali ed edifici aeroportuali

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.

1.3.2 Sorveglianza dei Confini

L'obiettivo di questo Sottosettore è di indirizzare la ricerca e lo sviluppo verso una tematica fondamentale per la Sicurezza dei Confini, ovvero la capacità di "sorvegliare" in maniera integrata e coordinata insieme ai paesi confinanti, tutti gli spazi di transito (terrestre, marittimo, aereo) che permettono di varcare il perimetro frontaliero di un paese.
Le sottotematiche di ricerca più rilevanti sono le seguenti:

- Sistemi di sorveglianza Integrata per il monitoraggio terrestre e aereo
- Sorveglianza dei confini marittimi

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 che cercano di superare i correnti dispositivi di sorveglianza aerea civile e militare.
Questo scenario, inerente all'ambito dei confini aerei, è da considerarsi una "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) mediante le applicazioni di controllo del territorio.
Un'ulteriore esigenza è rappresentata dalla sorveglianza dell'intero perimetro frontaliero territoriale italiano per il contenimento di attività illegali (quali traffico droga, immigrazione clandestina). La complessità che deriva da questa esigenza è mitigata dal fatto che la relativa sorveglianza è da ricondurre ad una dimensione di appartenenza alla Unione Europea. Questo scenario, inerente l'ambito terrestre dei confini, è da considerare un'ulteriore 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 in assoluto a più alta priorità alta tra i 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 al fine di poter operare in modo tempestivo, tenendo conto del quadro di riferimento complessivo. Di conseguenza, 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).

1.4 Cyber Security

Per cyber-security si intende quell'insieme di tecnologie, processi e metodologie progettati per proteggere reti, sistemi, programmi e dati da attacchi, danni o accessi non autorizzati. Il ruolo

fondamentale assunto dalle Tecnologie per l'Informazione e la Comunicazione (ICT) nella nostra vita quotidiana ha prodotto, oltre ad innegabili benefici, un nuovo scenario nel quale risultiamo essere sempre più esposti a minacce di natura informatica, che non hanno più come obiettivo solo e soltanto il nostro personal computer, ma possono colpire qualsiasi sistema che usi le tecnologie ICT (da quelli per l'intrattenimento alle infrastrutture critiche per la fornitura dei servizi d base al cittadino). Numerose sono le prove che dimostrano come queste minacce stiano rapidamente evolvendo ed abbiano ormai raggiunto livelli di elevata pericolosità e complessità. Azioni sofisticate, mirate e coordinate sono state condotte negli ultimi anni contro obiettivi sensibili, a riprova della mutata natura assunta dagli attacchi informatici e della dimensione globale che ormai li caratterizza. Le *botnet* sono un chiaro esempio di questa nuova generazione di attacchi, in quanto fanno uso di un elevato numero di *host*, il cui comportamento è coordinato al fine di eseguire sia azioni di attacco di tipo tradizionale (forza bruta), sia attacchi di nuova concezione, subdoli e pressoché invisibili (*stealthy attacks*). Il concetto di cyber-security va quindi ormai ben oltre quello tradizionale di sicurezza informatica e il fattore discriminante è proprio l'incremento di scala nella dimensione e nella complessità degli attacchi e nell'impatto, anche di tipo economico e sociale, che essi possono avere. Non a caso, il nuovo programma di ricerca HORIZON 2020 della Commissione Europea ha incluso la cyber-security come uno dei temi chiave per affrontare la sfida della promozione di società inclusive, innovative e sicure. Nuove strategie e nuove tecnologie sono necessarie per far fronte a questa nuova forma di minacce e per garantire la protezione del cittadino, delle infrastrutture e dei servizi.
Le problematiche della Cyber Security comprendono sia la protezione dei dati trattati dai sistemi informatici che quella delle persone e/o beni da essi controllati/gestiti. Dato che questo campo è molto ampio, occorre individuare chiaramente le priorità da affrontare. Sono state identificate le seguenti tematiche:

- Sistemi di accesso;
- Sicurezza delle reti da attacchi e intrusioni;
- Information management su sistemi ad alte prestazioni;
- Studio e sviluppo di sistemi per la gestione della crisi.

Sistemi di accesso

Andrà affrontata 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 i singoli individui e per i gruppi, per 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 fisica sia quella logica.

Sicurezza delle reti da attacchi e intrusioni

Occorre 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: "pianifica, controlla, reagisci". 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. Particolare rilevanza assumono in questo contesto le tecnologie per la *Security Information and Event Management (SIEM).*

Studio e sviluppo di sistemi per la gestione della crisi

Risulta cruciale per la protezione di sistemi distribuiti e complessi adottare strategie globali di cyber-security che si basino su azioni coordinate che prevedano la collaborazione tra tutti gli attori coinvolti. É necessaria un'analisi estesa ed accurata di informazioni e dati riguardanti tutti i componenti e/o i livelli del sistema da difendere al fine di averne una visione completa e di poter individuare con efficacia e tempestività i potenziali rischi e, qualora l'attacco sia già in corso, i suoi sintomi.

1.5 Sicurezza Agroalimentare

Il settore agroalimentare è secondo in Italia per dimensione, subito dopo il metalmeccanico, e primo a livello europeo, seguito questa volta dal metalmeccanico. Il settore agroalimentare italiano è inoltre il terzo per fatturato nell'Unione Europea, dopo Francia e Germania. Questo settore si compone di filiere agroalimentari allineate su una moltitudine di attori che complessivamente occupano 2,5 milioni di addetti, rappresentando il motore economico e occupazionale più importante del Paese. L'obiettivo della sicurezza agroalimentare è di sviluppare e applicare sistemi atti a garantire l'integrità della filiera ed ad impedire la manipolazione e l'alterazione degli alimenti lungo la stessa. L'applicazione di sistemi tecnologicamente avanzati nel contesto agroalimentare permetterà un salto sistemico dell'efficacia e dell'efficienza del meccanismo di controllo pubblico (es. dogane, NAS, Istituti Ministeriali), nonché del sistema di autocontrollo delle imprese della filiera allo scopo di garantire il benessere del cittadino, oltre alla gestione rapida ed efficiente delle crisi alimentari con mitigazione del panico sociale e delle ripercussioni sulla competitività del *Made in Italy* sui mercati internazionali. A tale fine è necessario prevenire le alterazioni indotte da un *handling* non autorizzato delle derrate, dal *tampering* degli imballi e delle confezioni lungo tutta la filiera, dall'importazione di materie prime non sicure e da quelle conseguenti al non corretto funzionamento di altre infrastrutture quali la rete elettrica, i trasporti e le telecomunicazioni. Di fondamentale importanza è anche la prevenzione e la gestione delle contaminazioni volontarie o di inquinamenti involontari con sostante chimiche, biologiche o radiologiche a livello della produzione primaria, come conseguenza di azioni di agroterrorismo, di incidenti industriali, di disastri naturali, di alterazioni climatiche, di calamità del territorio e di squilibri ecosistemici. Tali tecnologie e sistemi potranno servire anche a prevenire alterazioni volontarie e frodi di alimenti protetti da marchi ed indicazioni di origine, con l'obiettivo di garantire la sicurezza dei cittadini sia tramite la tutela delle filiere alimentari sia di tutelare il *Made in Italy* alimentare. Le misure difensive da adottare riguardano lo sviluppo di tecnologie atte a sviluppare sistemi per identificare rapidamente (negli alimenti e non solo) la presenza di contaminanti introdotti volontariamente, per individuare precocemente organismi e microrganismi alieni in cibi, nell'acqua potabile o negli alimentari freschi o trasformati potenziali responsabili di pandemie vegetali, animali o umane, per quantificare la presenza di contaminanti biotici ed abiotici (es. tossine, patogeni umani, pesticidi, radionuclidi) negli alimenti, per prevenire incidenti e governare l'evento indesiderato verso il contenimento del danno e la minimizzazione dell'impatto, per applicare sistemi di tracciabilità e riconoscibilità lungo tutta la filiera e per evidenziare la manipolazione e/o di una non corretta conservazione del prodotto alimentare.

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, criminalità e mitomania, di garantirne un funzionamento continuo nel tempo, e se il caso, 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 ambiti urgenti di ricerca che, se attivati, avrebbero grande impatto sulla security per il settore agroalimentare.

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 le possibilità di manipolazione e per il mantenimento della catena del freddo. In aggiunta, eventi geopolitici possono mettere a rischio la fluidità dei trasporti e la sicurezza del contenuto spesso deperibile. 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 e controllata dall'esterno. L'obiettivo è di identificare e progettare nuove soluzioni a "sicurezza intrinseca" per sistemi mobili per alimenti e derrate, dotati di tecnologie innovative dedicate alla dissuasione dell'accesso al prodotto e con sistemi real-time di geolocalizzazione satellitare per l'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 o contenere le conseguenze del disastro (*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, biologica e nucleare 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 di filiera

Quest'area di ricerca dovrà promuovere linee di ricerche in campi avanzati, come l'ICT avanzato, la sensoristica intelligente e le tecnologie satellitari per il controllo del territorio e dell'ambiente, in grado di generare innovazioni di processo e di prodotto atti a garantire una maggiore security alimentare in ogni fase della catena, partendo dal campo 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 è indicatore di una forte richiesta da parte del mercato verso il prodotto *Made in Italy*, anche se privo di 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 e l'autenticità 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.

1.6 Sicurezza & Salute

L'obiettivo della tematica Sicurezza & Salute, è elaborare strategie e meccanismi per reagire alle minacce di origine dolose o ambientali che possono produrre stress sui alcuni settori del sistema Salute. 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 e gestirne la successiva ospedalizzazione. Occorre inoltre facilitare il trasferimento del paziente presso le strutture che più efficacemente possono prestargli il soccorso necessario. Negli scenari descritti, lo spostamento del paziente da una struttura ad un'altra non è di facile realizzazione. Questa difficoltà deve essere superata con l'ausilio della Telemedicina che permette di spostare, verso strutture di eccellenza, l'informazione relativa alle condizioni dell'assistito. L'applicazione alla medicina degli strumenti telematici (teleconsulto, tele monitoraggio) è fondamentale in caso di epidemia/pandemia per ridurre i contatti diretti tra persone e in situazioni di emergenze naturali (catastrofi, isolamento di intere zone, incidenti, etc.) o di attentati bioterroristici. In questi casi la richiesta di consulenza specialistica in tempi rapidi è essenziale per salvare un alto numero di persone coinvolte.
Durante le emergenze sanitarie (e non), le sale operatorie e le sale sanitarie da campo sono classificate come reparti ad alto rischio infettivo, in quanto in esse si registrano elevati valori di incidenza di infezione ospedaliera. Le possibilità di contaminazione chimico/biologica all'interno del blocco operatorio sono legate essenzialmente alla contaminazione da parte di strumentazione non sterile e alla contaminazione diretta o indiretta da parte di agenti microbici aerodispersi. 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. Il rischio biologico in ambiente ospedaliero e nelle sale sanitarie da campo è intrinsecamente correlato con l'attività dell'operatore sanitario per il diretto contatto con i malati, possibili portatori di patologie infettive, e con i loro liquidi biologici (sangue, saliva, aerosol respiratori, urine, feci, ecc.) anch'essi potenzialmente infetti.

Sottotematica: Emergenze Sanitarie

In uno scenario di emergenza sanitaria, i problemi che il personale medico deve affrontare sono molteplici:

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.

Tutti questi aspetti, assieme al teleconsulto medico (consulenza specialistica per ospedali di 1°e 2° livello) e alla gestione delle informazioni cliniche (Telemedicina), permettono di migliorare l'impiego dei servizi e delle strutture sanitarie disponibili. L'attenzione deve essere rivolta inoltre 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

Gramnegativi, assume una rilevanza non trascurabile. Un altro aspetto importante coinvolge la gestione dei "Gas Medicinali" che sono classificabili in: comburenti (permettono e mantengono la combustione ma non possono bruciare), combustibili (possono bruciare soltanto in presenza di un comburente), inerti e asfissianti (non mantengono la vita, non sono infiammabili, non permettono e non mantengono la combustione), tossici (nocivi per l'organismo a partire da una certa concentrazione e in funzione della durata dell'esposizione) e corrosivi (reagiscono chimicamente con molti prodotti come metalli, vestiti, tessuti umani, ecc.). I principali gas utilizzati nelle terapie sono: l'aria compressa (O2/N2), l'elio (He), l'ossigeno (O2), il protossido d'azoto (N2O), l'anidride carbonica (CO2) etc. I "Gas Medicinali" sono prodotti che possono essere usati in sala operatoria, nelle sale sanitarie da campo e sui mezzi di pronto intervento.

Sottotematica: Sicurezza in ambito Ospedaliero e nei prodotti-procedimenti farmaceutici

Nello scenario di emergenza successiva al verificarsi di un evento catastrofico, gli operatori sanitari, i pazienti e la popolazione (visitatori, familiari etc.) che frequentano presidi ospedalieri possono essere sottoposti a intensi campi elettromagnetici prodotti dal massiccio utilizzo di apparecchiature di tipo diagnostico/terapeutico.
L'obiettivo della ricerca riguarda:

a) Studio degli effetti biologici e genotossici di intensi campi magnetici statici e alternati.
b) Monitoraggio in continuo delle prestazioni delle apparecchiature di Risonanza Magnetica durante attività intensa e continuativa.
c) 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.
d) Sviluppo di sistemi, metodologie e strumenti per l'identificazione di farmaci e dispositivi biomedicali 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.
Nel settore della sicurezza nei prodotti-procedimenti farmaceutici, l'obiettivo è quello di 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. Bisogna tenere presente 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'ottica la lotta alla contraffazione diviene una della priorità per la sicurezza in ambito sanitario.

1.7 Sicurezza integrata dei beni culturali e del costruito

La necessità di assicurare la sicurezza dei beni culturali e del costruito rappresenta un'esigenza dal tremendo impatto sociale e culturale, come recentemente testimoniato sia dal sisma del 6 Aprile 2009 in Abruzzo, sia dalla serie di eventi di crollo che hanno interessato sempre recente-

mente uno dei siti archeologici più importanti al mondo quale quello di Pompei.
Tale esigenza assume un carattere ambivalente, dal momento che riguarda sia la Safety, con riferimento al rischio legato ad alterazioni ambientali e calamità naturali, sia la Security, riguardo ai danni connessi all'intervento umano e, in particolare, ad eventi terroristici e criminosi.
Sono notevoli le implicazioni di potenziali danni sia per la fruizione, specie per il bene culturale, che per la sicurezza degli utenti che usufruiscono della struttura (si pensi ad esempio ai visitatori di un museo o di un sito archeologico).
La necessità di mirare ad una sicurezza integrata dei due ambiti è bene evidenziata, peraltro, dalla raccomandazione UNESCO del 2012 relativa al Paesaggio Storico Urbano, che interpreta il paesaggio storico urbano come "area urbana risultato di una stratificazione storica di valori e caratteri culturali e naturali che vanno al di là della nozione di "centro storico" o "*ensemble*" sino ad includere il più ampio contesto urbano e la sua posizione geografica". Questo più ampio contesto include la topografia, la geomorfologia, l'idrologia e le caratteristiche naturali del sito, il suo ambiente costruito, sia storico che contemporaneo, le sue infrastrutture sopra e sotto terra, i suoi spazi aperti e giardini, i suoi modelli di utilizzo del suolo ed organizzazione spaziale.
È con riferimento a tale modello, che, Confindustria Servizi Innovativi e Tecnologici e la Fondazione Industria e Cultura, al fine di accrescere la partecipazione italiana nei programmi di ricerca europei nell'ambito del patrimonio culturale, hanno promosso la creazione della Piattaforma Tecnologica Italiana per il *Cultural Heritage* (CH) "IPOCH2", partecipata da oltre 130 imprese, università e centri di ricerca italiani, le cui tematiche sono di forte interesse anche per la sicurezza del nuovo costruito. Inoltre, la *Focus Area Cultural Heritage* (FACH) e la Piattaforma Tecnologica Europea delle Costruzioni (ECTP), all'interno della quale la protezione dei beni culturali è una delle esigenze più sentite, stanno congiuntamente portando avanti uno sforzo per favorire l'inserimento delle attività di ricerca riguardanti il Patrimonio Culturale all'interno dell' 8° Programma Quadro di Ricerca e Innovazione della Comunità Europea, Horizon 2020.
Va sottolineato come le esigenze di sicurezza siano alla base del nuovo concetto di "*Smart Cities*" e trasversali rispetto agli ambiti delle "*smart mobility, smart culture e smart environment*", ai fini di garantire uno sviluppo equilibrato a scala urbana e metropolitana. A riprova della rilevanza e dell'attualità del concetto di *smart cities*, sono da segnalare anche l'evento DNA Italia e i bandi, di recente emanazione da parte del MIUR, riguardanti la presentazione di idee progettuali in riferimento alle tematiche *Smart Cities* e *Communities*.
Da un punto di vista tecnologico, l'esigenza di sicurezza 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 e dei beni culturali. Ne consegue che le tecnologie abilitanti i due ambiti del costruito e dei beni culturali, dal momento che devono rispondere ad esigenze comuni, fra le quali la più stringente è quella della non-invasività, sono in notevole misura le stesse. Ad esempio, nell'ambito delle tecnologie di osservazione e *sensing*, è di primaria importanza assicurare un monitoraggio *long-term* della struttura e del bene culturale ai fini di una corretta manutenzione e programmazione degli interventi di consolidamento, restauro e *retrofitting*. 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 per la valutazione veloce dello stato e per l'identificazione di anomalie nel comportamento dinamico della struttura.

1.7.1 Sottosettore guida: Sicurezza e sostenibilità del costruito

L'ambito di questa attività di ricerca riguarda la promozione ed il miglioramento della 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 un' 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 particolarmente importante per la verifica della bontà e dell'efficacia delle operazioni di rinforzo e al tempo stesso, pone sfide interessanti in termini di attività di ricerca legate alla necessità di monitorare nuovi materiali (FRP, CAM, SMA). 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 un impatto sia sulla definizione delle priorità nella programmazione degli interventi, sia sulla *situation awareness* riguardante le strutture ed infrastrutture da impiegare nelle fasi immediatamente successive alla crisi.
Infine, assicurare condizioni di "safety e security" rappresenta una necessità cruciale alla base delle definizione di "*smart building"* quale "entità intelligente", capace sia di assicurare la sostenibilità rispetto al territorio e all'ambiente in termini di impatto ambientale ed efficienza energetica, sia di sfruttare al meglio le tecnologie abilitanti ICT per un controllo da remoto e continuo ed un monitoraggio degli impianti tecnologici ai fini di un risparmio energetico ed una migliore qualità della vita, oltre che per la gestione efficace delle situazioni di crisi per le persone e gli impianti, in seguito ad eventi naturali e/o atti criminosi.

Controllo degli elementi di un edificio

L'obiettivo della ricerca riguarda l'implementazione di un sistema di 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. Questo 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.

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.

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

Con riferimento al concetto di "*smart buildings*", l'obiettivo della ricerca riguarda il controllo continuo degli edifici con il duplice fine di evitare danni e malfunzionamenti dei diversi impianti tecnologici, anche conseguenti ad attacchi terroristici, e fornire inoltre supporto alla gestione delle situazioni di crisi con particolare riferimento alle procedure di evacuazione.

1.7.2 Sottosettore guida: Protezione dei beni culturali

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 i processi di fruizione vanno garantiti, da un lato, il rispetto delle condizioni di valorizzazione di Beni Culturali, con particolare attenzione a esistenza o prospettive di candidature a siti UNESCO e, dall'altro, la sicurezza stessa dei visitatori. Cruciale è anche la realizzazione di strumenti per la gestione di situazioni inerenti manomissioni o furti. È 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 differenti 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.

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. Un ulteriore importante obiettivo è la realizzazione di sistemi integrati atti a garantire la sicurezza dei visitatori nel rispetto della valorizzazione e della tutela, mediante rivelazione di situazioni di rischio ambientale sia per le opere esposte che per le opere in custodia, dei Beni Culturali e, al tempo stesso, di 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 duplice aspetto: da un lato, la sintesi e la messa in opera di tecniche per il riconoscimento automatico di persone, l'analisi automatica di scene e l'identificazione di comportamenti potenzialmente maligni tramite analisi di osservazioni connesse temporalmente, dall'altro l'approfondimento dei temi legati alla privacy delle persone in visita ad un sito di valore culturale che solleva diversi problemi quanto dal momento che 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 consiste nel rispondere all'esigenza di Sicurezza riguardante sia il rischio collegato ad eventi dolosi o terroristici, sia i rischi che si possono determinare durante il

trasporto, includendo anche le 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 un'efficacia limitata e le esercitazioni sul campo sono estremamente costose e difficili da allestire in modo realistico, può essere sicuramente 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*").

2. Nuovi Gruppi di Lavoro

2.1: TA 7 “Aspetti legali ed etici della sicurezza”

L’istituzione di una nuova area denominata “TA 7” e orientata alla disamina degli aspetti giuridici e sociali della sicurezza serve a colmare un importante gap all’interno di SERIT.
È opinione infatti di molti esperti che gli avanzamenti tecnologici, ed in special modo quelli inerenti la sicurezza, non possano prescindere da un›attenta analisi di un’ importante serie di altri aspetti legali, sociali ed etici.
Con riferimento, ad esempio, al settore della videosorveglianza, lo sviluppo inarrestabile negli ultimi anni ha evidenziato, da una parte, un’indubbia efficacia per migliorare la sicurezza dei cittadini, dall’altra, una certa perplessità per ciò che attiene alla tutela della privacy, soprattutto quando all›analisi tradizionale delle immagini si sono affiancate nuovi approcci come l›analisi comportamentale o la fusione di queste con tecnologie di tipo biometrico.
Sin dalla sua istituzione all›interno di SERIT, nel dicembre del 2011, quest’area ha suscitato un grande interesse da parte di studiosi di etica, scienze sociali e diritto. Oltre alla forte motivazione nell’apportare contributi alla nuova area, è apparso subito evidente che il TA7 sarebbe stato caratterizzato da una forte complessità, soprattutto a causa del gran numero di implicazioni associate ad un settore di per sé stesso vasto come quello della sicurezza.
Per tentare di dare, fin dall’inizio, un senso di concretezza alle attività di TA7, gli esperti del nucleo iniziale dell›area hanno identificato una missione ed alcuni obiettivi iniziali. In particolare, il mandato di TA7 è quello di offrire un supporto alle altre aree tecnologiche di SERIT nella disamina degli aspetti legali, sociali ed etici coinvolti nelle tecnologie senza, allo stesso tempo, rinunciare ad approfondire specifici temi propri.
Per ciò che attiene agli obiettivi iniziali, essi sono stati individuati in: (1) *data protection*, (2) tutela dei diritti della persona e (3) certificazione in tema di sicurezza.
Il primo obiettivo (*data protection*) fa riferimento ai vari aspetti inerenti la tutela dei dati personali con particolare riferimento alle tecnologie orientate alle sicurezza. Come già messo precedentemente in evidenza per il settore della video sorveglianza, un innalzamento delle misure di sicurezza può infatti comportare, in alcuni casi, un potenziale pericolo per i dati personali che, se sottovalutato, può influire negativamente, e talvolta in maniera decisiva, sul successo di una tecnologia. Come buona norma, infatti, qualsiasi innovazione dovrebbe essere supportata da un robusto e chiaro quadro normativo, mentre invece nella pratica, molto spesso il legislatore non riesce ad affrontare in maniera tempestiva il rapidissimo evolversi della scienza e della tecnica.
Del resto, i rischi connessi nella sottovalutazione della “*compliance*” di una data tecnologia con gli aspetti giuridici, sociali ed etici, con particolare riferimento alla protezione dei dati personali, consistono in una possibile inapplicabilità della tecnologia stessa. Essa infatti, passando da una fase sperimentale ad una applicativa, potrebbe trovare ostacoli dal punto di vista giuridico con possibili forti ripercussioni dal punto di vista economico e/o di limitazioni tecnologiche imposte.
Il tema della protezione dei dati personali sarà inoltre messo in stretta correlazione con la sempre maggiore diffusione delle banche dati. Ad esempio, sempre con specifico riferimento al tema della sicurezza, i progressi tecnologici compiuti nella realizzazione degli archivi di dati biometrici e, soprattutto, del DNA, sollevano una serie di questioni di tipo non solo tecnico ma

anche legale ed etico, per cui appare più che opportuno che un'area culturale di pertinenza del settore della sicurezza possa, all'occorrenza, offrire un contributo nell'affrontare eventuali punti di criticità e proporre soluzioni efficaci.
Il tema della tutela dei diritti della persona, secondo obiettivo iniziale di TA7, si prefigge di analizzare la posizione dell'utente nei confronti di una società dell'informazione sempre più onnipresente nella vita comune, con i suoi vantaggi ma anche con i suoi pericoli. Particolare attenzione sarà posta nel settore della cyber-safety, e cioè nello studio delle tecnologie più opportune per la tutela dei minori nell'uso di Internet.
Per ciò che attiene infine la "certificazione in tema di sicurezza", terzo obiettivo di TA7, la discussione con gli esperti del settore non sarà limitata all'ambito giuridico, ma sarà spinta ad esprimere valutazioni di opportunità in merito alla effettiva possibilità di affrontare in tempi ragionevoli un tema così complesso ma allo stesso tempo interessante ed indispensabile per lo sviluppo in Italia di nuove tecnologie utili nel contesto del sicurezza.
Allo scopo di disseminare le attività di TA7, saranno adoperate due strategie differenti basate sull'organizzazione di eventi e sulla produzione di monografie sugli specifici temi di competenza. Nell'autunno del 2012 è prevista l'organizzazione di una conferenza sulle attività dell'area tecnologica. L'evento, a carattere fortemente divulgativo, nelle intenzioni degli organizzatori vedrà una vasta partecipazione di esperti, sia del settore tecnico che giuridico, e avrà il compito di creare una convergenza e stimolare il confronto tra i due contesti culturali.
Per ciò che riguarda infine la disseminazione mediante pubblicazioni, saranno curate specifiche monografie in formato elettronico che saranno rese fruibili attraverso il sito web agli utenti di SERIT, i quali avranno modo di commentare i documenti attraverso l'uso di contesti di comunicazione quali blog o forum di discussione.

2.2: SG8 "Sicurezza delle Smart City"

Diversi fattori convergenti, come l'aumentato bisogno di sicurezza urbana, l'esigenza di una maggiore fruibilità di servizi pubblici e di diffusione delle informazioni, l'attenzione sempre maggiore rivolta al risparmio energetico e all'ambiente etc, hanno spinto le grandi aree metropolitane a ripensare la modalità attraverso cui gestire il complesso insieme cittadino.
La sicurezza urbana è da sempre un argomento controverso e ampiamente dibattuto che riguarda la gestione delle città: la prevenzione del crimine richiede un controllo capillare del territorio che ha imposto alle amministrazioni locali costi rilevanti, a cui si sommano i recenti tagli alle forze di sicurezza nazionali che hanno messo in crisi la capacità di monitoraggio della sicurezza dei cittadini.
Le catastrofi naturali purtroppo frequenti, così come l'accentuata instabilità politica sul territorio, hanno dato origine a nuovi rischi ambientali e terroristici, che richiedono una sempre maggiore capacità di prevedere, prevenire e reagire alle potenziali situazioni di crisi.
Allo stesso tempo, gli aumentati fabbisogni energetici e i relativi costi, nonché l'attenzione sempre maggiore verso l'ecologia e l'ambiente urbano, hanno portato a nuove esigenze da soddisfare sia nell'ambito del controllo energetico, sia del monitoraggio ambientale.
Infine, la maggiore quantità di informazioni a disposizione insieme alla capacità di comunicazione, hanno alimentato la crescita delle aspettative da parte dei cittadini per quanto riguarda la fruibilità e l'efficienza dei servizi, nonché di una rapida e capillare diffusione delle informazioni, utile non solo in caso di crisi o allerta, ma anche nel quotidiano.
Il tema delle *città intelligenti* ha proporzioni molto più ampie rispetto ai confini nazionali, tant'è

che l'Europa ha previsto investimenti di diversi miliardi di euro nei prossimi dieci anni per incentivare le Smart City, città di medie dimensioni capaci di coniugare sostenibilità e competitività in risposta alle diverse esigenze sopra citate .
La complessità di una Smart City è tale da dover considerare molteplici aspetti di Sicurezza a livello di tutte le componenti e la loro integrazione:

- **Sicurezza Fisica**: Sicurezza fisica delle infrastrutture di una Smart City, compresi gli edifici pubblici e privati, le infrastrutture di comunicazione, etc.;
- **Sicurezza Informatica**: necessità di garantire un elevato livello di sicurezza per lo "*Urban Cyber Space*", inteso come spazio virtuale di raccolta, elaborazione e scambio delle informazioni, e "nucleo" indispensabile per la gestione, il comando e il controllo di una città intelligente, dei servizi fruibili, dello scambio di informazioni etc.;
- **Sistemi di Trasporto**: sicurezza delle componenti del trasporto urbano ma anche della loro interconnessione, dei meccanismi di controllo e gestione dei mezzi, delle infrastrutture e dei servizi fruibili etc.;
- **Sistemi Energetici**, al fine di garantire la sicurezza delle infrastrutture adibite alla produzione pulita dell'energia , controllo dei consumi e riduzione al minimo di eventuali sprechi, gestione delle Smart Grid etc.;
- **Logistica Intermodale**: una città caratterizzata da un'ampia e variegata rete di trasporti perfettamente integrata e gestita a livello centrale per rendere la rete più efficiente.

Ad oggi, le tecnologie e i prodotti che possono essere fungere da *enablers* per la realizzazione di una Smart City sono tutte quelle componenti atte a garantire:

- Sicurezza fisica (per edifici, infrastrutture, etc);
- Cyber Security e resilienza agli attacchi informatici;
- Info Mobility (per la gestione e il controllo del traffico urbano/extraurbano/multimodale e per la gestione dei servizi associati) e *multi-devices networking*;
- Sicurezza nelle comunicazioni (sia a livello dell'informazione trasmessa, sia a livello di mezzo di trasmissione);
- Operazioni di gestione Multimodale (sia a livello di controllo delle infrastrutture sia a livello di gestione dei servizi associate);
- Infrastrutture per stress-testing (intesi come strumenti per la diagnostica e il test dell'insieme delle infrastrutture che compongono una Smart City (penetration testing)).

Le suddette caratteristiche *Smart* di una città intelligente, considerate sotto tutti i diversi profili, necessitano quindi di una centrale di gestione in grado di governare le diverse componenti nella gestione quotidiana, e al tempo stesso di pianificare e coordinare eventuali interventi, e di gestire un'eventuale situazione di crisi e post-crisi.

3. Coinvolgimento End User

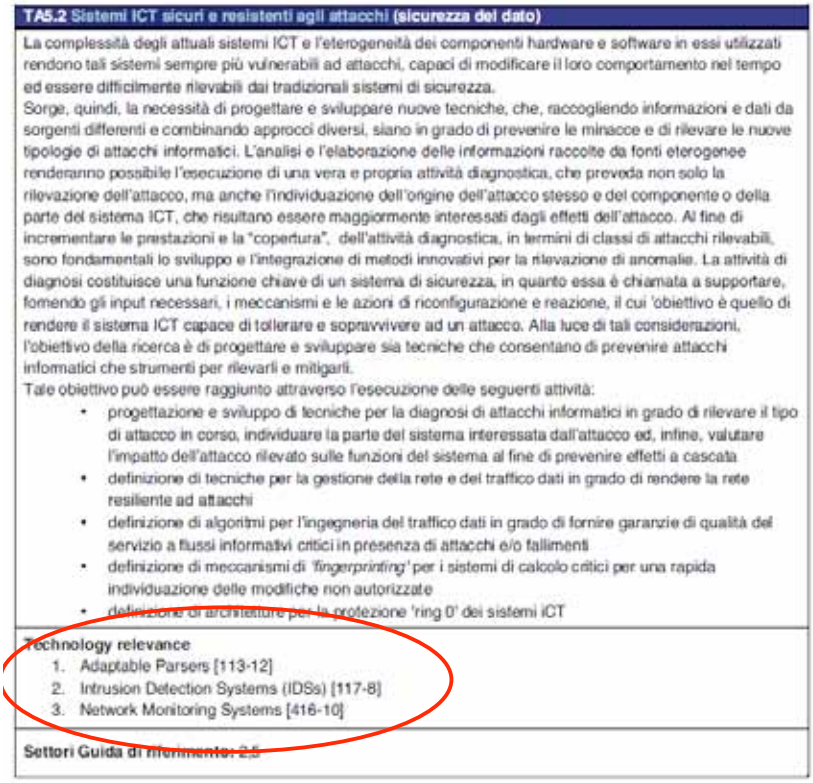
Le attività portate avanti dalla piattaforma (dall' identificazione delle priorità nei diversi temi afferenti alla sicurezza nazionale alla definizione dei relativi sviluppi tecnologici da perseguire nei prossimi anni), necessitano di una validazione e di una valorizzazione da parte degli stakeholder nazionali coinvolti nei settori della Sicurezza, al fine di riflettere e soddisfare al meglio i bisogni nazionali.
Per questo motivo, nel proseguire le attività lanciate nello scorso anno, si è cercato di coinvolgere attivamente, all'interno della piattaforma, un numero sempre maggiore di end-user con esperienza rilevante nei diversi domini applicativi.
Il coinvolgimento attivo degli utenti all'interno della piattaforma è un elemento imprescindibile per garantire che i risultati raggiunti siano elaborati, fin dalle prime fasi, in accordo ai requisiti espressi dagli stessi utenti, e successivamente validati attraverso un processo iterativo in grado di tenere conto costantemente delle mutevoli e nuove esigenze che possono manifestarsi in materia di sicurezza.
La piattaforma si è strutturata dunque in maniera tale da coinvolgere quanto più possibile gli utenti finali all'interno delle rispettive aree di maggiore interesse, in modo tale da attivare una proficua sinergia tra quella che è la domanda (requisiti utente) e l'offerta (capacità e competenze tecnologiche trasversali ai vari domini applicativi).
Per questo, è stato creato un comitato di *Liason* verso gli end-user partecipato da alcuni tra i membri di SERIT che hanno la possibilità di coinvolgere attivamente nella piattaforma una vasta gamma di *stakeholder* e utenti finali.
Le modalità di collaborazione tra gli utenti, guidate dai membri del *liason board*, sono estremamente flessibili (incontri telematici, richiesta di feedback su documenti, interviste telefoniche, partecipazione occasionale a workshops) e calibrate nel tempo, in modo da ottimizzare le risorse e la disponibilità di chi si impegna ad aderire.
L'adesione alla platea è uno strumento che permette agli utenti di trarre vantaggi in termini di:

- **Networking:** Creazione di una Rete di stakeholder Nazionali qualificati coinvolti nei settori della Sicurezza (utenti finali delle amministrazioni pubbliche e dei privati, industrie e PMI, istituzioni, centri di ricerca, università, …) con conseguente agevolazione del trasferimento delle conoscenze, possibilità di collaborazioni per opportunità di finanziamento, sviluppo di idee progettuali in iniziative e progetti R&D (nazionali e comunitarie), nonché l'attivazione di partenariati pubblico-privati (inclusa la filiera delle PMI), di sinergie negli interventi pubblici nazionali e regionali (distretti tecnologici) e la salvaguardia delle eccellenze tecnologiche;
- **Rafforzamento delle iniziative internazionali** tese a sviluppare tecnologie per la Security, supportando le linee di ricerca prioritarie nel VII Programma Quadro ed influenzando quelle del nuovo Programma Quadro Europeo (HORIZON 2020), trasferendo in un contesto più ampio le esigenze italiane di finanziamento per ricerca e sviluppo individuate dai membri della Piattaforma SERIT;
- **Aumento della 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 così incentivando l'accesso ad opportunità di marketing.

4. La Roadmap Tecnologica

Il lavoro svolto dalla Piattaforma SERIT ha permesso la definizione di una *roadmap* di sviluppo tecnologico per supportare la strategia di crescita dell'Italia in ambito sicurezza.
Basandosi sulle *capability* necessarie per ognuno dei settori guida, identificate nelle attività dello scorso anno, la piattaforma ha individuato una lista di tecnologie prioritarie su cui il paese dovrebbe investire, indicandone il livello di maturità tecnologica, i trend evolutivi ed il valore dell'investimento necessario nei prossimi tre anni per portare la tecnologia identificata ad un livello di maturità superiore.

Le tecnologie sono state classificate secondo una tassonomia condivisa, strutturata in quattro sezioni/sotto-sezioni:



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

1. ***Technologies & components*** (Sensor Technology and Components; Information Technologies, Artificial Intelligence & Decision support; Computing & Information Security Technologies; Biotechnology)
2. ***Equipments and sub systems*** (Sensor Equipments and signal protection; Forensic technologies)
3. ***Systems & Services functions*** (Human behaviuor and Identity Management; Simulation and Design tools, including Ergonomics and Human Factor)
4. ***Integrated platforms and systems*** (Platforms; Integrated Systems; Networks and information security systems)

Lo scopo della *roadmap* è quello di rappresentare uno strumento di riferimento per la comunità scientifica e tecnologica e per i decisori politici.
La *roadmap* mantiene nella sua rappresentazione i legami con le missioni di riferimento, i nuovi settori guida, ma permette anche di evidenziare la trasversalità delle tecnologie, rispetto alla *capability* da implementare.
Di seguito sono riportate le tabelle per SG delle *capabilities* prioirtarie (colonna) e l'indicazione delle sezioni/sottosezioni tecnologiche, di cui i TA hanno sviluppato le relative roadmap.

		Technologies&Components				Equipments and sub systems		Systems & Services functions		Integrated platforms and systems		
		Sensor Technology and Components	Information technologies Artificial Intelligence & Decision support	Computing & Information Security Technologies	Biotechnology	Sensor Equipments and signal protection	Forensic technologies	Human behaviuor and Identity Management	Simulation and Design tools, including Ergonomics and Human Factor	Platforms	Integrated Systems	Networks and information security systems
TA1	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			
	TA1.7 Sistemi di sorveglianza perimetrale		x	x								
	TA1.9 Strumenti di supporto alla sorveglianza mediante riconoscimento di scene e cross correlation di informazioni		x	x								
TA2	TA2.2 Reti wireless ad-hoc e di sensori					x						
	TA2.4 Integrazione del segmento satellitare a supporto di applicazioni evolute		x							x	x	
	TA2.6 Middleware, architetture di rete e comunicazione (Network Centric Communication), per l'integrazione di reti e sistemi eterogenei			x								
TA3	TA3.1 Detection ed imaging di persone e oggetti attraverso gli ostacoli (fuoco, muri, smog, metalli e altro)	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									
	TA3.3 Individuazione di eventi anomali basata sull'analisi integrata di misure ambientali, comportamentali e fisiologiche, incluse le biometriche		x	x								
	TA3.4 Check-point biometrico del futuro con auto accreditamento passeggeri	x	x									
	TA3.5 Soluzioni che individuano minacce collegate ai conducenti di mezzi di trasporto pubblico		x					x				
TA4	TA4.1 Sistemi innovativi di anti-intrusione	x						x	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	x			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	x							x	
	TA4.7 Metodologie e strumenti per l'analisi del rischio e l'ottimizzazione costo/benefici basati su simulazione e modellistica analitica		x									
TA5	TA5.1 Fusione delle informazioni raccolte da diverse sorgenti al fine di aumentare e migliorare il contenuto informativo		x									
TA6	TA6.3 Piattaforme multisensori intelligenti per la riduzione dei falsi allarmi nel monitoraggio di bio-hazard	x			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									

Settore Guida: Sicurezza dei Trasporti

		Technologies&Components				Equipments and sub systems		Systems & Services functions		Integrated platforms and systems		
		Sensor Technology and Components	Information technologies Artificial Intelligence & Decision support	Computing & Information Security Technologies	Biotechnology	Sensor Equipments and signal protection	Forensic technologies	Human behaviuor and Identity Management	Simulation and Design tools, including Ergonomics and Human Factor	Platforms	Integrated Systems	Networks and information security systems
TA1	TA1.7 Sistemi di sorveglianza perimetrale		X	X								
TA2	TA2.6 Middleware, architetture di rete e comunicazione (Network Centric Communication), per l'integrazione di reti e sistemi eterogenei			X								
	TA2.10 Sicurezza di Rete		X	X								X
TA4	TA4.7 Metodologie e strumenti per l'analisi del rischio e l'ottimizzazione costo/benefici basati su simulazione e modellistica analitica		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								X	
TA5	TA5.2 Sistemi ICT sicuri e resistenti agli attacchi (sicurezza del dato)			X							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			X	
TA6	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									
	TA6.9 Strumentazione portatile attiva o passiva per il monitoraggio di materiale radioattivo in discariche o in container commerciali	X	X			X						

Settore Guida: Sicurezza del Sistema Energetico

		Technologies& Components				Equipments and sub systems		Systems & Services functions		Integrated platforms and systems		
		Sensor Technology and Components	Information technologies Artificial Intelligence & Decision support	Computing & Information Security Technologies	Biotechnology	Sensor Equipments and signal protection	Forensic technologies	Human behaviuor and Identity Management	Simulation and Design tools, induding Ergonomics and Human Factor	Platforms	Integrated Systems	Networks and information security systems
TA1	TA1.2 Data Fusion di sensori eterogenei		x						x			
	TA1.4 Tecnologie abilitanti per il settore spaziale	x								x		
	TA1.6 Sistemi di localizzazione, navigazione e guida assistita		x							x		
	TA1.7 Sistemi di sorveglianza perimetrale		x	x								
	TA1.8 Piattaforme di sorveglianza marittima, terrestre e aerea		x	x						x	x	
	TA1.10 Sensori per la sorveglianza marittima e costiera, basati a terra o imbarcati		x									
TA2	TA2.6 Middleware, architetture di rete e comunicazione (Network Centric Communication), per l'integrazione di reti e sistemi eterogenei			x								
	TA2.9 Architetture di rete orientate al fast deployment			x							x	
TA3	TA3.1 Detection ed imaging di persone e oggetti attraverso gli ostacoli (fuoco, muri, smog, metalli e altro)	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									
	TA3.3 Individuazione di eventi anomali basata sull'analisi integrata di misure ambientali, comportamentali e fisiologiche, incluse le biometriche		x	x								
	TA3.4 Check-point biometrico del futuro con auto accreditamento passeggeri	x	x									
TA4	TA4.7 Metodologie e strumenti per l'analisi del rischio e l'ottimizzazione costo/benefici basati su simulazione e modellistica analitica		x									
TA5	TA5.1 Fusione delle informazioni raccolte da diverse sorgenti al fine di aumentare e migliorare il contenuto informativo		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	x								x
TA6	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										
	TA6.2 Sensori per monitoraggio a distanza di pericoli chimici e biologici da postazione mobile o fissa	x	x	x		x						
	TA6.3 Piattaforme multisensori intelligenti per la riduzione dei falsi allarmi nel monitoraggio di bio-hazard	x			x	x						
	TA6.4 Tecnologie microfluidiche accoppiate a nanostrutture molecolari per la detezione di biohazard	x			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	x			x						
	TA6.7 Nanotecnolgie per sistemi in spettrometria di massa: applicazioni nella rivelazione di esplosivi, droghe (metaboliti e impurezze).	x										
	TA6.8 Strumenti compatti ed efficienti per la rivelazione di parti metalliche di armi e munizioni o detonatori	x										

Settore Guida: Sicurezza dei Confini

		Technologies&Components				Equipments and sub systems		Systems & Services functions		Integrated platforms and systems		
		Sensor Technology and Components	Information technologies Artificial Intelligence & Decision support	Computing & Information Security Technologies	Biotechnology	Sensor Equipments and signal protection	Forensic technologies	Human behaviuor and Identity Management	Simulation and Design tools, including Ergonomics and Human Factor	Platforms	Integrated Systems	Networks and information security systems
TA2	TA2.7 Studio architetture Software Defined Radio & Cognitive Radio per applicazioni di sicurezza			X								
TA2	TA2.8 Protezione e disturbo del canale di trasmissione dati		X			X						X
TA2	TA2.10 Sicurezza di Rete		X	X								X
TA3	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									
TA3	TA3.3 Individuazione di eventi anomali basata sull'analisi integrata di misure ambientali, comportamentali e fisiologiche, incluse le biometriche		X	X								
TA3	TA3.4 Check-point biometrico del futuro con auto accreditamento passeggeri	X	X									
TA3	TA3.5 Soluzioni che individuano minacce collegate ai conducenti di mezzi di trasporto pubblico		X					X				
TA3	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	X								
TA5	TA5.2 Sistemi ICT sicuri e resistenti agli attacchi (sicurezza del dato)			X							X	
TA5	TA5.3 Piattaforme, architetture ed algoritmi per l'analisi in tempo reale di grandi volumi di dati (high performance computing)		X	X				X				
TA5	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			X	
TA6	TA6.3 Piattaforme multisensori intelligenti per la riduzione dei falsi allarmi nel monitoraggio di bio-hazard	X			X	X						

Settore Guida: Sicurezza ICT (CyberSecurity)

		Technologies&Components				Equipments and sub systems		Systems & Services functions		Integrated platforms and systems		
		Sensor Technology and Components	Information technologies Artificial Intelligence & Decision support	Computing & Information Security Technologies	Biotechnology	Sensor Equipments and signal protection	Forensic technologies	Human behaviuor and Identity Management	Simulation and Design tools, including Ergonomics and Human Factor	Platforms	Integrated Systems	Networks and information security systems
TA4	TA4.7 Metodologie e strumenti per l'analisi del rischio e l'ottimizzazione costo/benefici basati su simulazione e modellistica analitica		X									
TA6	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										
TA6	TA6.3 Piattaforme multisensori intelligenti per la riduzione dei falsi allarmi nel monitoraggio di bio-hazard	X			X	X						
TA6	TA6.4 Tecnologie microfluidiche accoppiate a nanostrutture molecolari per la detezione di biohazard	X			X	X						
TA6	TA6.7 Nanotecnolgie per sistemi in spettrometria di massa: applicazioni nella rivelazione di esplosivi, droghe (metaboliti e impurezze).	X										

Settore Guida: Sicurezza Agroalimentare

		Technologies&Components				Equipments and sub systems		Systems & Services functions		Integrated platforms and systems		
		Sensor Technology and Components	Information technologies Artificial Intelligence & Decision support	Computing & Information Security Technologies	Biotechnology	Sensor Equipments and signal protection	Forensic technologies	Human behaviuor and Identity Management	Simulation and Design tools, including Ergonomics and Human Factor	Platforms	Integrated Systems	Networks and information security systems
TA6	TA6.2 Sensori per monitoraggio a distanza di pericoli chimici e biologici da postazione mobile o fissa	X	X	X		X						

Settore Guida: Sicurezza & Salute

		Technologies&Components				Equipments and sub systems		Systems & Services functions		Integrated platforms and systems		
		Sensor Technology and Components	Information technologies Artificial Intelligence & Decision support	Computing & Information Security Technologies	Biotechnology	Sensor Equipments and signal protection	Forensic technologies	Human behaviuor and Identity Management	Simulation and Design tools, including Ergonomics and Human Factor	Platforms	Integrated Systems	Networks and information security systems
TA1	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			
	TA1.3 Elaborazione di immagini satellitari (SAR, ottico) ad alta risoluzione		X	X								
TA2	TA2.2 Reti wireless ad-hoc e di sensori					X						
TA4	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	X	
	TA4.7 Metodologie e strumenti per l'analisi del rischio e l'ottimizzazione costo/benefici basati su simulazione e modellistica analitica		X									
TA5	TA5.5 Realizzazione di algoritmi e processi per l'estrazione automatica e l'elaborazione del contenuto informativo di immagini		X			X						

Settore Guida: Sicurezza dei Beni Culturali e del Costruito

4.1 Technologies & Components

4.1.1 Sensor Technology and Components

Ambiti prioritari di ricerca

- Tecniche di rivelazione neutroniche
- Tecnologie Multispettrali
- Nanotechnologies for sensors
- Tecnologie a raggi X
- Tecnologia Sistemi Microelettromeccanici (MEMS)
- Tecnologie Gamma
- Tecnologia Terahertz
- Tecnologia Spettrometria a Mobilità Ionica
- Sensor related imaging and mapping techniques

- **Tecniche di rivelazione neutroniche**

Descrizione dello Stato dell'arte

Le tecnologie di rivelazione neutroniche includono sia le analisi non distruttive che utilizzano i neutroni come particelle primarie di interrogazione sia tecnologie di rivelazione che guardano ai neutroni come risultato di reazioni nucleari (interrogazioni attive) o di eventi di decadimento (interrogazioni passive). I sistemi di ispezione che fanno uso di neutroni come particelle primarie sono classificate a seconda dell'energia delle particelle (FNA/TNA: analisi neutronica con neutroni veloci/termici) o a seconda delle caratteristiche dei fasci (neutroni veloci pulsati, neutroni etichettati). La performance dei sistemi di ispezione neutronici è stata studiata in gran dettaglio durante gli ultimi 20 anni essenzialmente per rivelare esplosivi e/o materiali di contrabbando nei container. Tale studio è stato motivato dalla capacità di tali tecniche di identificare il material trasportato tramite l'analisi dei raggi gamma prodotti. Generalmente i sistemi neutronici sono stati proposti come sostitutivi dei scanner a raggi X. Tuttavia questa sostituzione non ha avuto successo a causa del lungo tempo di scanning caratteristico di tali sistemi e dalla mancanza di capacità discriminativa tra alcuni esplosivi e materiali di uso comune. L'utilizzo dei sistemi neutronici come sistemi di seconda linea dopo gli scanner X ha avuto maggiore successo, con il loro impiego solo in casi sospetti. Lo sviluppo di sistemi compatti altamente integrati e quindi mobili disegnati per ispezione di piccoli oggetti ha rappresentato un secondo *step* nell'uso di questa tecnologia. Per esempio, EADES-SODERN ha sviluppato ULIS (*Unattended Luggage Inspection system*). È importante menzionare che tutti i sistemi che utilizzano neutroni come particelle primarie soffrono di difficoltà autorizzative a causa del rischio da radiazione. Come esempio di sistemi passivi, la rivelazione di neutroni è richiesta per la rivelazione di Materiale Speciale Nucleare (SNM), nel contrasto del contrabbando nucleare. La rivelazione passiva di neutroni è estremamente efficace nel caso di isotopi del Pu mentre per uranio altamente arricchito l'emissione di neutroni e/o gamma deve essere stimolata da una radiazione primaria di interrogazione (come neutroni o gamma). È importante menzionare anche che la rivelazione e l'identificazione di SNM richiede specificatamente l'uso di tecniche nucleari essendo le tecnologie X non efficaci nel discriminare SNM da materiali pesanti. La rivelazione di neutroni è attualmente un importante campo di R&D a causa della così detta crisi del 3He dovuta all'enorme richiesta commerciale di gas 3He utilizzato per i rivelatori standard impiegati in applicazioni di Sicurezza Nazionale.

Descrizione dei Gap tecnologici

La prima gap tecnologica è rappresentata dalla sorgente stessa di neutroni. È infatti generalmente accettato che le sorgenti radioisotopiche (come il 252Cf) devono essere rimpiazzate con sorgenti elettroniche (piccolo acceleratori o macchine a plasma). Tuttavia questi sistemi sono di tipo dual-use con forti restrizioni a causa delle regole anti-proliferazione. Inoltre i generatori di neutroni devono essere autorizzati come macchine radiogene (sia per l'emissione di neutroni che per la presenza di circa 1 TBq di trizio). Sono attualmente in fase di sviluppo nuove tecniche di accelerazione come l'uso di cristalli piroelettrici per generare differenze di potenziale di 100 kV o l'applicazione di nano-strutture nella sorgente di ioni. Una seconda gap è rappresentata dalla difficoltà di trovare siti di test europei autorizzati per la sperimentazione con neutroni in cui siano disponibili anche campioni di material fissile. La terza gap è rappresentata dal rischio da radiazione intrinseco nelle tecnologie neutroniche attive. Questo impli-

ca la necessità di valutare l'impatto delle nuove tecnologie sull'utilizzatore e sulle operazioni standard. Studi specifici sono necessari per minimizzare i problemi connessi con il rischio da radiazione. Infine una gap tecnologica è dovuta agli algoritmi decisionali. A causa della estrema varietà degli scenari operative per i sistemi neutronici, è necessario disporre di un esteso database di risultati di test. Questo rende necessarie lunghe champagne di test in laboratorio e dimostrazioni sul campo.

Trend evolutivi

Gruppi di ricerca di altri paesi EU sono attivi in progetti nazionali o in ambito FP7 dedicati a tecniche di ispezione neutroniche. Tecniche neutroniche sono in via di sviluppo anche in USA (specialmente per la rivelazione di materiale nucleare), Russia (esplosivi e SNM) ed altri paesi (Canada, Giappone, Corea, India). Un prototipo di sistema mobile di ispezione è stato sviluppato nell'ambito di INDUSTRIA2015 in Italia. Inoltre azioni R&D nel campo della rivelazione passiva di neutroni per l'identificazione di SNM sono in atto nell'ambito di progetti FP7 con importante partecipazione italiana (MODES_SNM e SCINTILLA). Similarmente, la presenza di gruppi di R&D nel campo della tecnologia degli acceleratori è un importante pre-requisito per la possibilità di sviluppo di un programma nazionale sulle sorgenti di neutroni.

Livello attuale di TRL TRL5

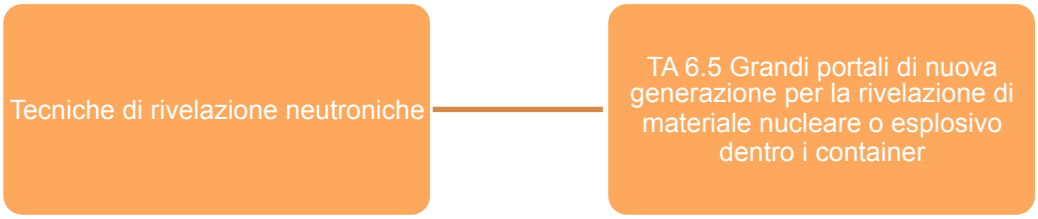
Step Necessari per arrivare a TRL + 1

I gruppi italiani di R&D hanno generalmente collaborato in progetti internazionali per lo sviluppo di sistemi neutronici e sono in attività gruppi nei campi delle tecnologie degli acceleratori e dei rivelatori. Lo sviluppo delle tecnologie neutroniche in Italia richiederà la definizione di un programma nazionale per lo sviluppo di sorgenti elettroniche portatili di neutroni basate su tecnologie avanzate di accelerazione. Un programma nazionale è richiesto per colmare la gap con altri paesi (come Francia, UK e Germania in EU) in cui hanno sede industrie manifatturiere di sorgenti neutroniche. Senza riempire questa gap le capacità italiane rimarranno limitate ad alcuni sotto sistemi (come rivelatori, elettronica di front-end o software) ma sarà difficile progettare e realizzare sistemi di ispezione basati su di un know-how nazionale. D'altra parte le sorgenti neutroniche possono essere anche interessanti in numerose applicazioni industriali (come l'industria petrolifera o medicale).

Costo associato per arrivare a TRL +1 (anni ed investimento economico)

Un programma nazionale per le sorgenti neutroniche può avere un costo di circa 3ME per tre anni e dovrà coinvolgere i più importanti enti di ricerca (ENEA, INFN), Università e partner industriali. L'uso di tecnologie innovative e di materiali al top dello stato dell'arte nel design della prossima generazione di sorgenti neutroniche potrà rendere il programma italiano in questo campo competitivo con i sistemi disponibili al giorno d'oggi in altri paesi che spesso adattano per le applicazioni di Sicurezza Civile materiale di derivazione militare. D'altra parte l'uso di generatori di neutroni nell'industria petrolifera rappresenta un mercato importante in seguito alla richiesta di sviluppare nuove tecnologie che permettano di realizzare interrogazioni con neutroni durante lo scavo di nuovi pozzi.

I TA di riferimento TA1, TA3, TA4, TA6



- **Tecnologie Multispettrali**

Descrizione dello Stato dell'arte

La rapida individuazione ed identificazione delle minacce (composti esplosivi, agenti di guerra biologica e chimica, nonché potenziali agenti tossici) è un problema primario per proteggere la società umana da attacchi terroristici. Per rilevare un gran numero di sostanze si richiedono sensori sofisticati e un database di spettrale. Tecnologie multispettrali come RAMAN, NIR, sono state applicate per individuare mediante profili spettrali sia composti singoli come pure multi-analita in matrici complesse. Tecnologie multispettrali MS (anche multibanda) si basano su sistemi che utilizzano la luce dalle frequenze della banda visibile al lontano infrarosso (termico), da 0,4 a 14 micron, comprese le piattaforme di acquisizione dati multispettrali e iperspettrali, piattaforme con la fotografia aerea, sensori iperspettrali e LIDAR (light detection and ranging). Tecnologie MS possono produrre immagini in cui ogni pixel contiene informazioni spettrali. A differenza delle tecnologie iperspettrali, metodi MS raccolgono meno di 20 bande spettrali, che non sono contigui. Il prodotto è una firma spettrale, riportando la riflettanza o l'assorbanza di un oggetto verso un intervallo di lunghezze d'onda; che è unica per ciascun materiale. Questa firma può essere utilizzata per l'identificazione e per la discriminazione. In tutti i casi, l'analisi è resa possibile per confronto con una libreria di spettri di riferimento a partire da materiali di composizione nota anche in condizioni diverse. Le tecnologie di rilievamento includono anche gli strumenti necessari per analizzare i dati, hardware e software per l'elaborazione automatica delle immagini, per l'Intelligenza Artificiale. Il telerilevamento MS permette il riconoscimento della copertura del suolo, di aree edificate, dell'acqua, della vegetazione. Tecnologie MS sono utili come metodi non invasivi per la misurazione dei processi biologici. Ad esempio, applicazioni sono state provate nel controllo degli alimenti, per esempio la presenza abnorme di carcasse di animali o superfici contaminate nei frutteti di e mela: questo può portare a casi di manomissione intenzionale con successivo blocco delle catene di approvvigionamento alimentare. A titolo di esempio, Headwall Photonics in prima linea nell'imaging iperspettrale, fornisce sensori HyperspecTM per la in-linea di controllo del pollame, frutta, verdura e colture speciali. L'imaging multispettrale è in grado di identificare le sostanze chimiche e particelle di esplosivi su superfici, come ad esempio le impronte digitali di TNT. Può essere applicato alla rivelazione di agenti biologici e al rilevamento di esplosivi improvvisati in forme diverse dalla fabbricazione allo rilevamento della distribuzione prima e durante le analisi forensi. Diversi dispositivi sono disponibili in commercio, ad esempio VideometerLab2 da Analitik Ltd, HyperspecTM da Headwall Photonics, VISIMSS dalla Pacific Advanced Technology. Per quanto riguarda la biometria, le tecnologie MS possono estrarre caratteristiche uniche sia dalla superfice che sotto la pelle.

Descrizione dei material tecnologici

Lacune tecnologiche sono presenti, in quanto gli analiti devono essere separati (come nell'analisi a GasCromatografia - IR) o essere disciolti in solventi appropriati (privi di vapore acqueo) o iniettati su superfici adeguate (trasparenti alla lunghezza d'onda utilizzata) o un ciclotrone con campo elettromagnetico. La richiesta che occorrerà affrontare nei prossimi anni è quella di combinare queste analisi con degli strumenti automatici che forniscano un elevato flusso di dati, come per esempio strumenti robotizzati, che utilizzano la microfluidica, e i nanomateriali. Lacune tecnologiche riguardano inoltre le sorgenti laser necessarie per coprire la gamma di lunghezze d'onda da utilizzare nei vari dispositivi. Un'altra lacuna è la necessità di algoritmi che discriminano i falsi positivi e falsi negativi, insieme con le biblioteche di spettri di riferimento. Nello sviluppo di tecnologie per la sicurezza, riveste un ruolo importante la fusione dei dati e lo scambio degli stessi verso l'operatore in modo da essere utilizzati facilmente con la condivisione di standard comuni, ed una versatilità alle esigenze di altri operatori stessi. L'armonizzazione è un bisogno primario, dal momento che ogni sistema o software sviluppato da una società di solito è incentrata sulle attività di proprietà. L'integrazione tra aziende diverse, paesi, sistemi è un compito difficile ma necessario.

Trend evolutivi

Miglioramenti sono previsti nell'aumento della sensibilità tramite lo sviluppo di nuovi rivelatori, nella separazione della luce di fondo, nell'uso di laser sintonizzabili, in nuovi materiali con range ottimale di trasmittanza ottica. i molteplici benefici e la mole di informazioni che si ricavano, hanno aperto nuovi campi di applicazione come nei Gas (GC), nella cromatografia liquida (nanovolumes) ad elevata risoluzione di singoli composti combinata con spettri IR, nella spettrometria a Termogravimetria infrarossa, negli spettrometri FTIR che combinano sia l'assorbimento che la modalità in emissione/Raman. L'utilizzo di tecnologie MS è ancora in gran parte limitata all'imaging e la ricerca è focalizzata allo sviluppo dei diversi componenti, cioè laser, filtri, sistemi confocali, analisi dell'immagine, che consentirà di ampliare il mercato dei dispositivi MS. Si prevede che il mercato sia influenzato dalla richiesta di sistemi per la difesa, con l'esercito come principale utilizzatore finale. Il mercato è destinato a crescere a 10 milioni di dollari entro il 2020.

Livello attuale di TRL TLR-5

Step Necessari per arrivare a TRL + 1

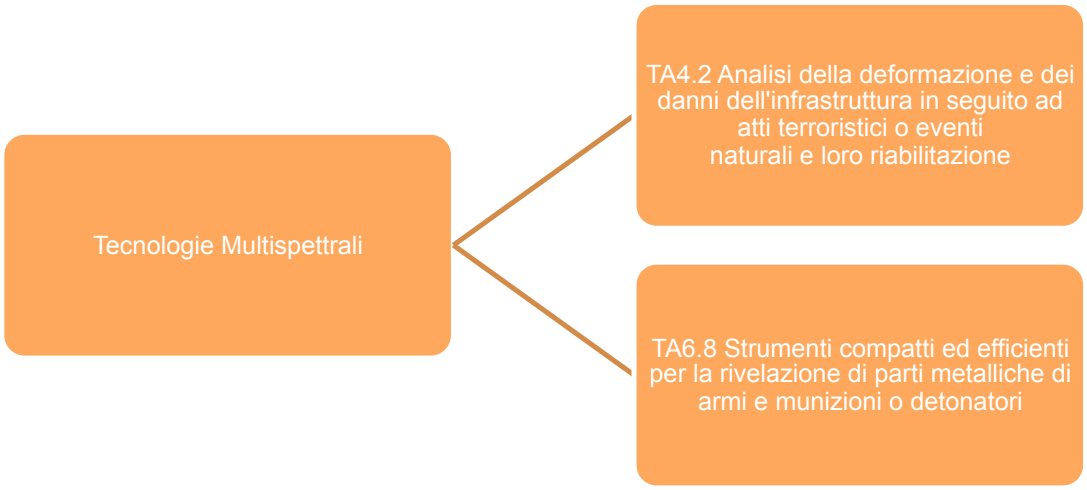
Migliorare la gamma di sostanze o elementi che possono essere rilevati: migliorare gli algoritmi e le librerie. Sviluppo di tecniche capaci di integrare nanomateriali nei supporti funzionali a costi affidabili e con elevato throughput.

Costo associato per arrivare a TRL +1 (anni ed investimento economico)

1,5million euro (500 keuro/year)

I TA di riferimento

TA1, TA3, TA4, TA6



- **Nanotechnologies for sensors**

Descrizione dello Stato dell'arte

Le nanotecnologie sono state e sono tutt'ora largamente utilizzate per aumentare la prestazione dei sensori in termini di sensibilità, selettività, stabilità e tempo di risposta. In complesso, lo sviluppo di tali tecnologie comporta approcci sia *top-down* che *bottom-up*. Nonostante che molti approcci diversi e combinazioni degli stessi siano stati sviluppati e studiati, le tecniche *top-down* sono usate soprattutto per preparare substrati funzionali (micropiastre riscaldanti, nanocantilever) con la struttura controllata a scala micro e nano, mentre i metodi *bottom-up* sono per lo più usati per sviluppare materiali funzionali, con lo scopo di sfruttarne le uniche proprietà funzionali. A seconda degli strumenti si usano approcci diversi, come ad esempio i sensori basati sui nanomateriali (CNT, nanofili a ossido di metalli, …) integrati su substrati o sensori "macroscopici" basati su trasduttori litografati (es. nanofili di Pd litografati), ma le prestazioni più innovative si ottengono integrando i due approcci (es: nanomateriali integrati su substrati micromacchine o nanocantilever funzionalizzati da recettori ingegnerizzati chimicamente). Prestazioni ancora più eccitanti si ottengono attraverso lo sfruttamento di architetture gerarchiche, che presentano diversi materiali o strutture organizzate a livelli diversi e scale diverse. La riduzione di scala di dimensioni e lunghezze aumenta l'importanza dei fenomeni di superficie e di interfaccia, così che grandi sforzi vengono dedicati ad adattare le proprietà di superfici e interfacce (es. nanoparticelle metalliche rivestiti con recettori organici). La selettività viene studiata con approcci diversi, tra cui lo sviluppo e l'integrazione di recettori specifici e l'uso di array di sensori non specifici in una configurazione da naso elettronico. La sensibilità è studiata sia migliorando le funzioni di recettori (es funzionalizzazione di superficie con recettori sensibili) e di trasduzione (es. ridurre la scala dei cantilene). La stabilità è considerata sia migliorando la qualità dei materiali (es. riducendo la presenza di difetti che inducono deriva e riducono la riproducibilità), sia lo sviluppo di protocolli diversi (es. fotoattivazione di reazioni chimiche anziché attivazione termica per evitare le instabilità associata alla attivazione termica). Sul mercato, alcune nanotecnologie sono già state adottate da aziende che vendono strumenti (es. sensori di gas basati su ossidi nanostrutturati). Alcuni strumenti per preparare

nanomateriali *bottom-up* sono disponibili sul mercato, con aziende che forniscono crescita omogenea su strati sottili. Analogamente, grandi aziende hanno strumenti litografici per gli approcci *top-down*, specialmente quelle coinvolte nelle tecnologie Si, e presentano alti tassi di produzione compatibili con il mercato. Infatti, substrati con caratteristiche di micro e nano-scala sono già disponibili sul mercato. Nonostante ciò, le soluzioni più innovative che comportano l'integrazione di nanomateriali e nanosubstrati non sono ancora compatibili con la produzione industriale (vedi le sezioni successive).

Descrizione dei Gap tecnologici

Vale la pena di notare che diversi sensori commerciali già sfruttano almeno in parte la nanotecnologia (ad esempio i sensori di gas commerciali con strati nanostrutturati). Le sfide principali per rendere i nanosensori adatti per lo sfruttamento industriale e la produzione di strumenti riguardano: lo sviluppo di metodi adatti per integrare nanomateriali in strumenti funzionali con costi e tassi di produzione accettabili. Oltre a questo, una sfida ulteriore riguarda lo sviluppo di metodi adatti all'uso di tali nanomateriali come blocchi di costruzione per preparare architetture con proprietà innovative o migliorate; ii) per un dato nanomateriale, la capacità di produrre un grande numero di unità quasi identiche; iii) adattare una appropriata interfaccia per scambi di trasportatori di carica; iv) mantenere la dimensione e l'organizzazione nano delle nanostrutture, evitando involontari autoassemblaggi e fenomeni di modificazione che possono alterare le proprietà dei materiali funzionali preparati.

Trend evolutivi

Diverso impegno è stato dedicato allo sviluppo di tecniche in grado di lavorare in parallelo, manipolare (muovere, orientare) più nanomateriali su più substrati allo stesso tempo. Analogamente, altre tecniche sono state dedicate a crescere direttamente nanomateriali su substrati funzionali. Le tecniche di autoassemblaggio appartengono a tali approcci. Sensibilità e selettività si cercano di solito in combinazione con altri sistemi, come preconcentratori o sistemi purge and trap, adatti ad aumentare la concentrazione ai livelli richiesti. Ciò è a volte necessario, ad esempio con gli esplosivi, la cui pressione di vapore è troppo bassa per avere una concentrazione misurabile direttamente in fase gassosa.

Livello attuale di TRL TRL4

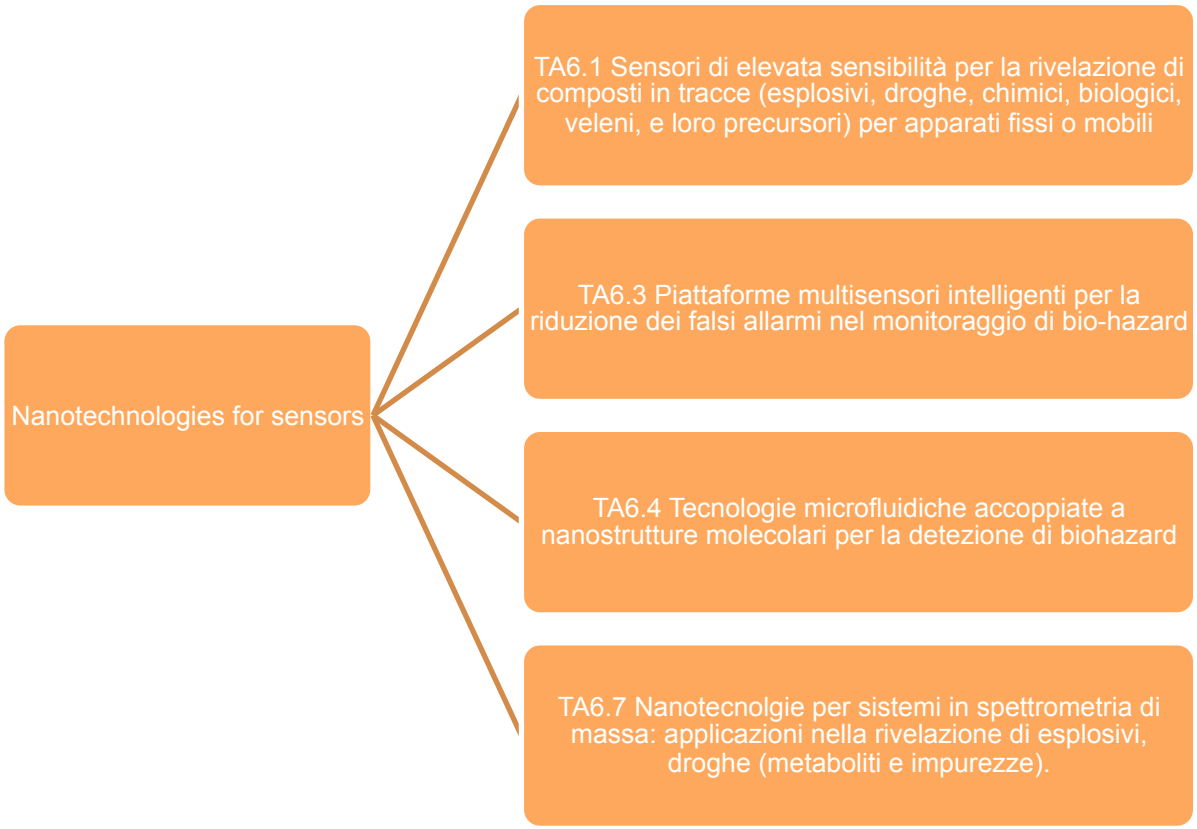
Step Necessari per arrivare a TRL + 1

Sviluppare tecniche in grado di integrare nanomateriali nei substrati funzionali a costi accessibili e con high throughput.

Costo associato per arrivare a TRL +1 (anni ed investimento economico)

3-5 anni con robusto investimento (centinaia di MEuro).

I TA di riferimento TA3, TA6



- **Tecnologie a raggi X**

Descrizione dello Stato dell'arte

L'ispezione con raggi X di container a scopo di controllo di sicurezza e interdizione del contrabbando si è rapidamente affermata nei porti a livello mondiale. Gli attuali sistemi di ispezione basati sui raggi X sono disegnati specificamente per il controllo di container marini, camion e carrozze ferroviarie con la possibilità di operare in spazi ridotti e producendo immagini di ottima qualità senza interferire con le normali attività portuali. Sono due le componenti primarie che determinano la qualità dell'immagine: la sorgente di raggi X che deve avere sufficiente energia per penetrare completamente i container anche se trasportano materiali con alta densità e il sistema di rivelazione che deve essere altamente sensibile con un range dinamico ampio per provvedere dati che riflettono accuratamente l'oggetto sotto ispezione. I tubi a raggi X sono limitati in energia a 450 kV con un potere di penetrazione corrispondente a circa 100 mm di acciaio, con ovvi limiti nello scanning di container. Gli acceleratori lineari forniscono energia variabile fino a 9 MV con potere di penetrazione di oltre 400 mm di acciaio. Numerosi produttori di sistemi di ispezione per container hanno trovato che acceleratori lineari tra 3 e 6 MV realizzano il miglior compromesso tra costi e performance complessiva. Sotto i 2 MV la penetrazione dei raggi X non è completa per container a pieno carico. Al contrario, in caso di accelerazioni significativamente superiori a 9 MV diventano necessarie schermature estese e vengono generati neutroni come prodotto non voluto. Sistemi recenti di ispezione includono anche tecnologie "dual view" e "dual energy". I sistemi a raggi X utilizzati negli aeroporti per ispezione di bagagli sono generalmente limitati come capacità di penetrazione della sorgente ma includono sia

tecnologie sofisticate per il riconoscimento dei materiali ("dual energy", misure simultanee di trasmissione e retrodiffusione) sia tecnologie avanzate tomografiche CT. Infine sistemi mobile di *back-scattering* sono commercialmente disponibili montati su furgoni per la rivelazione di esplosivi ed altri materiali pericolosi. Lo sviluppo di nuovi scanner X è realizzato in generale da grandi gruppi industriali che hanno la capacità di ingegnerizzare sistemi complessi. In questo campo sono attive alcune grandi industrie europee. Una industria di medie dimensioni è attiva in Italia nel campo dei sistemi di controllo per aeroporti. D'altra parte, azioni di R&D che potranno portare a sotto-sistemi innovativi sono attualmente in corso negli enti di ricerca e nelle università. È importante anche sottolineare come gruppi di ricerca italiani siano attivi sia nel campo delle tecnologie di rivelazione sia nell'elaborazione che nella ricostruzione delle immagini, poiché tali campi possono trovare significative applicazioni anche in altri campi industriali come il medicale.

Descrizione dei Gap tecnologici

Uno dei maggiori sviluppi richiesti per la prossima generazione di scanner X per bagaglio è la capacità di rivelare esplosivi plastici anche in forma di foglio. Questi oggetti mostrano un basso contrasto e le loro caratteristiche all'ispezione X sono simili a quelle di alimenti di uso comune. Di conseguenza, è difficile poter identificare con chiarezza questi esplosivi nel bagaglio. Una possibilità per superare questo problema è l'implementazione di sistemi a "*multi-energy*" rispetto a quelli "*dual energy*" comunemente adottati nei sistemi di controllo. L'analisi "*multi-energy*" può essere ottenuta irradiando il bagaglio con un fascio di raggi X ad ampio spettro energetico ("bianco") e rivelando il fascio trasmesso con rivelatori sensibili all'energia. Con questa procedura è possibile ottenere contemporaneamente un numero di immagini in falso colore ottimizzando il contrasto tra materiali con una piccola differenza nel numero atomico effettivo.

Trend evolutivi

Ad oggi sembra che le industrie nazionali ed i centri di ricerca italiani non siano coinvolti nello sviluppo di sistemi di ispezione X per container. Al contrario, esistono industrie nazionali attive nel campo di sistemi per controllo del bagaglio. La realizzazione di sistemi "*multi-energy*" richiede lo sviluppo di alcuni sotto-sistemi: i) il generatore di fasci bianchi di fotoni; ii) rivelatori spettroscopici; iii) elettronica di *front-end* e *back-end*; iv) algoritmi per l'analisi dell'immagine e l'identificazione di specifici materiali pericolosi. Vi sono numerosi gruppi di ricerca italiani che hanno una grande esperienza in questi campi. Inoltre, sistemi "*multi-energy*" possono trovare impiego in altri campi di interesse rilevante per l'industria italiana, come il controllo di qualità dell'industria alimentare oppure per test di saldature.

Livello attuale di TRL TRL5

Step Necessari per arrivare a TRL + 1

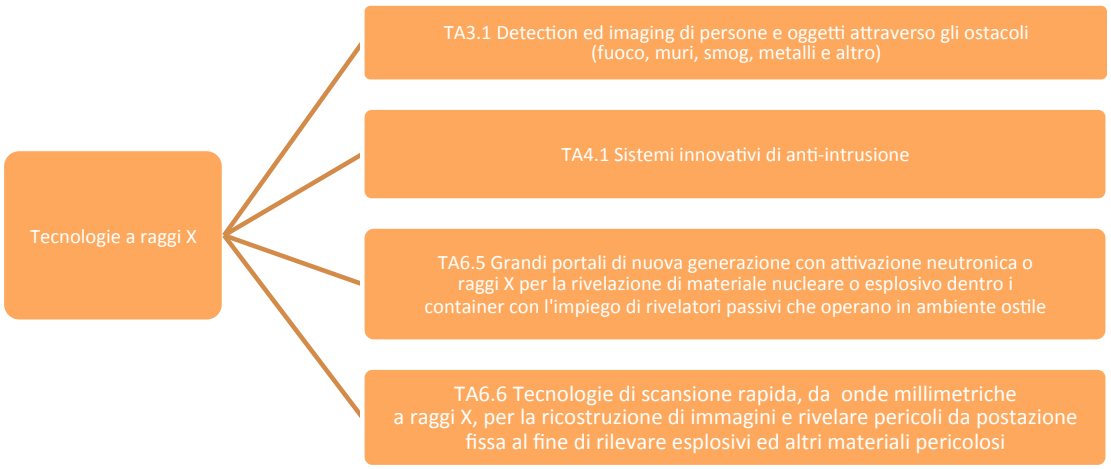
Definizione di un progetto nazionale basato su un'analisi approfondita dei trend internazionali nel campo dell'R&D, delle richieste degli end-users nelle differenti applicazioni e sulle future possibilità di mercato, con l'obiettivo di sviluppare: 1) tecnologie avanzate per la preparazione di rivelatori X ad alta risoluzione con costi minori e migliori caratteristiche spettroscopiche rispetto ai rivelatori attualmente disponibili; 2) miglioramento dell'elettronica di *front-end* e *back-end* per massimizzare la risoluzione in energia dei rivelatori; 3) algoritmi per l'analisi dell'immagine e l'identificazione di materiali pericolosi; 4) prototipi di scanner a raggi X con migliorate capacità

rispetto ai sistemi attualmente in commercio.
A questo fine il ruolo degli end-user è estremamente importante per definire le necessità che nascono dall'attività sul campo.

Costo associato per arrivare a TRL +1 (anni ed investimento economico)

Considerando le capacità industriali nazionali esistenti e la presenza di forti gruppi di ricerca e sviluppo nelle università ed enti di ricerca, la durata di un progetto è stimato in due anni con un costo di circa 5 MEuro.

I TA di riferimento TA1, TA3, TA4, TA6



- **Tecnologia Sistemi Microelettromeccanici (MEMS)**

Descrizione dello Stato dell'arte

I sistemi microelettromeccanici (Micro-Electro-Mechanical Systems MEMS) integrano elementi meccanici — sensori, attuatori ed elettronica — su un substrato di silicio comune attraverso una tecnica di micromanifattura, usando processi compatibili di "micro machining" che sottraggono in modo selettivo parti del wafer di silicio o aggiungono nuovi strati strutturali per formare gli strumenti meccanici ed elettromeccanici. Sono largamente usati per radiofrequenza e per componenti della microfluidica, e anche per biocompositi, con una grande varietà di applicazioni nelle industrie per la salute umana, militari e automobilistiche. I MEMS uniscono la microelettronica basata su silicio con le tecnologie di micro machining, rendendo possibile la realizzazione di sistemi completi su chip. I MEMS sono una tecnologia che consente lo sviluppo di prodotti intelligenti, aumentando la capacità computazionale della microelettronica con le capacità di percezione e controllo dei microsensori e dei microattuatori, ed espandendo le possibilità di progettazione ed applicazione. I MEMS possono essere fusi non solo con la microelettronica ma anche con altre tecnologie, come la fotonica (integrazione eterogenea). Le applicazioni dei sensori ovviamente richiedono la miniaturizzazione e i MEMS basati su silicio o su SiC sono promettenti per questi forti requisiti. Il mercato principale per i MEMS è attualmente intorno a $8 miliardi e ci si aspetta che crescerà a $30 miliardi per il 2050. La dinamica di mercato per i MEMS sarà molto simile a quella del mercato

dei semiconduttori. Ci sono oggi due applicazioni principali per gli strumenti MEMS. La prima è uno strumento attivo come una testina di stampante a getto d'inchiostro Ink Jet Printer o un microspecchio per proiettori, la seconda è uno strumento passivo come un sensore. Poiché ogni applicazione richiede le proprie caratteristiche speciali per ogni sensore, che dipendono dai requisiti adatti, è necessario capire la prestazione totale del sistema così come le prestazioni delle diverse componenti del sistema.

Descrizione dei Gap tecnologici

Per fabbricare un microstrumento si devono eseguire parecchi processi, tra cui la deposizione del film e la schematizzazione con le microcaratteristiche desiderate e la rimozione di parti del film. Per esempio, nella fabbricazione di una scheda di memoria standard ci sono fino a 70 o più passaggi (litografia, ossidazione, scolpitura, funzionalizzazione, etc.). La complessità dei processi di microfabbricazione può essere descritta dal conteggio delle "maschere". Il numero dei diversi strati costituisce un punto critico. Per esempio, i moderni microprocessori sono fatti con 30 maschere, mentre poche maschere sono sufficienti per uno strumento microfluidico o per un diodo laser. Un'altra importante limitazione è che i processi MEMS vengono svolti in camere pulite (clean rooms), che richiedono alti costi.

Trend evolutivi

Poiché il mercato richiede strumenti più piccoli, più efficaci e più economici, servono nuovi approcci per la manifattura dei MEMS. I mercati in rapida crescita guidati dalle applicazioni al consumatore sono:

- Dipendente dalle dimensioni: es. smartphone e computer portatili;
- Dipendente dalle prestazioni: es. aerospaziali ;
- Dipendente dal costo: es. Applicazioni di volume come telefoni cellulari, automobili, consolle per videogiochi.

Perciò, tra le tecniche di manifattura MEMS, sono necessarie tecnologie di packaging e materiali specifici necessarie per risolvere questi problemi, e le seguenti possono essere importanti:

- A livello di substrato: SOI, vetro, wafer sottili, silicio etc.;
- A livello di MEMS: condizioni ambientali opportune all'interno dei MEMS (getters), adesione spontanea di substrati (fusion bonding), riduzione della frizione-statica (release stiction), lavorazione selettiva di strati sacrificali et al. (singulation), CMOS MEMS in cui è necessaria una processatura elettronica molto compatta, etching ionici reattivi profondi (DRIE), tecnologie di isolamento tra parti adiacenti dei dispositivi (trench isolation);
- A livello di packaging per iduzione dimensioni e costi: packaging 3D del tipo Through Silicon/Glass Via (TSV, TGV), scaling dal packaging a livello di wafer a quello di pixel (pixel-level packaging), incapsulamento dei MEMS mediante strati a film sottile (thin film capping), bonding diretto tra il wafer ASIC ed il wafer MEMS (active capping).

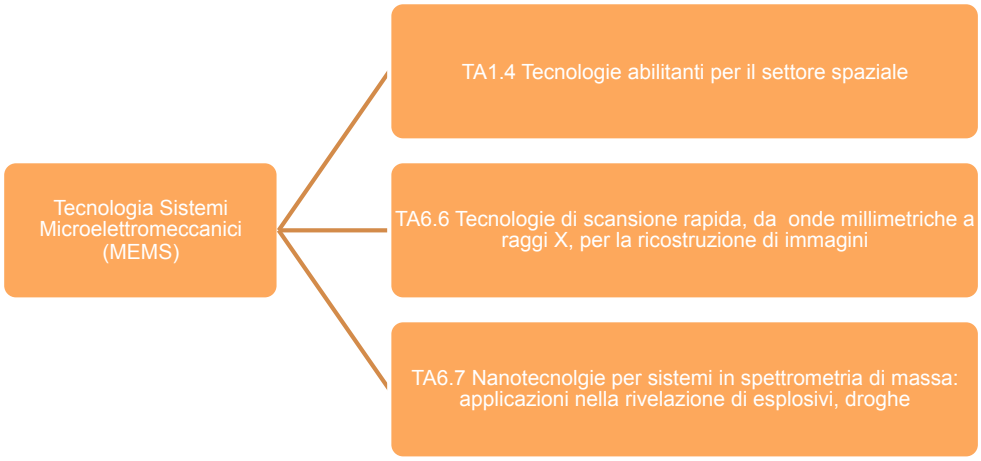
Livello attuale di TRL TRL 5-6

Step Necessari per arrivare a TRL + 1

Acquisizione di tecnologie innovative per la riduzione di scala dei dispositivi ed il loro costo

Costo associato per arrivare a TRL +1 (anni ed investimento economico)
1-2 anni e circa 1 M€/anno

I TA di riferimento TA2, TA3, TA6



- **Tecnologie Gamma**

Descrizione dello Stato dell'arte

Le tecnologie gamma sono necessarie in relazione a sistemi di interrogazione attivi neutronici nella ricerca di esplosivi, nell'individuazione di sostanze illecite o di materiali speciali nucleari (SNM). Queste tecnologie rappresentano inoltre la componente più importante in sistemi passivi come portali di radiazione autonomi utilizzati per lo screening contro i materiali radioattivi in diversi scenari operativi. I requisiti per le due applicazioni sono sostanzialmente diversi poiché i sistemi ad interrogazione attiva normalmente richiedono alte velocità di conteggio e rapidità di risposta, mentre i portali di radiazione richiedono soprattutto una buona efficacia di rivelazione. Rivelatori a scintillazione e semiconduttori vengono generalmente impiegati allo scopo. In entrambi i casi la maggior parte della R & S è stata eseguita all'interno di grande collaborazioni internazionali con notevole partecipazione italiana. Tuttavia la produzione di rivelatori avanzati si trova oggi in UE e negli USA (sia HPGe che nuovi materiali a scintillazione), mentre la produzione di massa di quelli più maturi (come gli scintillatori NaI(Tl)) viene realizzata anche nei paesi dell'est (Ucraina, Russia, Cina). Allo stesso tempo, c'è un'attività di ricerca costante (anche in Italia) per lo sviluppo di rivelatori di raggi gamma che operano a temperatura ambiente, in modalità spettroscopica basati su alto Z (materiali CdZnTe, TlBr, InI). L'Italia ha ancora un ruolo di primo piano nel settore dell'elettronica di *front-end*.
Guardando in particolare ai requisiti per la prossima generazione di sistemi basati su rivelatori gamma, vale la pena di citare lo sviluppo di sistemi (passivi) per la rilevazione e l'identificazione di materiale radioattivo e Speciale Nucleare SNM per sostituire quelli comunemente utilizzati nei dispositivi Radiation Portal Monitor (RPM) e di identificazione a radioisotopi (RID, dispositivi portatili) impiegati in diversi scenari operativi. Gli sviluppi principali di queste tecnologie sono legati all'aumento della sensibilità degli RPM per abbassare i limiti di rivelazione e alla richiesta di poter eseguire nei portali anche l'identificazione della sorgente (selettività) come nei RID.

Quest'ultima funzione è necessaria per chiarire direttamente la fonte di contaminazione, definire il rischio per gli operatori e per il pubblico in generale e, infine, per decidere la strategia di riduzione del rischio. A tal fine, una nuova generazione di strumenti, i cosiddetti portali di radiazione spettroscopici sono stati sviluppati negli Stati Uniti sotto la guida dell'Ufficio Domestic Nuclear Detection. Tuttavia questi nuovi prototipi soffrono di costi molto elevati e non hanno una risoluzione sufficiente in energia quando vengono realizzati utilizzando scintillatori NaI (Tl). Una ulteriore possibilità per ottenere l'identificazione della sorgente è l'uso di scintillatori organici plastici tradizionali (come i liquidi) con l'aggiunta di un più avanzato sistema di lettura ed elaborazione dati per estrarre le informazioni sugli isotopi. Tale tecnica può essere anche impiegata nei RID.

Descrizione dei Gap tecnologici

Considerando che oggi rivelatori standard di raggi gamma possono essere trattati come COTS (Commercially available Of The Shelf) e che vi è una capacità industriale italiana nel campo dell'elettronica nucleare, uno dei gap tecnologici maggiori è rappresentato dall'assenza di capacità nella progettazione di nuovi sistemi di rilevamento delle radiazioni. Ciò è causato dalla mancanza di una significativa iniziativa industriale nel campo degli strumenti per il controllo della radiazione.
Nuovi portali avanzati e strumentazione portatile RID potrebbero essere progettati senza fare uso di rivelatori ad alto costo. Infatti una più avanzata elettronica di raccolta ed elaborazione dati potrebbe comportare un sostanziale miglioramento delle capacità del sistema basato su sensori di raggi gamma a basso costo, che soddisfa le specifiche generali delle maggiori agenzie internazionali e le prescrizioni tecniche degli standard esistenti.
La riduzione dei costi e / o la valorizzazione delle prestazioni dei rivelatori di raggi gamma ad alta risoluzione utilizzando nuovi materiali è la parte centrale del problema. Tali rivelatori ad alta risoluzione sono inoltre necessari in applicazioni analitiche nel campo della sicurezza, come, per esempio, nel sistema analitico per il rilevamento della radioattività in campioni liquidi comunemente utilizzati in medicina, o per la protezione ambientale. In questo campo, esiste una lunga tradizione nella comunità di ricerca italiana che ha bisogno di essere guidato verso la progettazione di prodotti industriali.

Trend evolutivi

Alcuni gruppi italiani (industria + R & D di base) sono già attivi in progetti di ricerca del 7° PQ nel settore dei rivelatori di radiazione per la sicurezza. Alcune attività di ricerca sono state effettuate anche all'interno dei programmi nazionali del MIUR INDUSTRIA2015. Di conseguenza, un certo lavoro in generale in questo campo è in corso. Tuttavia, un programma nazionale più mirato e finalizzato alla applicazione di nuove tecnologie in nuovi prodotti è richiesto con un forte legame tra i gruppi di ricerca e gli utenti nazionali per definire meglio le esigenze e le necessità di ogni specifica applicazione. Anche in questo caso, un partner industriale deve garantire che le attività di R & S siano focalizzate verso lo sviluppo di prototipi con una quota del mercato futuro.

Livello attuale di TRL TRL5

Step Necessari per arrivare a TRL + 1

Definizione di un progetto nazionale sulla base di un'indicazione delle tendenze di R&D internazionali, delle esigenze degli utenti finali nelle diverse applicazioni e delle possibilità future

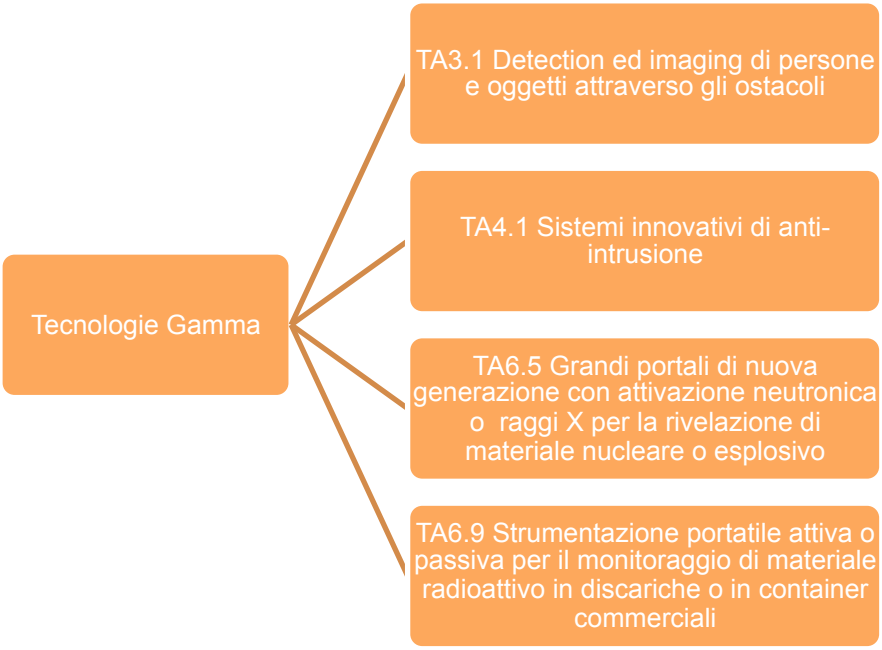
applicazioni del mercato con l'obiettivo di sviluppare:

1) tecnologie avanzate per la realizzazione dei rivelatori di raggi gamma ad alta risoluzione a bassi costi e con una migliore prestazione spettroscopica rispetto ai rivelatori attualmente disponibili
2) prototipi di strumenti portatili RPM e RID con capacità spettroscopiche basate su rilevatori di raggi gamma a basso costo e una maggiore capacità rispetto alla linea di base degli attuali dispositivi commerciali. A questo proposito, il ruolo degli utenti finali è estremamente importante per definire le necessità operative.

Costo associato per arrivare a TRL +1 (anni ed investimento economico)

Tenendo conto delle attuali capacità industriali nazionali e la presenza di forti gruppi di R & S nelle università e negli istituti di ricerca, il tempo necessario è stimato nell'ordine di 2 anni, con un costo del progetto di circa 3 MEuro.

I TA di riferimento TA1, TA3, TA4, TA6



- **Tecnologia Terahertz**

Descrizione dello Stato dell'arte

Generalmente il termine Terahertz copre tutte le applicazioni delle radiazioni elettromagnetiche nella gamma di frequenze da 300 GHz a 3 THz, con un confine tra l'IR lontano (far-IR) e le onde submillimetriche. In passato la tecnologia Terahertz era una nicchia esclusiva nella spettroscopia ad alta risoluzione e nell'area di remote sensing in cui tecniche di eterodina e trasformata di Fourier hanno permesso agli astronomi, chimici, e gli scienziati dello spazio di misurare, catalogare le righe di emissione termiche di un'ampia varietà di molecole leggere. Oggigiorno, la radiazione Terahertz è molto interessante in quanto non è ionizzante e ha in comune con le microonde la capacità di penetrare attraverso una vasta gamma di materiali non conduttivi. Le radiazioni

Terahertz possono passare attraverso i vestiti, la carta, il cartone, il legno secco, la muratura, la plastica e la ceramica. Può anche penetrare attraverso la nebbia e le nuvole, ma non può penetrare il metallo o l'acqua. Queste peculiarità si trasformano in possibilità di utilizzare la tecnologia Terahertz nella sorveglianza, nei controlli di sicurezza, per scoprire armi nascoste su una persona anche a distanza. Ciò è di particolare interesse perché molti materiali hanno delle "impronte digitali" univoche nella banda dei Terahertz. Molti materiali di interesse per applicazioni di sicurezza, tra cui gli esplosivi, gli agenti chimici e biologici hanno spettri THz caratteristici che possono essere utilizzati al fine della loro identificazione. le peculiarità di questa tecnologia offrono la possibilità di combinare l'identificazione spettrale con la immagini ad alta risoluzione (radiazioni superiori a 300 GHz hanno una risoluzione spaziale inferiore ad 1 mm). Apparati Terahertz attivi o passivi utilizzano una sorgente di radiazione, dei rivelatori, sistemi di invio / ricezione e un'elettronica dedicata. Attualmente le fonti disponibili sono: gyrotron, ondulatori, laser nel lontano infrarosso, laser a cascata quantica, laser ad elettroni liberi, fonti di luce di sincrotrone, le fonti photomixing, a ciclo unico fonti utilizzate nella spettroscopia di dominio del tempo Terahertz (come emettitori di rettifica fotoconduttrici e ottica). I rivelatori tipici sono bolometri, piroelettrici, diodi Schottky GaAs, giunzioni Josephson. In linea di principio la tecnologia THz può essere applicata a stand-off di rilevamento se si ha a disposizione una sorgente di elevata potenza. Punto controverso ancora non chiarito a livello mondiale è la sicurezza delle radiazioni Terahertz come potenziale rischio per la salute in applicazioni di controllo della persona o per il gestore del sistema. La questione è ancora in discussione a causa dei limiti esistenti da organizzazioni standard internazionali come ICNIRP, IEEE e ANSI che si basano solo su un'estrapolazione. Nonostante le peculiarità molto interessanti, solo un numero limitato di imprese commerciali sono disponibili sul mercato (Teraview, Picometrix, Emcore, diodi Virginia). In caso di sistemi passivi la Thruvision Systems Ltd nel Regno Unito è in grado di offrire di immagini nelle onde submillimetriche. Al contrario molti progetti nazionali e internazionali (UE + USA, Canada, Giappone e Cina) sono finanziati per promuovere questa tecnologia in Europa e particolarmente specialmente in Germania, Francia, Regno Unito ed in Italia.

Descrizione dei Gap tecnologici

Il componente più critico di un apparato Terahertz è la sorgente di radiazione. In linea di principio a questo elemento è richiesta una doppia funzione: alta potenza emessa e accordabilità in frequenza. A questa lista, è importante aggiungere anche impulsi di breve durata, bassa divergenza e facilità d'uso in applicazioni sul campo. La portabilità della sorgente inoltre costituirebbe nel futuro un'ulteriore caratteristica molto apprezzata. Nessuna delle tecnologie attuali (gyrotron, ondulatori, laser nel lontano infrarosso, laser a cascata quantica, laser ad elettroni liberi, fonti di luce di sincrotrone) possiede insieme tutte queste caratteristiche. Una situazione analoga si può trovare nei sistemi Terahertz passivi, dove solo una piccola impresa è in grado di offrire immagini submillimetriche. I sensori Terahertz costituiscono la seconda componente critica di questi apparati a causa della bassa potenza delle sorgenti THz a stato solido, che richiedono l'uso di sistemi bolometrici a raffreddamento con elio liquido o dispositivi simili. Dispositivi Terahertz a impulsi brevi hanno spesso bisogno di detector ad apertura temporale controllata (*gated*). I sensori Terahertz inoltre soffrono di una mancanza di componenti elettronici disponibili commercialmente, come resistori, condensatori e induttori, amplificatori e bassa perdita di trasmissione. Insiemi di rivelatori commerciali ottimizzati per Terahertz sono disponibili solo in versione prototipale. Lo sforzo tecnologico è tuttavia in costante aumento e società giapponesi, come la NEC, hanno recentemente introdotto nel mercato un prototipo di fotocamera THz.

Trend evolutivi

Vi è un forte interesse a livello mondiale nello sviluppo di questa tecnologia a causa di possibili vantaggi che si possono ottenere in diversi campi di applicazioni. Nella sicurezza, la capacità di passare attraverso i tessuti e successivamente indagare e discriminare le diverse minacce mediante l'impiego della spettroscopia, risultano molto attraenti. Se la modalità di funzionamento stand-off verrà raggiunta nel prossimo futuro, oltre alle capacità precedenti, è facile immaginare la possibile diffusione di questa tecnologia in siti sensibili inclusi i sistemi di trasporto di massa. Il doppio uso di questa tecnologia è evidente e tanto atteso per salvare la vita umana da attacchi terroristici (come nel caso degli attentatori suicidi). Per supportare questa evoluzione, diversi progetti di ricerca sono finanziati nel quadro di organizzazioni nazionali o internazionali, mentre le grandi imprese sono coinvolte nello sviluppo dei componenti di base. Altri settori importanti per i quali lo sviluppo Terahertz è essenziale sono la conservazione del patrimonio culturale e la tutela dell'ambiente. Per la Conservazione dei Beni Culturali, la tecnologia Terahertz ha già dimostrato la capacità di rivelare dipinti coperti da materiali di rivestimento murale come intonaco e materie simili o da patine invecchiate negli anni. Per l'ambiente, il monitoraggio a lungo raggio degli eventi di incendio nei boschi, o il movimento vicino ai vulcani di lava sono temi interessanti per alcune istituzioni nazionali e internazionali

Livello attuale di TRL TRL3

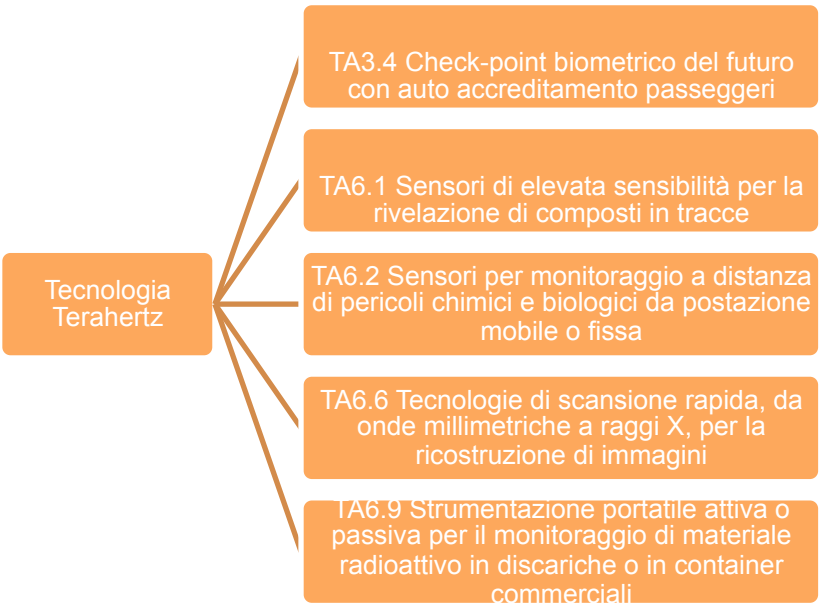
Step Necessari per arrivare a TRL + 1

Nuovi miglioramenti sono necessari per sviluppare componenti tecnologici di base come le sorgenti di radiazione, e i sensori elettronici associati.

Costo associato per arrivare a TRL +1 (anni ed investimento economico)

Il prossimo livello potrebbe essere raggiunto in tre anni, con un consistente piano di investimenti stimato nell'ordine di alcune centinaia di M€ a livello mondiale

I TA di riferimento TA1, TA2, TA4, TA5,TA7



- **Tecnologia Spettrometria a Mobilità Ionica**

Descrizione dello Stato dell'arte

La tecnologia Spettrometria a Mobilità Ionica (IMS) rappresenta attualmente lo stato dell'arte negli strumenti analitici per la caratterizzazione di sostanze chimiche. IMS è l'evoluzione della più nota HPLC (High-cromatografia liquida), già sviluppata negli anni '50. Nella tecnologia IMS, il campione in fase vapore viene iniettato, insieme ad un gas carrier tampone, in una zona di deviazione successivamente ionizzato. Gli sciami di ioni si muovono attraverso un gradiente di tensione applicato verso il detector che rivela i differenti coefficienti di mobilità. La sezione trasversale degli ioni quando colpiscono il rivelatore è legata alla dimensione e alla forma ionica. La tecnologia IMS ha dimostrato di essere in grado di effettuare una separazione rapida e veloce di una grande varietà di composti semi-volatili, quali gli agenti di guerra chimica, gli esplosivi o le droghe. In linea di principio la tecnologia IMS è veloce, a basso costo e sensibile a diversi composti. L'analisi può essere ottenuta in linea di principio, in meno di qualche centinaio di millisecondi. L'altro vantaggio di questa tecnologia è la possibilità di poter ottenere strumenti compatti dedicati. Anche se il principio è molto semplice, in pratica, l'obiettivo non è ancora completamente raggiunto. Le prime applicazioni di questa tecnologia sono state nel campo della sicurezza militare, nel rilevamento di materiali di contrabbando come droghe ed esplosivi. Oggigiorno IMS sta diventando uno strumento di analisi moderno ed innovativo. Più di 10.000 IMS sono impiegati negli aeroporti di tutto il mondo e più di 50.000 dispositivi IMS sono utilizzati nell'esercito americano (US Army). Strumenti IMS sono impiegati in medicina per l'analisi del cancro polmonare, delle sarcoidosi, degli scarti potenziali dopo il trapianto polmonare e delle relazioni con batteri all'interno del polmone. Attualmente il campo di applicazione di interesse è stato allargato anche al controllo di aree da dismettere, aree di prova attrezzate, o per rilasci tossici gassosi in eventi CBRNE. Nucleo del sistema è la camera di ionizzazione che può essere formata da una scarica a corona, per fotoionizzazione a pressione atmosferica, per ionizzazione a elettrospray, o da una sorgente radioattiva, per esempio ^{63}Ni o ^{241}Am, simile a quelli utilizzati nei rilevatori di fumo a ionizzazione. L'architettura più comune utilizzata per la rivelazione è il tempo di volo IMS (TOFIMS) dove il sistema misura la velocità che un dato ione, muovendosi in un campo elettrico uniforme, attraverso una fissata atmosfera. Alla fine una piastra di Faraday raccogliere gli ioni e misura la mobilità ionica. Molti progetti internazionali e comunitari di sicurezza sono dedicati per personalizzare le prestazioni IMS e l'aggiornamento alle richieste degli utenti finali.

Descrizione dei Gap tecnologici

Nonostante le caratteristiche interessanti (elevata selettiva, risposta veloce, compatto e trasportabile), l'affidabilità rimane un problema non pienamente raggiunto. La pulizia del dispositivo, il numero di misurazioni da eseguire di routine rappresentano ancora delle questioni aperte. L'ambiente in cui viene utilizzato lo strumento influenza fortemente i risultati finali (umidità, polvere, pollini). Il campionamento e la concentrazione dei componenti da analizzare è ancora un problema critico. Il limite di rilevabilità è determinato da come viene effettuato il campionamento. Diverse tecniche sono state applicate per il campionamento e per la concentrazione (corona, spugne organiche, ecc), ma devono essere ulteriormente migliorate per essere affidabili. La miniaturizzazione è ancora un problema da risolvere al fine di ottenere strumenti manuali portatili per lo screening del personale. da non sottovalutare il problema di utilizzare sorgenti a ionizzazione radioattiva che nel caso di rottura possono inquinare l'ambiente circostante.

Trend evolutivi

Diverse aziende industriali internazionali e dell'Unione europea sono coinvolte nello sviluppo della tecnologia IMS e alcune di loro con un forte indirizzo nel settore della sicurezza. La tendenza è di migliorare le prestazioni degli IMS e di aumentarne la loro sensibilità principalmente limitando la selettività molecolare in base allo scenario a cui si pensa di utilizzarlo. Molti progetti americani e della CE del 7 ° PQ sono stati finanziati per l'aggiornamento della tecnologia IMS.

Livello attuale di TRL TRL7

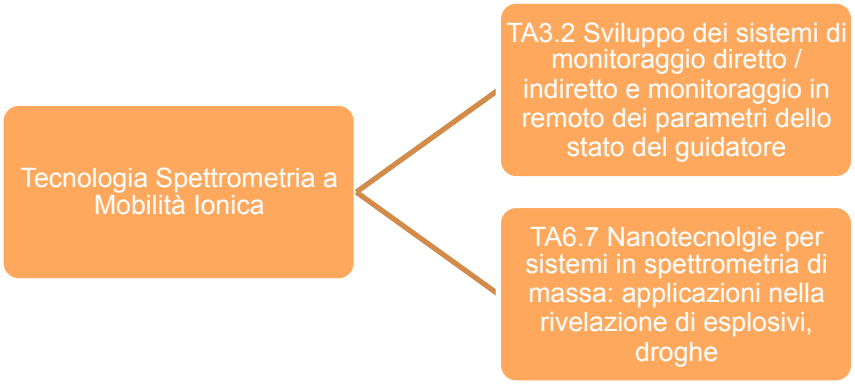
Step Necessari per arrivare a TRL + 1

La tecnologia IMS ha necessità di diventare sempre più conveniente e affidabile per poter lavorare nella sua forma definitiva e alle differenti condizioni previste in diversi scenari. I componenti interni devono essere selezionati nei COTS, al fine di ridurre i prezzi finali e per ottenere una vasta diffusione.

Costo associato per arrivare a TRL +1 (anni ed investimento economico)

Si presume un impegno di ricerca industriale tra tre e cinque anni con un investimento pari a centinaia di M€.

I TA di riferimento TA1, TA3, TA4, TA6



- **Sensor related imaging and mapping techniques**

Descrizione dello Stato dell'arte

Le metodologie e le tecniche di telerilevamento e diagnostica rappresentano importanti strumenti per la determinazione di parametri di rischio, assumendo un carattere ambivalente di interesse sia per la Safety (rischio legato ad eventi naturali e a difetti strutturali) che per la Security (eventi causati da comportamenti non leciti quali ad esempio quelli terroristici). Con riferimento agli edifici, alle strutture ed alle infrastrutture, la sicurezza va assicurata attraverso un monitoraggio regolare per il mantenimento in efficienza, per la prevenzione contro i rischi naturali (sismi, frane..) e antropici, e per la gestione di fasi di crisi e post crisi, conseguenza di attacchi terroristici e/o disastri naturali. Le tecnologie classiche prevedono prevalentemente campagne di misura operate con mezzi e strumenti di portatili con conseguentemente costi elevati, tempi di risposta variabili, un grado non trascurabile di invasività. e problematiche legate

a situazioni di difficoltà di accesso, pericolosità e interruzione delle normali condizioni di uso della struttura. Una risposta a queste necessità è fornita dalle tecniche di sensing, imaging e mapping, in particolare ti tipo acustico e/o elettromagnetico, operanti anche da remoto o installati in corrispondenza della struttura e operabili da remoto. Tra i sensori in situ sono d'interesse strumentazioni radar, senosri in fibra ottica, camere infrarossi ed ottiche, sensori iperspettrali, per il monitoraggio della superficie ed dello stato interno e del comportmaneto dinamico della struttura, che ben complementano generale gli usuali sensori di misurazione di parametri puntuali (temperatura, distanze, ecc). Negli ultimi anni si sono sviluppate anche tecnologie di sensing ed imaging remote utilizzate per prevalentemente per monitorare rischi associati a fenomeni naturali su aree estese a piccola scala. Un esempio in tal senso è fornito dai sensori di osservazione da satellite, ottici e a microonde. In particolare i sensori Radar ad Apertura Sintetica (SAR), come quelli della costellazione COSMO/Skymed he consentono misurazioni in ogni condizione metereologica, sia di notte che di giorno e quindi risultano particolarmente efficaci in termini di operatività in condizioni di crisi. In tale contesto assume un ruolo di rilevanza lo sviluppo di tecnologie SAR con sensori aviotrasportati che consentono di superare le limitazioni dei sensori satellitari in termini di tempo di rivisitazione e di flessibilità operativa. Riveste analoga importanza anche 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.

Descrizione dei Gap tecnologici

Con riferimento all'applicazione protezione di edifici, strutture ed infrastrutture in situazioni di crisi, i gap tecnologici legati alle tecniche di sensing ed imaging sono legati all'integrazione di differenti tecnologie di sensing (minimamente invasive) per un monitoraggio con diverse scale spaziali e temporali, multi risoluzione e multi profondità. Un sistema che integra differenti tecnologie di sensing ed imaging, consente di definire volta per volta la risposta idonea alla problematica da analizzare in funzione anche delle condizioni al contorno che determinano i gradi di accessibilità, l'estensione spaziale delle aree da monitorare, ecc, di notevole interesse per un "quick damage assessment". Accanto allo sviluppo delle singole tecnologie di sensing, un elemento importante è quindi anche lo sviluppo di metodologie di correlazione ed integrazione di tecniche di sensing, in funzione della loro complementarità e ridondanza delle grandezze misurate, anche al fine di determinare un protocollo di misura efficiente ed economicamente sostenibile. La messa a punto di un tale sistema richiede d'altro canto anche lo sviluppo di architetture avanzate basate su web-sensing e reti wireless e di sensori, e dall'altro, l'integrazione di tecniche di diagnostica non invasiva basata principalmente su sensing elettromagnetico e/o acustico.

Trend evolutivi

I trend evolutivi delle tecnche di imaging e sensing riguardano da un lato lo sviluppo e il miglioramento delle singole tecnologie che consentano di ottenere monitoraggi di diversi parametri (deformazione, temperatura, ecc) distribuiti e su ampie aree, a basso costo di realizzazione, di operatività e manutenzione, e dall'altro lo sviluppo di sistemi di sensing ed imaging integrati per un monitoraggio 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. In particolare, tale sistema di monitoraggio, oltre a "sorvegliare

e monitorare" la singola struttura, deve consentire anche di analizzare e misurare anche i parametri di contesto, come ad esempio il comportamento dinamico delle aree circostanti (movimenti franosi, movimenti tellurici, etc). Elementi fondamentali in tale processo di integrazione di sensori riguarda anche le problematiche di georeferenziazione e fusione di informazioni di grandezze misurate non necessariamente omogenee, e lo sviluppo di reti wireless e tecniche di websensing. Questi dati risultano decisivi ai fini dell'identificazione di modelli del comportamento che consentano di ridefinire velocemente i livelli di rischio.

Livello attuale di TRL TRL6

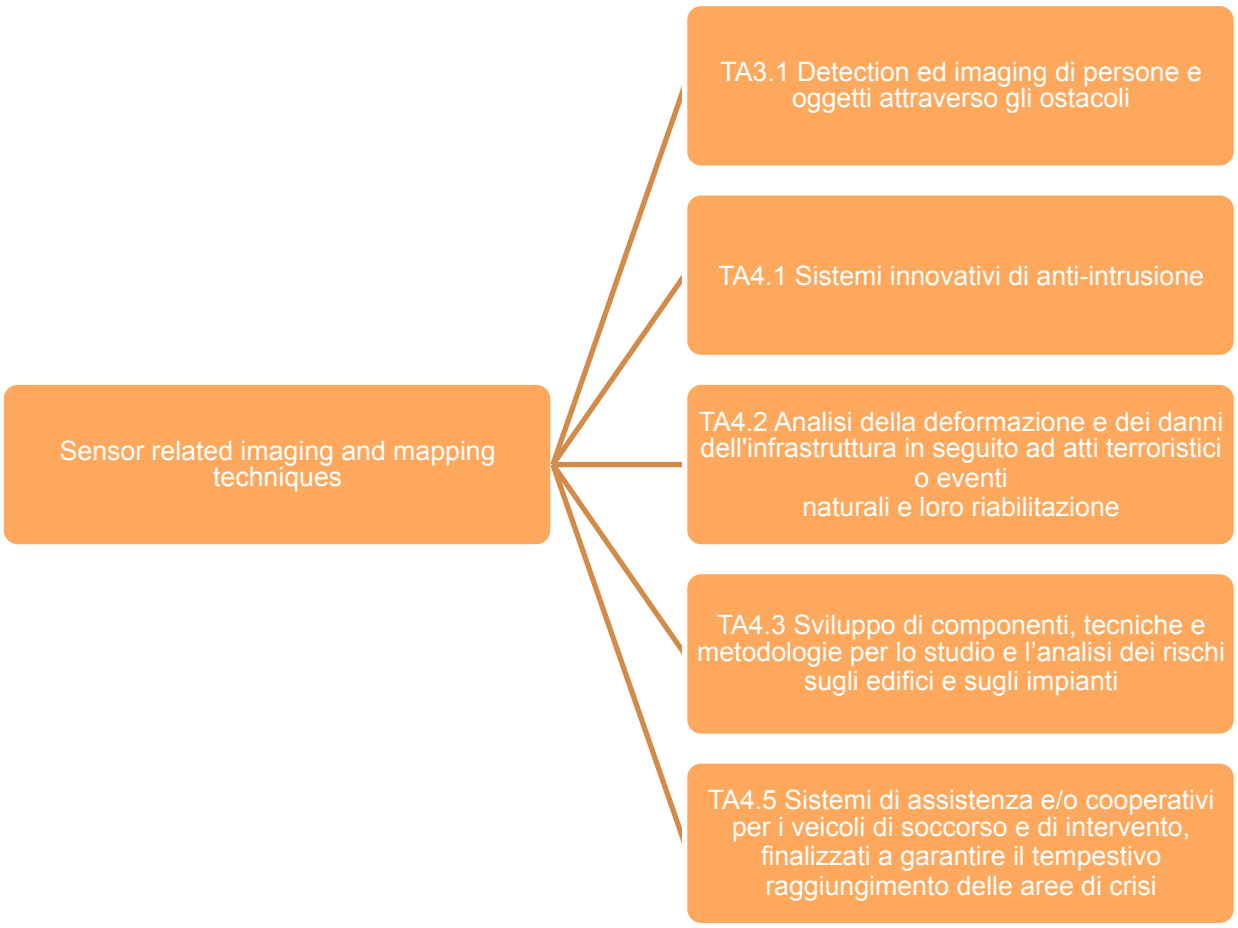
Step Necessari per arrivare a TRL + 1

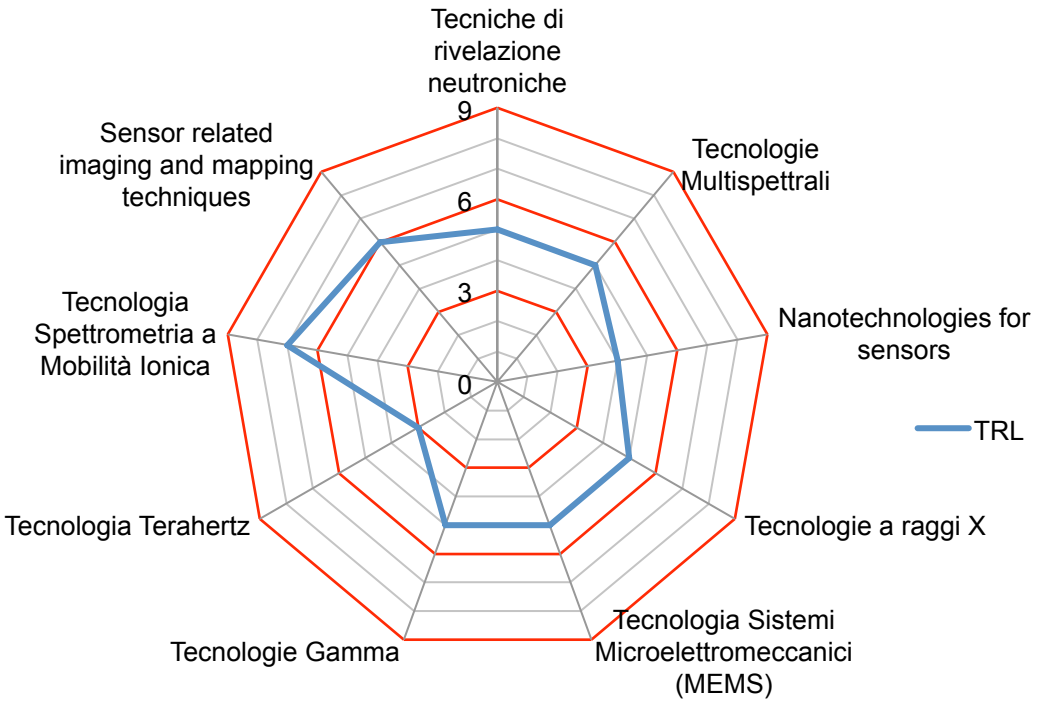
Per il raggiungimento del livello 7 (System prototype demonstration in an operational environment), è di cruciale importanza una forte interazione con il mondo degli end-users e quello industriale, capace di dettare i requisiti operativi ed economici dell'opzione tecnologica proposta.

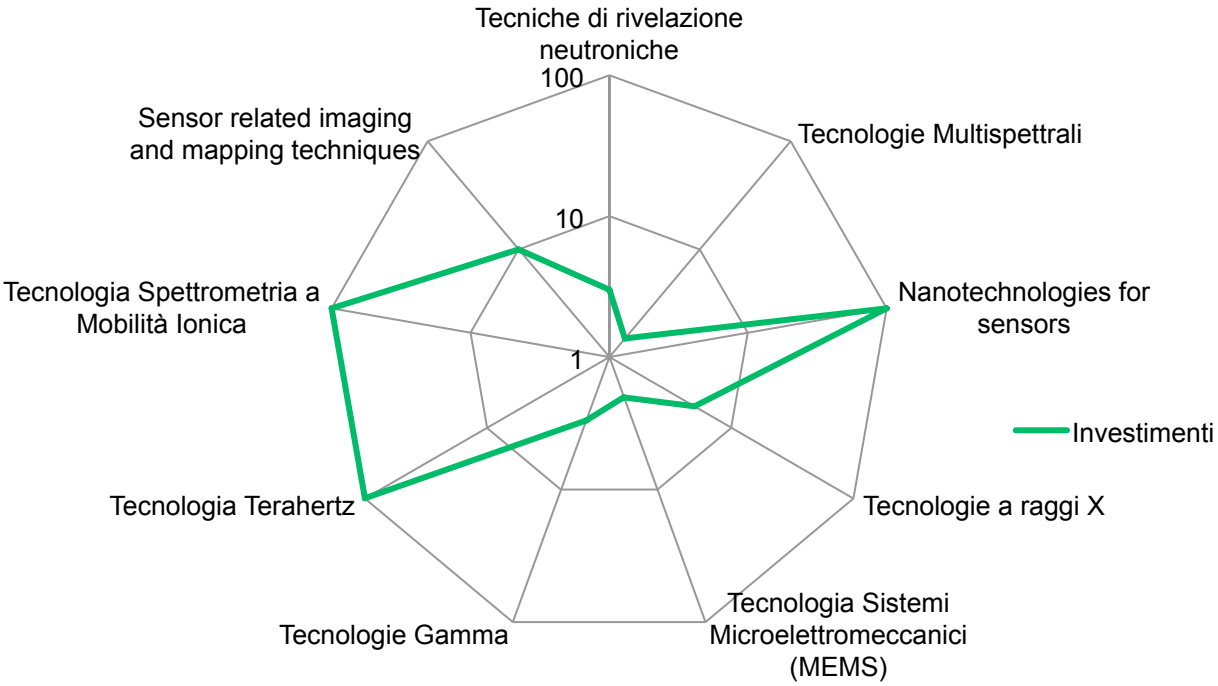
Costo associato per arrivare a TRL +1 (anni ed investimento economico)

3 anni e costo 10MEuro.

I TA di riferimento TA4




Tecniche di rivelazione neutroniche
9
6
3
0
Tecnologie Multispettrali
Nanotechnologies for sensors
Tecnologie a raggi X
Tecnologia Sistemi Microelettromeccanici (MEMS)
Tecnologie Gamma
Tecnologia Terahertz
Tecnologia Spettrometria a Mobilità Ionica
Sensor related imaging and mapping techniques
TRL


Tecniche di rivelazione neutroniche
100
10
1
Tecnologie Multispettrali
Nanotechnologies for sensors
Tecnologie a raggi X
Tecnologia Sistemi Microelettromeccanici (MEMS)
Tecnologie Gamma
Tecnologia Terahertz
Tecnologia Spettrometria a Mobilità Ionica
Sensor related imaging and mapping techniques
Investimenti

4.1.2 Information technologies Artificial Intelligence & Decision support

Ambiti prioritari di ricerca

- Tecnologia per l'elaborazione numerica di immagini e pattern (Re-identificazione)
- Data collection, classification & analysis
- Data Fusion
- Contextual Search Techniques
- Modeling and Simulation
- Knowledge Management

- **Tecnologia per l'elaborazione numerica di immagini e pattern - Re-identificazione**

Descrizione dello Stato dell'arte

La re-identificazione mira a riconoscere una persona quand'essa sia ripresa da differenti telecamere in differenti luoghi. La maggior parte degli approcci di re-identificazione (re-id) sono basati sulle caratteristiche esteriori delle persone (vestiti), e si possono suddividere in due classi: \ basati su addestramento e diretti. Nel primo caso, un insieme di dati viene suddiviso in due sottogruppi, di addestramento e di test, in cui il primo viene utilizzato per studiare le caratteristiche o le strategie migliori per il riconoscimento, e l'altro viene utilizzato per il test. Gli approcci diretti invece sono puramente estrattori di caratteristiche. Come metodi basati su addestramento, un insieme di caratteristiche e classificatori locali viene selezionato via boosting in [1]. In [2], viene studiata la dissimilarità tra coppie di immagini della stessa persona e applicata per la re-identificazione di nuove istanze. Similmente, in [3], la dissimilarità viene proiettata in uno spazio a bassa dimensionalità e modellata tramite Minimi Quadrati Parziali. In [4], la re-id viene modellata come un problema di ordinamento relativo in uno spazio ad alta dimensionalità. Come metodi diretti, in [5] viene proposto un metodo di estrazione e raggruppamento di caratteristiche locali, attraverso delle strutture grafiche a triangoli. In [6], caratteristiche locali di vario genere sono organizzate come matrici di covarianza. Principi di simmetria e asimmetria del corpo umano sono invece sfruttati in [7], utilizzando inoltre l'idea che caratteristiche più vicine agli assi di simmetria siano meno affette dal rumore. In [8], viene utilizzata un'analisi tramite epitomi per modellare gli aspetti più ricorrenti di una persona e condensarli in una rappresentazione visuale a bassa dimensionalità.

- [1] Douglas Gray and Hai Tao. Viewpoint invariant pedestrian recognition with an ensamble of localized features. ECCV, 2008.
- [2] Z. Lin and L.S. Davis. Learning pairwise dissimilarity profiles for appearance recognition in visual surveillance. ISVC, 2008.
- [3] W.R. Schwartz and L.S. Davis. Learning discriminative appearance-based models using partial least squares. SIBGRAPI 2009
- [4]Wei-Shi Zheng, Shaogang Gong, and Tao Xiang, "Person Re-identification by Probabilistic Relative Distance Comparison", CVPR, 2011
- [5] N. Gheissari, T. B. Sebastian, P. H. Tu, J. Rittscher, and R. Hartley. Person reidentification using spatiotemporal appearance. CVPR,2006.
- [6] X. Wang, G. Doretto, T. B. Sebastian, J. Rittscher, and P. H. Tu. Shape and appearance context modeling. ICCV, 2007.
- [7] M. Farenzena, L. Bazzani, A. Perina, V. Murino, and M. Cristani. Person reidentification by symmetry-driven accumulation of local features. CVPR, 2010.
- [8] Loris Bazzani, Marco Cristani, Alessandro Perina, Michela Farenzena, and Vittorio Murino. Multiple-shot person re-identification by hpe signature. ICPR, 2010.

Descrizione dei Gap tecnologici

Le tecniche di re-identificazione basate su aspetto esteriore si basano sul presupposto che le persone non si cambino d'abito durante il passaggio da una telecamera all'altra. Questo limita l'applicabilità'di queste tecniche a pochi casi, in cui il passaggio da una telecamera all'altra avvenga entro un breve periodo di tempo. Questo è in controtendenza rispetto a al paradigma di riconoscimento biometrico continuo che si sta sviluppando negli ultimi anni. D'altra parte, al

giorno d'oggi non sono presenti tecniche sostitutive all'analisi di caratteristiche esteriori dell'individuo, in grado di rispettare le norme vigenti di privacy

Trend evolutivi

Il trend evolutivo della re-identificazione mira a caratterizzare quindi un individuo tramite modelli in grado di catturare aspetti eterogenei di un essere umano, oltre alle sue caratteristiche esteriori. Si parla cioè di misure antropometriche (altezza, proporzioni) o comportamentali (segnali non verbali). Nel caso di caratteristiche esteriori, potrebbero essere considerate informazioni cromatiche e di tessitura, relative all'intero corpo o specifiche di parti quali braccia, torso, testa, gambe. Sono attualmente in corso di studio caratteristiche massimamente invarianti alle condizioni di acquisizione, per dare enfasi alla robustezza della caratterizzazione. Nel caso di caratteristiche antropometriche, sono attualmente in corso di studio misure soft-biometriche quali l'altezza di una persona e proporzioni anatomiche. In entrambe questi casi, i modelli generativi risultano particolarmente adatti, essendo in grado di gestire efficacemente il rumore di acquisizione. Nel caso di caratteristiche comportamentali (intese come sequenze di azioni e interazioni sociali), è attualmente in corso di studio l'utilizzo di segnali sociali per identificare quei tratti comportamentali maggiormente caratterizzanti, e allo stesso tempo evincibili da scenari reali. Più specificatamente, si stanno analizzando la tendenza alla socializzazione di una persona attraverso elementi di prossemica, di postura, di gestualità e di personalità.

Livello attuale di TRL TRL 2

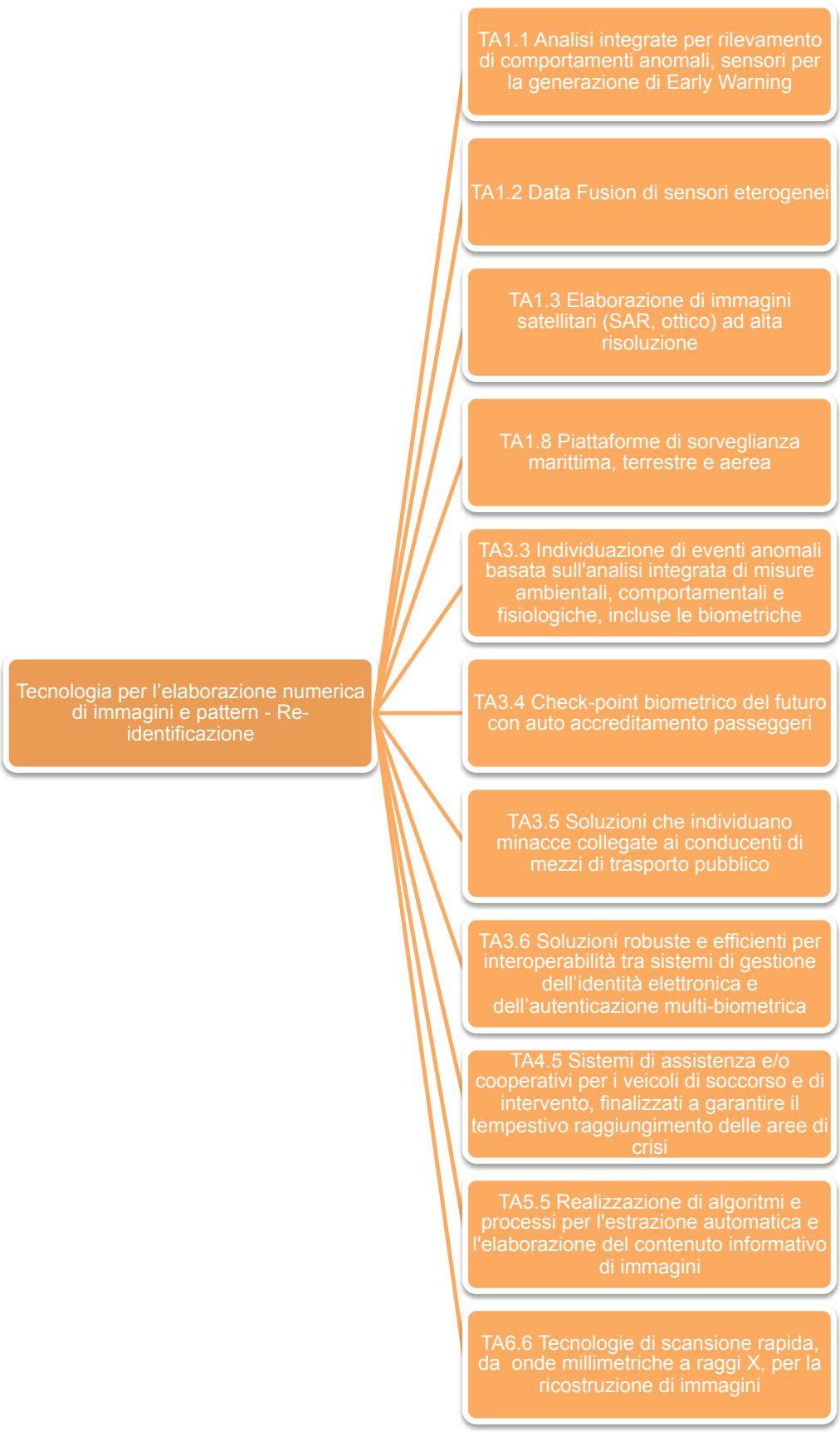
Step Necessari per arrivare a TRL + 1

È necessaria una fase di sviluppo di tecniche avanzate soft biometriche e comportamentali in grado di catturare l'identità di una persona senza considerare il suo aspetto esteriore

Costo associato per arrivare a TRL +1 (anni ed investimento economico)

1 anno

I TA di riferimento TA3


Tecnologia per l'elaborazione numerica di immagini e pattern - Re-identificazione
TA1.1 Analisi integrate per rilevamento di comportamenti anomali, sensori per la generazione di Early Warning
TA1.2 Data Fusion di sensori eterogenei
TA1.3 Elaborazione di immagini satellitari (SAR, ottico) ad alta risoluzione
TA1.8 Piattaforme di sorveglianza marittima, terrestre e aerea
TA3.3 Individuazione di eventi anomali basata sull'analisi integrata di misure ambientali, comportamentali e fisiologiche, incluse le biometriche
TA3.4 Check-point biometrico del futuro con auto accreditamento passeggeri
TA3.5 Soluzioni che individuano minacce collegate ai conducenti di mezzi di trasporto pubblico
TA3.6 Soluzioni robuste e efficienti per interoperabilità tra sistemi di gestione dell'identità elettronica e dell'autenticazione multi-biometrica
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
TA5.5 Realizzazione di algoritmi e processi per l'estrazione automatica e l'elaborazione del contenuto informativo di immagini
TA6.6 Tecnologie di scansione rapida, da onde millimetriche a raggi X, per la ricostruzione di immagini

- **Data collection, classification & analysis**

Descrizione dello Stato dell'arte

Con il termine Data Analysis s'intende il processo di sintetizzare e inferire valori da un insieme di dati. Gli obiettivi che si prefigge tale disciplina possono essere orientati alla loro esplorazione (ad esempio: individuazione di strutture interessanti e/o di valori anomali, sintesi dei dati, etc.), oppure alla conferma di alcune proprietà sui dati (ad esempio: determinare se un certo gruppo è differente da un altro, se un attributo cambia nel tempo, predire il valore di un certo attributo a partire da misure prese su altri attributi, etc.). Si può distinguere tra analisi descrittiva e inferenziale. La prima è orientata a indurre asserzioni specifiche sul data set che si sta esaminando. La seconda è orientata a cercare di trarre delle conclusioni che hanno una validità generale. La ricerca si focalizza sulla raccolta, la pre-elaborazione, la ricerca intelligente e il recupero automatico delle informazioni, e coinvolge il calcolo parallelo e distribuito, la scoperta e la gestione della conoscenza. Il processo di classificazione dei dati si può far ricadere nell'ambito dell'analisi intelligente dei dati. Gli strumenti adoperati nel "data analysis" interagiscono in maniera complessa tra di loro. In sostanza il "data analysis" è un processo iterativo che parte dai dati e, attraverso l'applicazione di algoritmi e tecniche specifiche, arriva alla partizione dei dati di partenza che vengono quindi riesaminati. L'evoluzione naturale del Data Analysis è l'Intelligent Data Analysis, che identifica un processo accuratamente pianificato e ponderato, coadiuvato da metodologie di Intelligenza Artificiale, che consente di supportare la scelta dei più opportuni strumenti, algoritmi e tecniche da adoperare per uno specifico problema, in cui soprattutto l'approccio statistico e il machine learning lavorano in sinergia per scoprire nuova conoscenza dai dati. Tra le metodologie principali per l'analisi intelligente dei dati annoveriamo la statistica classica, i metodi bayesiani, i support vector e i kernel methods, l'analisi di serie temporali, l'induzione di regole, le reti neurali, la logica fuzzy, i metodi di ricerca stocastica, le tecniche di analisi visuale dei dati , l'analisi intelligente di dati testuali basata su motori statistici e/o semantici, i repository semantici per l'immagazzinamento delle informazioni e l'interrogazione mediante linguaggi di query (es. SPARQL). Nello sviluppo di applicazioni nell'ambito della sicurezza, trovano sbocco, ad esempio, le metodologie di estrazione di mappe cartografiche a valore aggiunto multispaziali e multi temporali, la raccolta, la classificazione e l'analisi di dati meteorologici, dati delle reti geodetiche nazionali, dati satellitari, lo stream processing, lo sviluppo di moduli di raccolta ed elaborazione dei dati, gli algoritmi evolutivi, le architetture e algoritmi di signal processing, gli adaptable parsers per il monitoraggio di infrastrutture, le metodologie di text mining, audio e video analisi.

Descrizione dei Gap tecnologici

Le tecnologie e le metodologie attuali di raccolta, analisi e classificazione dei dati dovranno essere raffinate e specializzate, specialmente in un ambito critico come quello della sicurezza, a causa dell'incremento esponenziale dei dati, caratterizzati sempre più da dinamicità e da una continua evoluzione, che saranno disponibili negli anni a venire. Secondo recenti sudi, estrapolando dalle tendenze attuali, la produzione di dati potrebbe ipoteticamente raggiungere nei prossimi anni lo Yottabyte (10^{24}). A tal fine è necessario sviluppare ulteriormente la disciplina del Data Collection, Analysis and Classification: ad esempio avranno sempre più rilevanza gli approcci di filtraggio dei dati al fine di ridurre lo storage, gli algoritmi e le risorse di elaborazione, intese sia come hardware che software, al fine di rendere gestibile una tale quantità di dati, che può essere fonte preziosissima di informazioni, specialmente nell'ambito della sicurezza. Tutte

le attività che coinvolgono la sicurezza richiederanno la capacità di dedurre fatti in funzione della variazione di alcuni dati, caratterizzati dal fatto che essi fluiscono continuamente, velocemente, da sorgenti disparate e sono la maggior parte delle volte soggette a errori e incertezze, nonché affetti da ambiguità. In tale contesto gioca un ruolo fondamentale la ricerca interdisciplinare per l'analisi dei dati orientati alla sicurezza: tale paradigma consentirà di miscelare informazioni provenienti da video, audio, testo, sensori al fine di cooperare in sinergia realizzando sistemi che consentano l'incremento della sicurezza. Considerando lo sviluppo delle comunicazioni, di Internet e del Web in particolare, nell'ambito dell'analisi dei testi un gap da colmare sarà quello di realizzare motori semantici per applicazioni di text e audio mining, intercettare e analizzare le conversazioni e le interazioni tra soggetti e/o gruppi per individuare soggetti pericolosi a partire dall'interazione con altri soggetti e/o dall'appartenenza a gruppi, o anche a lanciare allarmi di varia natura.

Trend evolutivi

Poiché i dati a disposizione cresceranno sempre in maniera esponenziale, sarà molto importante assistere gli analisti durante il processo decisionale. Gli strumenti disponibili attualmente nello stato dell'arte sono utili a raggiungere tale scopo, tuttavia è necessario sviluppare metodologie e ricerche per sviluppare approcci che forniscano un'analisi profonda ed efficace dei dati.
I trend evolutivi saranno caratterizzati da:

- Sviluppo di sistemi di raccolta dati e sensori avanzati che supportino la piena comprensione dei fenomeni naturali e il riconoscimento di pericoli. I sensori dovranno diventare più accurati, affidabili e specifici;
- Miglioramento di modelli e tecniche di visualizzazione al fine di supportare la manipolazione dei dati e la previsione di scenari possibili;
- Sviluppo e miglioramento di algoritmi di machine learning per l'individuazione di anomalie nei dati;
- Sviluppo e miglioramento delle metodologie per la quantificazione dell'incertezza e l'analisi dell'errore, in maniera tale da fare delle predizioni e determinare incertezze per eventi rari;
- Sviluppo e miglioramento delle tecniche di text mining, basati anche sulla combinazione di motori statistici e semantici per migliorare il filtraggio e l'analisi del testo, finalizzate a individuare minacce possibili, gruppi o singoli individui pericolosi, particolarmente orientati all'analisi di forum, blog e microblogs, social networks, etc;
- Sviluppo di tecniche mirate di Web Crawling per l'individuazione di possibili minacce in base sia al contenuto informativo che alle modalità di gestione di fonti aperte (es: siti web);
- Sviluppo e miglioramento di modelli previsionali e di tecniche di visualizzazione informazioni precise e accurate;
- Miglioramento dei metodi di validazione di tali modelli.

Livello attuale di TRL

A seconda delle tecnologie il TRL è valutato a livello 3-4.

Step Necessari per arrivare a TRL + 1 (road-map)

<2013-2015> Sviluppo di tecniche innovative di feature extraction al fine di fare emergere

situazioni di potenziale pericolo per la sicurezza pubblica che vanno dal riconoscimento e localizzazione di gruppi di persone o di singoli soggetti socialmente pericolosi, alla scoperta di dinamiche comunicative che possano far pensare alla necessità di un monitoraggio a fini preventivi.

<2013-2015> Realizzazione di sistemi di monitoraggio specifici ed accurati al fine di identificare, descrivere, raccogliere, analizzare, e interpretare il sorgere di rischi chimici o biologici. Sviluppo di sistemi per l'individuazione in tempo reale di agenti contaminanti, sistemi di allarme e strumenti di analisi dei dati.

<2014-2016> Studio e messa a punto di sistemi software dotati di strumenti avanzati per l'analisi e la correlazione di ingenti quantità di dati provenienti da svariate sorgenti informative eterogenee, multicanali e multimodali.

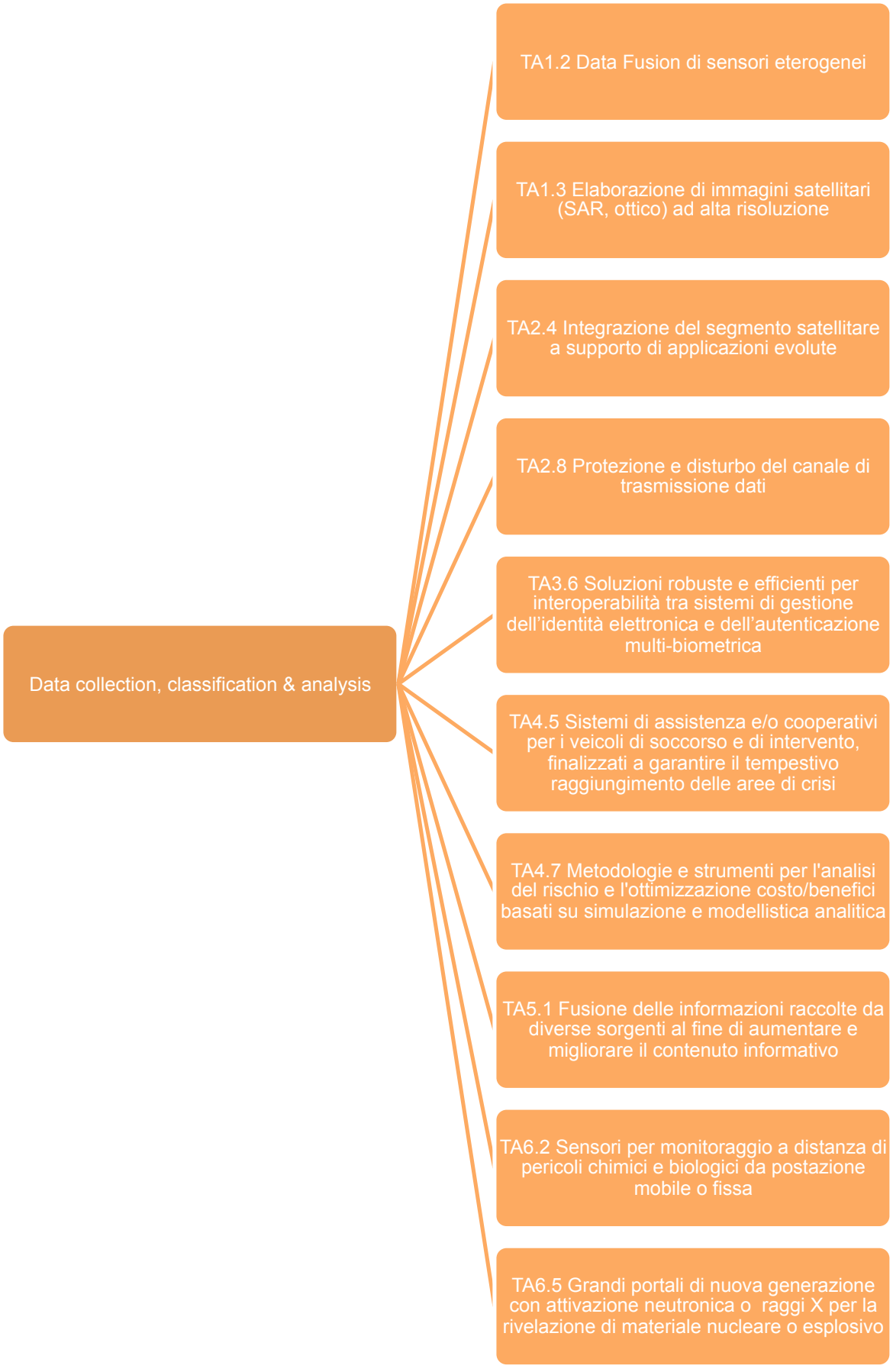
<2014-2016> Sviluppo di metodologie di Social Network Analysis al fine di analizzare e modellare il comportamento degli utenti sulla base delle loro connessioni o relazioni con altri componenti del gruppo.

<2014-2016> Realizzazione tecnologie e metodologie estremamente selettive, che forniscano le informazioni riguardanti possibili pericoli solamente dove e quando effettivamente necessario.

Costo associato per arrivare a TRL +1

Anni: 2,5
Investimento: 15 M€

TA di riferimento TA5


Data collection, classification & analysis
TA1.2 Data Fusion di sensori eterogenei
TA1.3 Elaborazione di immagini satellitari (SAR, ottico) ad alta risoluzione
TA2.4 Integrazione del segmento satellitare a supporto di applicazioni evolute
TA2.8 Protezione e disturbo del canale di trasmissione dati
TA3.6 Soluzioni robuste e efficienti per interoperabilità tra sistemi di gestione dell'identità elettronica e dell'autenticazione multi-biometrica
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
TA4.7 Metodologie e strumenti per l'analisi del rischio e l'ottimizzazione costo/benefici basati su simulazione e modellistica analitica
TA5.1 Fusione delle informazioni raccolte da diverse sorgenti al fine di aumentare e migliorare il contenuto informativo
TA6.2 Sensori per monitoraggio a distanza di pericoli chimici e biologici da postazione mobile o fissa
TA6.5 Grandi portali di nuova generazione con attivazione neutronica o raggi X per la rivelazione di materiale nucleare o esplosivo

- **Data Fusion**

Descrizione dello Stato dell'arte

Con data Data Fusion si indica il processo di combinazione di dati e informazioni provenienti da più sorgenti che ha lo scopo consentire una stima, di predire lo stato di un'entità, di inferire conoscenza sul mondo. L'importanza dei processi di data fusion può essere meglio compresa se si pensa alla capacità che caratterizza gli esseri umani di combinare in modo continuo i dati acquisiti per mezzo dei cinque sensi. Le informazioni acquisite vengono combinate e integrate nel tempo fra loro e con le informazioni presenti nella memoria umana. La ricerca sui problemi di data fusion ha visto il suo grande sviluppo in relazione ai dati multi sensore, trattando prima problemi di segnali unimodali e negli ultimi anni si sono affacciati i problemi di sensor fusion multimodale. La fusione dei dati è stata utilizzata per molti anni per molte applicazioni. Tradizionalmente, i dati da elaborare erano misure dei sensori senza restrizioni relative al tipo di applicazione. L'evoluzione tecnologica sta producendo la disponibilità di una crescente gamma di sensori di dispositivi mobili e con lo sviluppo di Internet di tecnologie che supportano la comunicazione globale. Problemi di fusione e combinazione dei dati emergono in numerose situazioni e le applicazioni sono:

- Applicazioni militari con il riconoscimento automatico degli obiettivi, guida per veicoli autonomi, sensing remoto, sorveglianza delle aree di battaglia e sistemi di riconoscimento automatico dei pericoli, focalizzandosi su problemi di localizzazione, caratterizzazione e identificazione di oggetti (unità militari, piattaforme e armi);
- Le applicazioni non militari includono sistemi di controllo automatico di processi industriali, mantenimento basato su condizioni di macchinari complessi, robotica e applicazioni per la sicurezza in contesti d'uso civile.

Va ricordato che la gamma di applicazioni ad uso civile sta crescendo di pari passo con la molteplicità di fonti di informazione, e con la tendenza crescente ad una condivisione delle informazioni globale. Questa tendenza, tuttavia pone problemi di fiducia e di accuratezza dell'informazione. I processi di data fusion devono pertanto combinare i dati fornendo strumenti di data mining che supportano l'utente nel reperimento delle informazioni e nella determinazione delle informazioni e dei dati affidabili e accurati. Fra le applicazioni ad uso civile i processi di data fusion hanno grande influenza sui metodi di human machine interaction. In particolare, l'uso combinato di più modalità nei processi di interazione può produrre un incremento della naturalezza. In questo caso il processo di fusione può coinvolgere approcci di tipo linguistico-grammaticale. Fra gli usi civili i processi di data fusion sono particolarmente importanti per applicazioni di security e antiterrorismo. tecniche di fusion, data mining e social network analysis, usando informazioni provenienti da sorgenti diverse (Internet, servizi segreti, dispositivi come cellulari o terminali di pagamento o sensori) possono contribuire ad incrementare la conoscenza delle attività pianificate da criminali e organizzazioni terroristiche al fine di produrre un atteggiamento proattivo rivolto a prevenire azioni criminose. Tra i metodi fino ad oggi utilizzati nei processi di data fusion vanno ricordati:

- Reti Bayesiane;
- Hidden Markov Models (HMMs);
- Gaussian Mixture Models (GMM);
- Approcci linguistici.

A questi vanno aggiunti i metodi e gli algoritmi di data mining. E di social network analysis.

Descrizione dei Gap tecnologici

Il gap tecnologico da superare è rappresentato dalla capacità di operare continuamente e in tempo reale operazioni rivolte a favorire la convergenza e la fusione dei dati e delle informazioni provenienti da sorgenti eterogenee (mondi reali e virtuali) al fine di favorire una lettura ed interpretazione corretta, non ambigua della realtà, per individuare le caratteristiche dei dati per applicazioni in materia di sicurezza.

Trend evolutivi

I trend evolutivi saranno caratterizzati da:

- Estensione del concetto di data fusion per una modellazione integrata di mondi virtuale e reale, con una potenziale convergenza multidisciplinare
- Sviluppo di modelli di rappresentazione di grandezze eterogenee e di relazioni fra queste in una visione evolutiva ed olistica.
- Sviluppo di algoritmi evolutivi e adattivi per la fusione dei dati.

Livello attuale di TRL

A seconda delle tecnologie il TRL è valutato a livello 3-4.

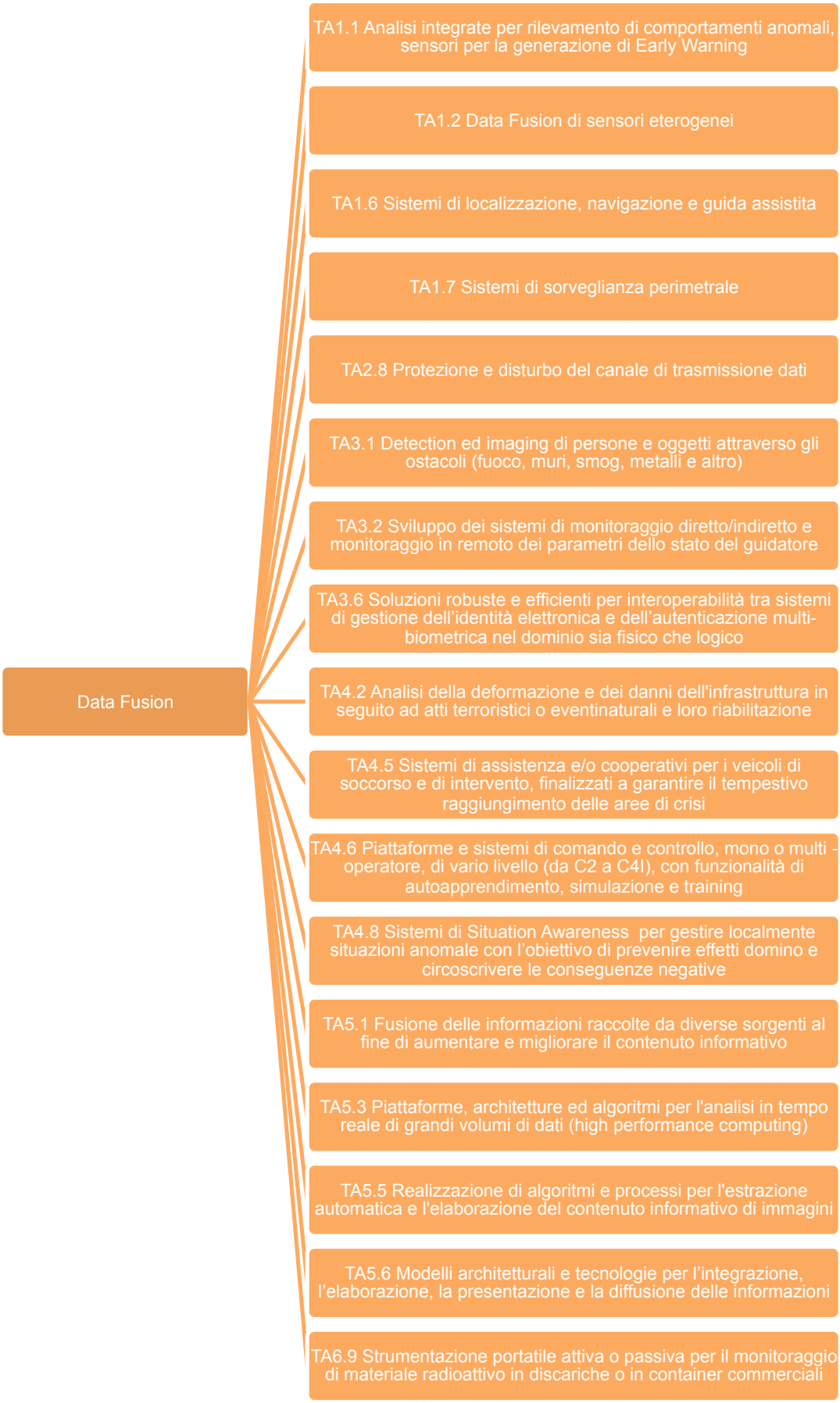
Step Necessari per arrivare a TRL + 1 (road-map)

<2013-2015>	Definizione di modelli di data fusion: per informazioni on-line, per informazioni provenienti da sensori e/o dispositivi mobili nel caso di informazioni modali e multimodali.
<2013-2015>	Definizione di modelli capaci di garantire l'accuratezza e l'affidabilità dei dati prodotti nei processi di data fusion.
<2014-2016>	Studio e definizione di metamodelli per il data fusion capaci di rappresentare (in un'ottica interdisciplinare) la dinamica degli oggetti e delle relazioni fra questi, siano essi sensori, entità virtuali o oggetti del mondo reale.
<2014-2016>	Studio e sviluppo di algoritmi evolutivi e adattivi ottenuti a partire dagli algoritmi esistenti, con un'analisi comparativa fra questi e algoritmi genetici e di tipo evolutionary per gestire la complessità di processi che nel data fusion ingloba-no processi di data mining e social network analisys .

Costo associato per arrivare a TRL +1

Anni: 2,5
Investimento: 10 M€

TA di riferimento TA5


Data Fusion
TA1.1 Analisi integrate per rilevamento di comportamenti anomali, sensori per la generazione di Early Warning
TA1.2 Data Fusion di sensori eterogenei
TA1.6 Sistemi di localizzazione, navigazione e guida assistita
TA1.7 Sistemi di sorveglianza perimetrale
TA2.8 Protezione e disturbo del canale di trasmissione dati
TA3.1 Detection ed imaging di persone e oggetti attraverso gli ostacoli (fuoco, muri, smog, metalli e altro)
TA3.2 Sviluppo dei sistemi di monitoraggio diretto/indiretto e monitoraggio in remoto dei parametri dello stato del guidatore
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
TA4.2 Analisi della deformazione e dei danni dell'infrastruttura in seguito ad atti terroristici o eventinaturali e loro riabilitazione
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
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
TA4.8 Sistemi di Situation Awareness per gestire localmente situazioni anomale con l'obiettivo di prevenire effetti domino e circoscrivere le conseguenze negative
TA5.1 Fusione delle informazioni raccolte da diverse sorgenti al fine di aumentare e migliorare il contenuto informativo
TA5.3 Piattaforme, architetture ed algoritmi per l'analisi in tempo reale di grandi volumi di dati (high performance computing)
TA5.5 Realizzazione di algoritmi e processi per l'estrazione automatica e l'elaborazione del contenuto informativo di immagini
TA5.6 Modelli architetturali e tecnologie per l'integrazione, l'elaborazione, la presentazione e la diffusione delle informazioni
TA6.9 Strumentazione portatile attiva o passiva per il monitoraggio di materiale radioattivo in discariche o in container commerciali

- **Contextual Search Techniques**

Descrizione dello Stato dell'arte

Si definisce Contextual Search la ricerca di documenti basata sull'intero loro contenuto, testuale ma potenzialmente anche multimediale, anziché sulla sola corrispondenza con i termini chiave di una ricerca. Ne fa parte anche il contesto della domanda, cioè il significato di una frase chiave di ricerca. La ricerca contestuale, rispetto a quella per parole chiave, è suscettibile di restituire un numero inferiore di risultati, ma più significativi rispetto alle intenzioni della ricerca stessa. La Contextual Search è fondamentale non solo per le classiche ricerche su Web, ma anche per ricerche specializzate, gestione di archivi, intelligence e altre applicazioni di gestione della conoscenza. Il cosiddetto "Web 1.0" era la "rete delle informazioni", abbastanza ben supportata dalla ricerca per parole chiave. Il "Web 2.0" è la "rete delle persone", arricchita dalle relazioni fra individui. Il "Web 3.0" sarà la "rete delle cose", in grado di riflettere la gestione virtualizzata del mondo che ci circonda; alle parole chiave e relazioni fra persone dovrà associarsi la descrizione concettuale della realtà, secondo i diversi linguaggi, culture e specializzazioni. Lo stato dell'arte si può riassumere in una serie di standard, in particolare promossi dal W3C, che preparano la descrizione contestualizzata delle informazioni aperte, e in alcune tecnologie che supportano la classificazione di contenuti testuali sia sul lato delle ricerche, sia su quello dei documenti da ricercare. XML, con i linguaggi descrittivi derivati, e più in generale i linguaggi associativi come RDF, sono un fondamento per il tagging delle informazioni e la loro descrizione strutturata. La tecnologia fondamentale è quella dei motori di ricerca, mentre altre tecnologie aiutano l'automazione della Contextual Search pur non essendone specifiche; fra queste ricordiamo:

- Text Processing (identificazione concetti per isolamento dei gruppi di parole rilevanti);
- Language Processing (identificazione concetti per analisi grammaticale, logica e lessicale);
- Document Processing e Classification (aggregazione e ordinamento di documenti attraverso indexing manuale e automatico);
- Taxonomy, Ontology Processing (rappresentazione e elaborazione di concetti strutturati);
- Knowdedge Management (gestione archivi documentali orientati alla descrizione della conoscenza e ai servizi di ricerca, navigazione e condivisione);
- Query Auto-Completion (varie tecniche, dai grandi motori di ricerca ai dispositivi embedded, come navigatori e cellulari, per interpretare e completare le interrogazioni in base al contesto delle domande precedenti e ai dizionari).

Descrizione dei Gap tecnologici

I principali gap tecnologici investono alcune delle tecniche a supporto:

- *Language e semantic processing:* gli approcci correnti sono poco generali rispetto alla molteplicità dei linguaggi, con le rispettive culture e forme idiomatiche; è difficile mantenere aggiornati dizionari, tassonomie e regole di descrizione, rispetto a linguaggi e culture in evoluzione;
- *Clusterization*: molti algoritmi sono disponibili per aggregare induttivamente i documenti in base ai contenuti, ma occorre aumentare il grado di comprensione e sintesi del significato delle aggregazioni ottenute;
- *Indicizzazione*: manca un ragionevole approccio di compromesso fra la crescita degli indici

e le prestazioni delle ricerche contestuali;
- *Ontology processing*: sono ancora insufficienti gli standard e gli algoritmi per far interoperare ontologie diverse, verificando coerenza e completezza dei risultati; mancano inoltre strumenti user-friendly per definire e modificare ontologie senza essere esperti dei linguaggi specializzati (ontologie dinamiche);
- *Scalabilità*: occorre che gli strumenti di indicizzazione e ricerca possano adeguarsi alla mole di informazioni da processare, federandosi in strutture distribuite e flessibili, e sfruttando l'evoluzione dell'ICT verso il Cloud computing;
- *Deducting vs. Inductive Knowledge*: mancano ad oggi elementi per scegliere fra gli approcci a regole, deduttivi alla rappresentazione della conoscenza (definizione di ontologie, regole, algoritmi espliciti) e quelli statistici, induttivi (costruzione della conoscenza a partire dai contenuti).

Trend evolutivi

I trend evolutivi saranno caratterizzati da:

- Sviluppo e federazione di modelli formali (o ontologie) con una semantica esplicita per annotare le risorse nel Semantic Web, tenendo conto di diversi contesti linguistici e culturali;
- Ulteriore standardizzazione di interoperabilità per servizi distribuiti di indicizzazione e ricerca semantica, che permetta di condividere risorse e conoscenze. Un approccio centralizzato al Semantic Web, come per es. il motore Google per l'indicizzazione chiave, non è praticabile;
- Crescita e diffusione degli approcci statistici / induttivi alla classificazione di linguaggi e documenti. Richiedono più risorse di elaborazione rispetto agli approcci a regole, ma alla lunga risulteranno più praticabili (es. come già oggi per la traduzione automatica);
- Miglioramento delle interfacce HCI verso rappresentazioni navigabili delle basi di conoscenza e dei risultati delle ricerche. In parallelo agli algoritmi di graph processing, indispensabili per caratterizzare la topologia delle basi di conoscenza e presentarla in modo sintetico agli analisti, anche a scopo di reportistica.

Livello attuale di TRL

Il TRL è valutato, relativamente alle principali tecnologie abilitanti, tra il livello 5 ed il 6.

Step Necessari per arrivare a TRL + 1 (road-map)

Il raggiungimento dell'obiettivo di riduzione dei gap tecnologici richiede l'esecuzione coordinata di una serie di attività di ricerca.

<2013-2015> Arricchimento e perfezionamento di modelli condivisi di rappresentazione della conoscenza, sia sul lato della ricerca sia su quello delle basi documentali.

<2013-2015> Definizione di approcci alla federazione dei motori di indicizzazione e ricerca, affiancando i motori tradizionali (generalisti e poco specializzati) con nuovi motori semantici (per specifiche basi documentali e conoscenze).

<2013-2016> Miglioramento delle tecnologie di base a diversi livelli architetturali: processing del testo – processing della semantica – processing degli elementi concettuali, loro indicizzazione – processing della rete di elementi verso una situa-

zione conosciuta, sua modellizzazione ontologica – sintesi della conoscenza e reportistica dei risultati

<2013 - 2016> Federazione di tecnologie di base e realizzazione di servizi dimostrativi per motori di ricerca e analisi contestuale, sia su Web che su specifiche basi documentali. Adeguamento e misura di indici di qualità dell'informazione semantica e rilevanza dei risultati di analisi contestuale.

Costo associato per arrivare a TRL +1

Anni: 3

Investimento: ~ 15 M€

TA di riferimento TA3

- **Modeling and Simulation**

Descrizione dello Stato dell'arte

Modellistica e Simulazione (M&S) si è dimostrata estremamente interessante come rapporto costo/beneficio per l'addestramento del personale civile e militare coinvolto nelle operazioni di reazione alla crisi e per la dimostrazione dell'impiego di nuove tecnologie. In questo contesto, l'enfasi è attualmente nella rappresentazione, riccamente grafica, dell'interazione di molteplici soggetti (persone o mezzi) all'interno di una realtà virtuale che replica in dettaglio le caratteristiche operative del territorio, includendo vie di comunicazione, folla, diffusione di nubi tossiche, meteo, etc. Notevole dispendio di energie è stato dedicato alla costruzione di sistemi hardware e software che simulano il più fedelmente possibile le reali condizioni operative dell'addestrato, prevedendo anche lo sviluppo temporale di scenari pilotati in linea da istruttori che, accedendo in tempo reale al sistema, possono evocare incidenti, malfunzionamenti, o far capitare eventi addizionali che complicano o disturbano la reazione alla crisi principale.

Descrizione dei Gap tecnologici

Mentre l'aspetto di interazione fra agenti simulati e di resa grafica degli eventi è stato abbondantemente indirizzato dalla tecnologia esistente, con lo sviluppo di standard di comunicazione locali e geografici, è stata finora meno efficacemente considerato l'approccio di simulazione stocastica su grandi numeri di scenari, e la conseguente analisi statistica dei risultati ottenuti, al fine di proporre al decisore criteri oggettivabili di scelta sull'allocazione delle risorse. In altre parole, l'aspetto di simulazione dinamica di una singola realizzazione tra le infinite situazioni possibili è prevalso finora rispetto all'analisi quantitativa della resa media delle strategie adottate su grandi numeri di realizzazioni.

Trend evolutivi

Esiste un chiaro e progressivo spostamento della filosofia di M&S a includere, oltre a elementi ingegneristici di sempre maggior complessità e integrazione, anche elementi matematico-statistici che offrono i metodi per garantire la correttezza e la possibilità di estrapolazione dei risultati ottenuti per simulazione.

Livello attuale di TRL TRL5

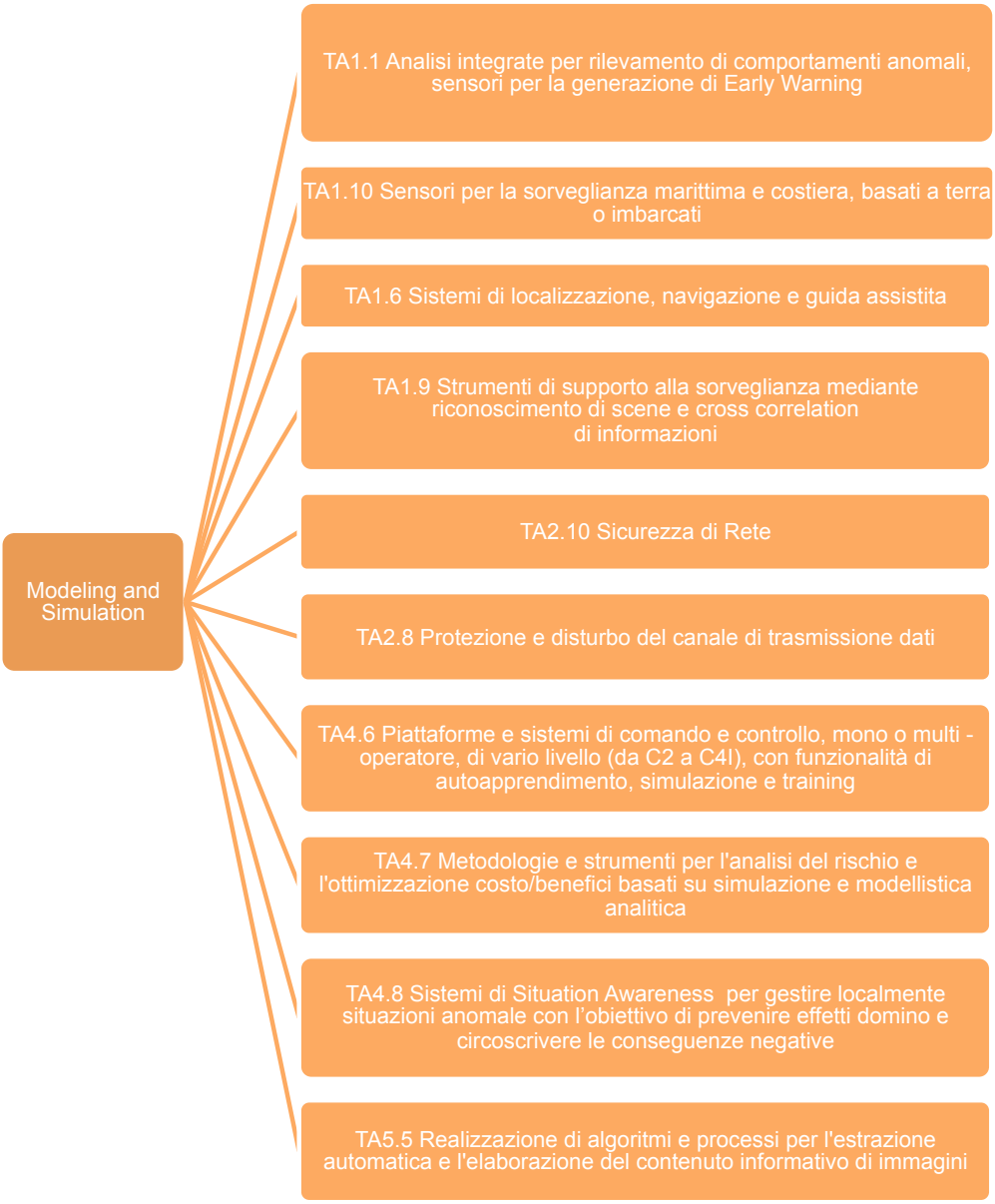
Step Necessari per arrivare a TRL + 1

- Maggiore integrazione tra le differenti discipline interessate;
- Modelli matematici applicati a scenari di crisis management;
- Strumenti software di analisi degli scenari e dei rischi mirati a creare le premesse per minimizzare effetti negativi di eventi complessi;
- Strumenti per l'integrazione sul territorio di un siffatto approccio;
- Formulazione di protocolli europei comuni di gestione del crisis management.

Costo associato per arrivare a TRL +1 (anni ed investimento economico)

Dai 2 ai 4 anni
dai 3 ai 5 milioni di Euro

I TA di riferimento TA4



- **Knowledge Management**

Descrizione dello Stato dell'arte

Knowledge management è un settore di ricerca teorica e applicativa che riguarda la gestione delle conoscenze esplicite ed implicite all'interno di una comunità di pratica o d'apprendimento tramite strumenti dell'information technology. Uno dei più recenti approcci alla modellizzazione della conoscenza è l'ontologia formale. Una ontologia è una specifica esplicita, formale di una concettualizzazione condivisa. Una ontologia può essere definita come una:

- Disciplina filosofica;
- Specifica di una concettualizzazione;
- Sistema concettuale informale;
- Descrizione semantica formale;
- Rappresentazione di un sistema concettuale attraverso una teoria logica;
- Vocabolario utilizzato da una teoria logica;
- Specifica o meta-livello di una teoria logica.

Dove la prima definizione fornisce utili linee guida, mentre, le tre successive danno una definizione al livello di conoscenza e le ultime tre forniscono una definizione al livello simbolico.
Nella rappresentazione delle ontologie esistono differenti gradi di formalismo come segue:

- *Highly informal* espressa in linguaggio naturale;
- *Semi-informal* espressa in una forma ristretta e strutturata del linguaggio naturale;
- *Semi-formal* espressa in un linguaggio artificiale formalmente definito;
- *Rigorously-formal* termini precisamente definiti con semantica formale, teoremi e verifica delle proprietà desiderate.

Esistono differenti tipi di ontologie che sono:

- *Top-level ontologies* in cui vengono definiti i concetti molto generali e sono indipendenti dal dominio;
- *Domain ontologies* o vocabolario relativo ad un determinato dominio (tipo, sicurezza, medicina);
- *Task ontologies* che sono vocabolario relativo ad un determinato task o attività (per esempio, emergenza, diagnostica)
- *Application ontologies* che integra la conoscenza proveniente da domain e task ontologies ed è una specializzazione di entrambi.

L'integrazione di ontologie è il processo per trovare elementi comuni tra due diverse ontologie, ottenendone una terza che faciliti l'interoperabilità tra i sistemi di computer basati sulle ontologie originarie. I livelli di integrazione possono essere distinti in:

- *Alineamento* è la forma più "debole" di integrazione e richiede cambiamenti minimi. Esso è utile per la classificazione ed il recupero delle informazioni;
- *Compatibilità parziale* richiede più cambiamenti per supportare maggiore interoperabilità;
- *Compatibilità totale (fusione o unificazione)* può richiedere grandi cambiamenti nelle ontolo-

gie attraverso una maggiore riorganizzazione che consente di ottenere la più completa interoperabilità.

Gli strumenti per la gestione delle ontologie vengono classificati in strumenti per lo sviluppo delle ontologie (per esempio OILEd, OntoEdit, Protégé, WebODE) e strumenti per l'integrazione e la fusione delle ontologie (per esempio, Chimaera, PROMPT, ODEMerge, FCA-Merge). Le ontologie permettono di far fronte a rappresentazioni eterogenee delle risorse web, fornendo una comprensione comune circa un dominio che puo essere condiviso da persone e strumenti software. Il Resource Description Framework (RDF) e un framework per la descrizione della conoscenza nel Web. Esso è stato creato, secondo una raccomandazione del W3C[10], per la descrizione dei metadati relativi alle risorse. OWL- Web Ontology Language è lo standard attualmente proposto dal W3C per la definizione di ontologie per il Semantic Web.

Descrizione dei Gap tecnologici

I principali gap tecnologici sono rappresentati da:

- *Interoperabilità semantica*: grado di facilità con cui è possibile scambiare ontologie per un'applicazione. È necessario che tool diversi interpretino le stesse cose nello stesso modo;
- *Performance*: tempo necessario per risolvere uno specifico task inferenziale (es. memorizzare ontologie di riferimento standard). Nella valutazione della performance è necessario disporre di benchmarks per analizzare la copertura, precisione, sostenibilità, flessibilità di una ontologia;
- *Scalabilità*: la performance ed il comportamento del tool rispetto alla memoria, in funzione dell'aumento della dimensione dell'ontologia;;
- *Memory allocation*: memoria necessaria al tool per gestire ontologie;
- *Integrazione in un framework*: la facilità di usare il tool in ambienti diversi;
- *Connettività*: capacità di collegarsi con altri tool (database, index servers, MS systems, Lotus Notes, etc);
- *Consistenza*: rispetto alla propria semantica. La valutazione della consistenza esprime quanto il tool sia capace di creare ontologie consistenti rispetto alla propria semantica, ovvero deve verificarsi che diverse parti di una ontologia non siano in contraddizione.

Trend evolutivi

I trend evolutivi saranno caratterizzati da:

- Sviluppo di modelli formali (o ontologie) con una semantica esplicita per annotare le risorse nel Semantic Web, in cui l'obiettivo è descrivere il contenuto delle risorse annotandole con informazione non ambigua per supportarne l'uso da parte di agenti intelligenti;
- Incremento nell'interazione delle applicazioni industriali con formati standard contestualmente accettati e con rappresentazioni formati in modo tale che le annotazioni possano essere create, sviluppate, mantenute da utenti diversi, siano esseri umani o agenti intelligenti. (Attualmente, RDF(S) o OWL sono usati come linguaggi formali per produrre annotazioni.);
- Gestione semantica di web services attraverso ontologie che permettano agli sviluppa-

tori ed amministratori di servizi web di predire ed osservare completamente come più servizi web si comportano, interagiscono, o possono entrare in conflitto;
- Sviluppo di approcci di supporto al Software Engineering per modellare i domini in maniera formale o semiformale che permettano: la specificazione del sistema in maniera indipendente dalla piattaforma su cui alla fine sarà sviluppato ed il supporto alla trasformazione delle specifiche di un sistema in specifiche per lo sviluppo in particolari piattaforme;
- Incremento della scalabilità e della compatibilità delle componenti nel Software Engineering attraverso l'impiego delle tecnologie del Semantic Web (metadati, ontologie formali e linguaggi) che supportano la rappresentazione non ambigua della terminologia di dominio, permettono il controllo automatico della consistenza e validazione delle regole (pre-condizioni e post-condizioni) e supportano la mediazione e trasformazione della terminologia basata su conoscenza;

Livello attuale di TRL

A seconda delle tecnologie il TRL è valutato a livello 3-4.

Step Necessari per arrivare a TRL + 1 (road-map)

<2013-2015> Studio, definizione e sviluppo di ontologie o modelli formali con una semantica esplicita per annotare (in modo automatico o semi-automatico) le risorse nel Semantic Web, per la condivisione e lo scambio di informazioni tra agenzie nel campo della sicurezza.

<2013-2015> Definizione di standard nelle rappresentazioni formali in modo tale che le conoscenze, modellate attraverso ontologie, possano essere create, sviluppate, mantenute da utenti diversi (umani o agenti intelligenti) nel campo della sicurezza.

<2014-2016> Studio, definizione e gestione semantica di web services che permettano agli sviluppatori ed amministratori di servizi web di predire ed osservare come più servizi web si comportano, interagiscono o possono entrare in conflitto.

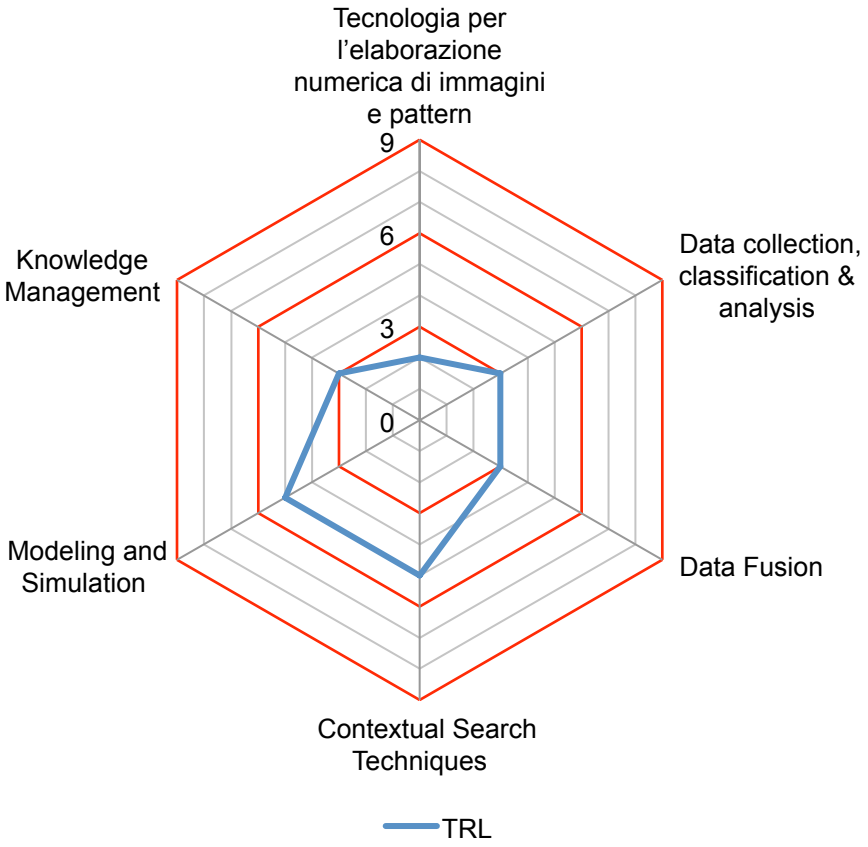
<2014-2016> Studio, definizione e sviluppo di ontologie come supporto al Software Engineering per modellare i domini di interesse nel campo della sicurezza in maniera formale o semiformale che permettano la specificazione del sistema in maniera indipendente dalla piattaforma su cui alla fine sarà sviluppato ed il supporto alla trasformazione delle specifiche di un sistema in specifiche per lo sviluppo in particolari piattaforme.

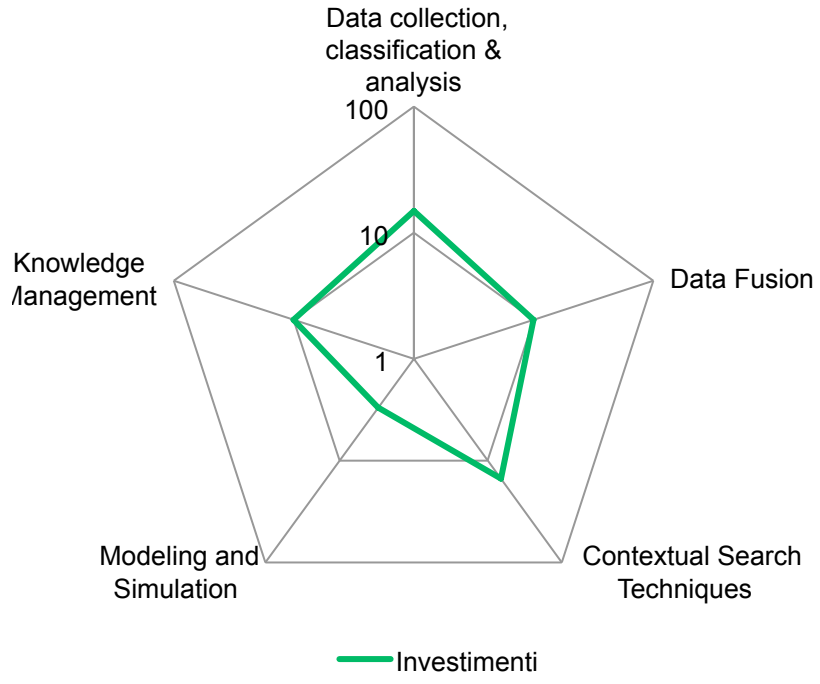
<2014-2016> Studio, definizione e sviluppo di tecnologie del Semantic Web, in particolare le ontologie, per incrementare la scalabilità e la compatibilità delle componenti in Software Engineering.

Costo associato per arrivare a TRL +1

Anni: 2,5
Investimento: ~ 10 M€

TA di riferimento TA5


Tecnologia per l'elaborazione numerica di immagini e pattern
9
6
3
0
Data collection, classification & analysis
Data Fusion
Contextual Search Techniques
Modeling and Simulation
Knowledge Management
TRL


Data collection, classification & analysis
100
10
1
Data Fusion
Contextual Search Techniques
Modeling and Simulation
Knowledge Management
Investimenti

4.1.3 Computing & Information Security Technologies

Ambiti prioritari di ricerca

- Cloud Computing
- Architetture Software
- Resilienza e Qualità del Servizio (QoS) dei Sistemi di Controllo Industriali
- High Performance Computing, Hybrid Computing
- IT Authentication technologies
- Intrusion detection technologie

- **Cloud Computing**

Descrizione dello Stato dell'arte

Più che una tecnologia in senso stretto, il cloud computing è una nuova modalità di fruizione, commitment-free e on-demand, di tecnologie e servizi - di calcolo, memorizzazione e connettività - già esistenti. Il nuovo modello di business introdotto dal cloud computing sta trovando terreno fertile, con investimenti massicci a livello globale e previsioni da parte di organismi indipendenti di crescita vertiginosa nei prossimi anni. Per le sue potenzialità in termini di riduzione dei costi (soprattutto di acquisizione ma anche di gestione), una migrazione verso il cloud computing è estremamente attraente, soprattutto per le Piccole e Medie Imprese (PMI). Le istituzioni governative e la pubblica amministrazione guardano con interesse alla possibilità di adozione del paradigma cloud per ridurre i costi e al tempo stesso aumentare le capacità delle loro infrastrutture ICT. Per esempio, la GSA (General Services Administration) del governo degli Stati Uniti offre già un portale per servizi di cloud computing. Sia i governi che le aziende sono tuttavia estremamente preoccupati degli aspetti di sicurezza legati all'utilizzo del cloud computing. In particolare, i governi hanno serie difficoltà a far percepire al pubblico che l'elaborazione di informazioni personali dei cittadini in infrastrutture cloud è sicura (almeno) quanto quella fatta utilizzando sistemi di tipo tradizionale. A complicare ulteriormente la vicenda contribuisce anche una serie di ostacoli legali e normativi, che di fatto impediscono a molti governi di adottare il cloud computing come paradigma ufficiale, anche se - sia i governi che le aziende - si rendono conto che molti dei loro impiegati fanno uso di servizi cloud-based sebbene ciò non rientri nelle loro policy ufficiali. Affinché il cloud computing possa realizzare appieno le proprie potenzialità è necessario che fornisca meccanismi affidabili di sicurezza dell'informazione. Infine, è importante notare che il cloud computing fa riferimento a delle tipologie di servizi differenti e precisamente: Software as a Service (SaaS), Platform as a Service (PaaS) e Infrastructure as a Service (IaaS). I rischi in termini di sicurezza associati a ciascuna di tali tipologie differiscono talvolta in maniera sostanziale.

Descrizione dei Gap tecnologici

Questo nuovo modello economico è supportato ed allo stesso tempo ha stimolato progressi tecnici importanti in termini di:

- Virtualizzazione - L'ottimizzazione dell'uso delle risorse computazionali richiede che queste siano rese disponibili attraverso dei meccanismi di astrazione dall'hardware sottostante. Utenti distinti ed indipendenti, che condividono risorse hardware e software, confidano su meccanismi di isolamento logico per proteggere i propri dati;
- Distribuzione - Le risorse di calcolo e i dati, in realtà distribuiti su scala geografica, appaiono prossimi all'utente, grazie ad efficaci di meccanismi di distribuzione;
- Scalabilità ed Elasticità - Le caratteristiche intrinseche di distribuzione e ridondanza dell'infrastruttura consentono di allocare e deallocare le risorse in funzione delle reali necessità e di riconfigurare il sistema per conferire allo stesso caratteristiche di tolleranza ai guasti.

Le tecnologie abilitanti del cloud computing hanno già tutte un sufficiente livello di maturità, ma sono tuttavia necessari ulteriori sviluppi per consentire una diffusione massiccia di questo modello computazionale. In uno studio condotto da ENISA (Survey - An SME Perspective on Cloud Computing), vengono individuati come principali gap tecnologici relativi alla sicurezza del cloud:

- La confidenzialità dell'informazione;
- La liability per incidenti che coinvolgono l'infrastruttura.

Trend evolutivi

È possibile ipotizzare che i trend evolutivi più importanti nel campo del Cloud Computing siano nei prossimi anni:

- L'arricchimento ed il perfezionamento del modello di business;
- Lo sviluppo di tecniche di virtualizzazione più efficaci, che garantiranno oltre ad una migliore capacità di utilizzare in maniera efficiente le risorse hardware disponibili anche maggiori garanzie di protezione della confidenzialità dei dati degli utenti;
- La definizione di standard, che favoriranno l'interoperabilità dei servizi e la componibilità degli stessi;
- Lo sviluppo di meccanismi per l'integrazione e la federazione di cloud (pubbliche, aziendali e private);
- L'implementazione di meccanismi efficaci di monitoraggio della Quality of Service (QoS), non solo a livello dell'infrastruttura di rete ma anche e soprattutto al livello dei processi di business;
- Lo sviluppo e la diffusione di strategie di routing più scalabili di quelle tradizionali, capaci di fornire soluzioni efficienti al problema della congestione dell'ultimo miglio (innanzitutto tecniche di Content Based Routing);
- L'integrazione all'interno della piattaforma di capacità computazionali più sofisticate e di maggiore potenza semantica (innanzitutto: Stream Processing e Complex Event Processing).

Livello attuale di TRL

Il TRL è valutato, relativamente alle principali tecnologie abilitanti, tra il livello 3 ed il 4.

Step Necessari per arrivare a TRL + 1 (road-map)

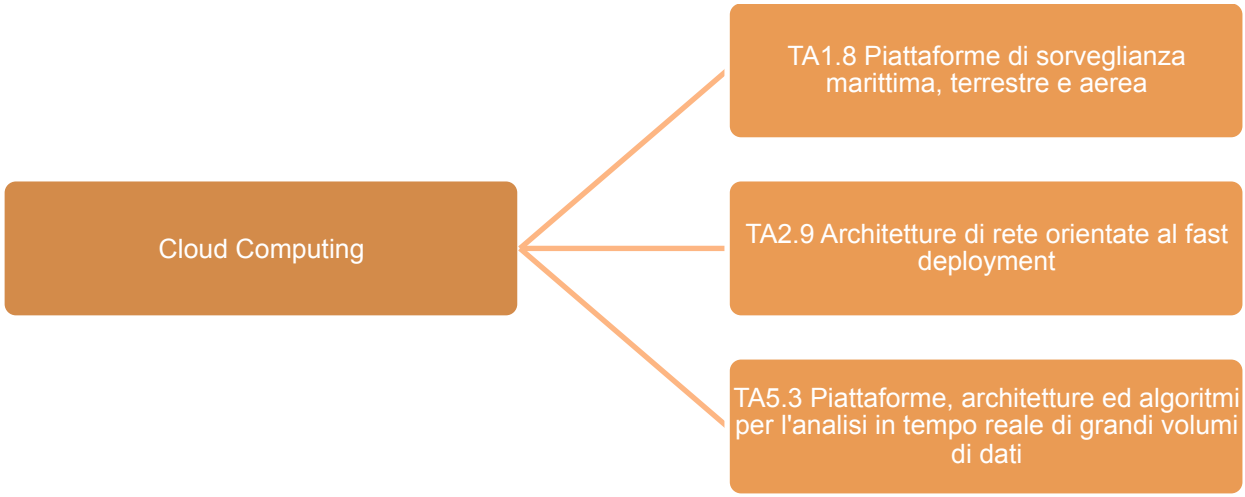
Il raggiungimento dell'obiettivo di riduzione dei gap tecnologici richiede l'esecuzione coordinata di una serie di attività di ricerca.

<2013-2015>	Arricchimento e perfezionamento del modello di business, sviluppo di tecniche di virtualizzazione più efficaci.
<2013-2015>	Definizione di standard per l'interoperabilità e la componibilità dei servizi, sviluppo di meccanismi per l'integrazione e la federazione di cloud.
<2014-2016>	Implementazione di meccanismi efficaci di monitoraggio della QoS, sviluppo delle tecniche di Content Based Routing
<2014- 2016>	Integrazione nelle piattaforme di funzionalità di Stream Processing e Complex Event Processing

Costo associato per arrivare a TRL +1

Anni: 2.5
Investimento: ~ 10 M€

TA di riferimento TA5



- **Architetture Software**

Descrizione dello Stato dell'arte

L'architettura [di un sistema] software è definita come l'organizzazione di base del sistema, comunemente rappresentata:

- Dalle sue parti componenti (scomposizione in sottosistemi)
- Dalle interazioni tra di loro e con l'ambiente esterno
- Dalle loro proprietà visibili (servizi forniti, prestazioni, uso di risorse condivise, ...)
- Dai principi che ne guidano il progetto e l'evoluzione.

La fase di progettazione di un'architettura SW è seguita in genere dalla progettazione di dettaglio, fase in cui ci si occupa degli aspetti "non visibili" dei sottosistemi, quali ad esempio le strutture interne di dati o gli algoritmi di calcolo. La scomposizione del processo di progettazione in due fasi serve a ridurre la complessità della realizzazione ma anche a soddisfare ulteriori requisiti quali la modularità (possibilità di riuso), modificabilità, portabilità, interoperabilità, il livello di prestazioni, il rispetto di vincoli derivanti dall'impiego di HW particolare, la sicurezza, la testabilità e la possibilità di sviluppo incrementale. La voce tassonomica "Architetture SW" comprende una serie di tecnologie che possono essere utilizzate per progettare architetture che presentino evidenti vantaggi rispetto a quelle "tradizionali"; tra queste rientrano alcune tecnologie ritenute particolarmente importanti per lo sviluppo di applicazioni nel campo della sicurezza, quali:

- Modelli di architetture orientate ai servizi (SOA, Service Oriented Architecture, Web services, Semantic Web Services), una serie di principi e metodologie per lo sviluppo di SW sotto forma di servizi interoperabili; i servizi rappresentano funzionalità ben definite e possono essere utilizzati (invocati) senza che sia richiesta alcuna conoscenza sul modo in cui vengono esplicati (accoppiamento lasco);
- Service oriented programming (SOP) platforms, ambienti distribuiti per l'esecuzione di applicazioni secondo uno specifico modello architetturale, quali gli ambienti virtuali di calcolo parallelo basati su Internet (iVCE, Internet-based virtual computing environment) che prevedono la collaborazione tra applicativi autonomi su base volontaria e in ambiente dinamico;
- Modelli architetturali "event driven" (EDA, Event Driven Architecture) in cui gli eventi significa-

tivi (interni o esterni al sistema) vengono immediatamente notificati ad alcune delle sue componenti per consentirne la valutazione e l'individuazione di un'opportuna reazione; questa architettura presenta un livello di accoppiamento tra componenti ancora più bassa di quella del modello SOA;
- Middleware e API (Application Program Interfaces) per la distribuzione real-time di dati secondo il modello "publish-subscribe", garantendo la qualità del servizio e un basso overhead.

Descrizione dei Gap tecnologici

Le tecnologie elencate al paragrafo precedente hanno tutte un sufficiente livello di maturità ma richiedendo tuttavia ulteriori sviluppi per consentirne e supportarne l'impiego in specifici campi applicativi, compreso lo sviluppo degli strumenti di supporto alla progettazione e codifica (CASE-coding-debug tool) necessari per la definizione ed attuazione di un processo di sviluppo adeguato al problema da risolvere e quindi all'architettura scelta. In particolare nel settore della sicurezza i principali gap tecnologici sembrano essere rappresentati da:

- Implementazione di architetture SOA che rispettino vincoli stringenti di sicurezza e che siano utilizzabili anche in presenza di risorse limitate (mancanza di collegamenti a banda larga, flussi di dati asimmetrici); questo al fine di allargare nel campo della sicurezza la possibilità di impiego di strumenti SW già largamente diffusi in altri settori;
- Implementazione del concetto di Semantic Web Services al fine di aumentare il livello di interoperabilità e di automazione dei sistemi (con conseguente riduzione dei tempi di risposta a minacce) e ridurre i costi di sviluppo e messa in opera (deployment) di nuovi sistemi;
- Sviluppo di modelli architetturali basati sulla combinazione dei modelli SOA e EDA;
- Realizzazione di strumenti per lo sviluppo e l'esecuzione di applicativi in ambiente distribuito (SOP, iVCE) che garantiscano la sicurezza, affidabilità e stabilità del sistema risultante;
- Sviluppo di Middleware per Data Distribution Services (DDS) che consentano la condivisione e lo scambio sicuro di dati in tempo reale anche in presenza di risorse limitate e quindi impiegabili anche su dispositivi mobili;
- Sviluppo di tecniche (e relativi strumenti di supporto) per la definizione e poi attuazione di un idoneo processo di progettazione dei sistemi ed in particolare della loro architettura di modo che essa assicuri il raggiungimento dei prefissati obiettivi di qualità del sistema risultante (come previsto ad es. dalle norme ISO nel settore). Lo sviluppo di tali processi e, possibilmente, la loro standardizzazione si considera di particolare importanza per lo sviluppo di applicazioni in ambito sicurezza (come in generale avviene per tutte le applicazioni "mission critical");
- Sviluppo di strumenti per la progettazione del sistema (ed in particolare della sua architettura), spesso noti come CASE tool, mediante la corretta esecuzione del processo previsto. Tali strumenti dovranno includere adeguati supporti di verifica delle operazioni compiute dal progettista di modo da assicurare l'attuazione delle best practice previste e l'esatta applicazione della sintassi dei linguaggi di modellazione adottati (es. UML, sue estensioni e/o linguaggi formali di specifica). Come già osservato a proposito dei processi, lo sviluppo di strumenti e, possibilmente, la loro standardizzazione rivesta carattere di particolare importanza nel settore specifico;
- Identificazione e documentazione di nuovi design pattern che catturino nuovi casi comuni nell'utilizzo delle nuove architetture prima menzionate e che invoglino il progettista a definire

l'architettura mediante il riuso di design pattern in accordo con le linee guida consigliate.

Trend evolutivi

I trend evolutivi più importanti nel campo delle architetture SW sono rappresentati dai seguenti concetti:

- Implementazione del modello di business orientato ai servizi, basato sulle tecnologie abilitanti soa e web services;
- Virtualizzazione, tendenza a sfruttare al massimo le risorse disponibili per semplificare la gestione dell'infrastruttura tecnologica ed evitare nuovi costi, potendosi adeguare rapidamente a nuove condizioni d'impiego;
- Standardizzazione, la possibilità per l'utente finale di scegliere le soluzioni più in linea con le proprie esigenze e disponibilità finanziarie senza dover rinunciare all'interoperabilità con le infrastrutture già esistenti o dover procedere a continui aggiornamenti;
- Crescente importanza di internet con possibilità di essere connessi ovunque, rendendo applicabili modelli di architetture distribuite su reti fisse o sistemi mobili.

In base a queste direttive è possibile ipotizzare:

- Un ulteriore sviluppo delle architetture orientate ai servizi (soa, web services), la sua estensione semantica (semantic web services), la risoluzione dei problemi di sicurezza e di applicabilità al segmento mobile;
- Lo sviluppo di service oriented programming platforms, ambienti distribuiti per l'esecuzione di applicazioni secondo uno specifico modello architetturale;
- Lo sviluppo di modelli architetturali che combinano i concetti soa e eda;
- Lo sviluppo di nuovi approcci progettuali che tengano in considerazione le potenzialità dell'integrazione del web semantico e più in generale di 'internet of things' nelle architetture descritte;
- Lo sviluppo di nuovi strumenti per la progettazione delle architetture e la transizione delle specifiche risultanti verso la fase di design di dettaglio e poi codifica anche mediante l'uso di trasformazioni automatiche dei modelli prodotti;
- L'identificazione di nuovi design pattern che combinino architetture orientate ai servizi con le estensioni tipiche del semantic web.

Livello attuale di TRL

A seconda delle tecnologie il TRL è valutato a livello 3-4.

Step Necessari per arrivare a TRL + 1 (road-map)

Il raggiungimento dell'obiettivo di riduzione dei gap tecnologici richiede l'esecuzione coordinata di una serie di attività di ricerca.

<2013-2015> Estensione SOA – Studio, definizione e sperimentazione di un'infrastruttura globale aperta, scalabile e flessibile, 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 nel campo della sicurezza – Soddisfacimento dei vincoli di

sicurezza e possibilità di impiego su segmenti di rete a banda stretta e dispositivi mobili.

<2013-2015> Web Semantico – Studio, definizione e sviluppo prototipale di applicazioni per la sicurezza basate sul concetto di web semantico per la condivisione e lo scambio di informazioni tra agenzie di law enforcement con impiego di un' ontologia comune. Implementazione dei concetti di "scoperta", utilizzo, composizione automatica e orchestrazione di servizi.

<2013-2015> Processi di Progettazione – Studio, definizione e possibilmente standardizzazione di nuovi approcci progettuali che permettano di fruire delle possibilità offerte dal web semantico e dal suo supporto ontologico.

<2014-2016> Studio e sviluppo di modelli architetturali basati sulla combinazione dei modelli SOA e EDA per consentire interazioni sia di tipo "pull" che "push", per permettere ai servizi di reagire dinamicamente agli stimoli esterni ("sense-and-respond" capabilities) e ottenere un adattamento dinamico dei processi basato su eventi.

<2014-2016> Definizione e sviluppo di una "Service oriented programming platform" per lo sviluppo e l'esecuzione di applicativi in ambienti di calcolo virtuali, sufficientemente sicuri e stabili.

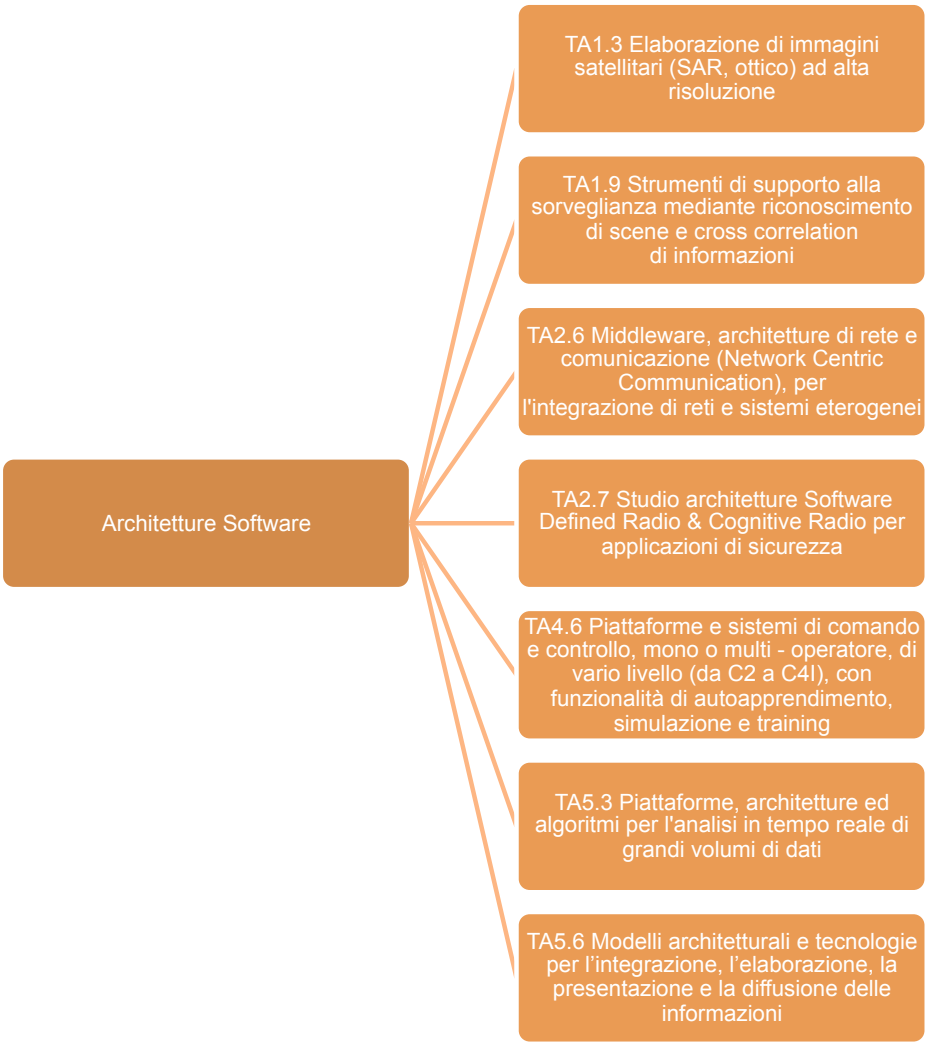
<2014-2016> Studio e sviluppo di strumenti di progettazione che supportino i nuovi processi e permettano la transizione dal modello architetturale verso le fasi successive mediante l'uso di trasformazioni automatiche.

<2014-2016> Identificazione e documentazione di design pattern che si originano dalle esperienze fatte nella realizzazione di architetture basate su modelli SOA ed EDA utilizzanti anche Semantic Web Services.

Costo associato per arrivare a TRL +1

Anni: 2.5
Investimento: ~ 13 M€

TA di riferimento TA5



- **Resilienza e Qualità del Servizio (QoS) dei Sistemi di Controllo Industriali**

Descrizione dello Stato dell'arte

Sistema di Controllo Industriale (ICS) è un termine generale che ingloba diversi tipi di sistemi di controllo, includendo i sistemi di Supervisione Controllo ed Acquisizione Dati (SCADA), i sistemi di controllo distribuiti (DCS), ed altre configurazioni come i Controllori Logici Programmabili (PLC) spesso trovati nei settori industriali e nelle Infrastrutture Critiche. Sono anche inclusi nel termine ICS, altri componenti di controllo e tecnologie di supporto come le Unità Terminali Remote (RTU) e i Dispositivi Elettronici Intelligenti (IED). C'è una preoccupazione crescente sulla cyber security dei sistemi ICS per le Infrastrutture Critiche (CI), dovuta alla crescente abilità dei cyber attackers di causare degradazioni della Qualità del Servizio delle CI persino catastrofiche che impattano larghi strati della popolazione (i.e. grandi blackouts elettrici). Questo è dovuto principalmente alla pervasività delle Tecnologie della Informazione e della Comunicazione (ICT) ed il conseguente de-isolamento dei sistemi ICS che rappresentano il sistema nervoso della maggior parte delle CI. Attacchi informatici possono bloccare la connessione tra il Centro di Controllo dell'ICS e le Unità Remote o inserire dei falsi comandi/misure nei dispositivi di co-

municazione dell'ICS come è accaduto con STUXNET worm. L'importanza della Resilienza e Qualità del Servizio dei Sistemi di Controllo Industriali (ICS), dalle quali dipende la QoS delle CI ai customers, è oggetto di linee guida europee. La resilienza rappresenta la capacità di fornire e mantenere un accettabile livello di servizio anche a fronte di eventi avversi di origine naturale, tecnologica e dolosa inclusi gli attacchi informatici. QoS è intesa come performability, resilienza e security, i tre angoli con cui definire in modo quantificabile le caratteristiche dei servizi forniti dagli ICS. Azioni concrete sono proposte nella Digital Agenda for Europe. Nel contesto della Protezione delle Infrastruttre Critiche, le interdipendenze tra ICT ed il settore Energia con i suoi sistemi ICS sono state indirizzate per prima dall'European Programme for Critical Infrastructure Protection (EPCIP). In questo contesto sono state definite azioni per proteggere l'Europa da attacchi informatici e distruzione (Communication on Critical Information Infrastructure Protection). Tutto ciò prende la forma di un piano di azione su come migliorare la Resilienza e la QoS dei sistemi ICS che complementa i progetti finanziati sotto la voce 'Trust and Security'del Research and Technological Development Framework Programme. Inoltre, in Europa, una attività considerevole nell'argomento è in svolgimento da parte di ENISA (European Network and Information Security Agency).

Descrizione dei Gap tecnologici

I sistemi ICS sono sempre più soggetti ad attacchi informatici e stanno evolvendo verso sistemi sempre più distribuiti ed interoperabili tra loro per accogliere i nuovi paradigmi tecnologici, come ad esempio quelli delle Infrastrutture Elettriche che vanno evolvendo per accogliere le Smart Energy Grids. Ciò sta aumentando il GAP tra quanto si sa fare è quanto è necessario fare per garantire la Resilienza e la QoS dei sistemi ICS.
In questo scenario tecnologico è necessario operare su fronti diversi:

- Seguire un approccio di difesa in profondità (defence in depth) ed includere la cyber security in fase di progettazione dei sistemi ICS;
- Focalizzare gli sforzi di cyber security su tutti i componenti dell'ics e della ci (i.e. Per le smart grids non solo smart meters ma anche automazione delle sottostazioni elettriche, microgriglie, Scada, ICT, etc);
- Individuare una specifica metodologia di risk assessment;
- La cyber security dovrebbe essere misurata in termini di Resilienza e Qualità di servizio;
- Sviluppare sistemi di supporto alle decisioni in tempo reale per gli operatori delle CI in termini di early detection di attacchi informatici, loro isolamento e riconfigurazione dei sistemi.

Trend evolutivi

I trend evolutivi più importanti nel campo della Resilienza e Qualità del Servizio dei Sistemi di Controllo Industriali sono rappresentati dai seguenti punti:

- Individuare, seguendo un approccio di defence in depth, una adeguata metodologia di risk assessment che consenta di valutare gli scenari tecnologici, i servizi forniti, i threats ad i cyber treats, le vulnerabilità dei sistemi ICS e le conseguenze dei cyber attacchi sui sistemi ICS (in termini di resilienza e QoS);
- Migliorare la Resilienza e la QoS delle CI rispetto agli attacchi cyber, mediante l'adozione in ciascuna CI di sistemi integrati di predizione del rischio che siano in grado di rilevare, prevenire, e reagire ai cyber threats;

- Investigare strategie di contenimento delle possibili conseguenze degli attacchi cyber a breve, medio e lungo termine;
- Stimolare la creazione di test beds europei e la valutazione della security dei sistemi ICS
- Stimolare la creazione di una entità di Cybersecurity Europea (European Computer Emergency Response Team) che fronteggi incidenti cyber di larga scala.

Livello attuale di TRL

Per i diversi aspetti tecnologici il TRL è valutato tra il livello 2 ed il livello 3

Step Necessari per arrivare a TRL + 1 (road-map)

<2013-2015> investigare una metodologia di risk assessment per ICS di tipo all hazards che include gli attacchi informatici

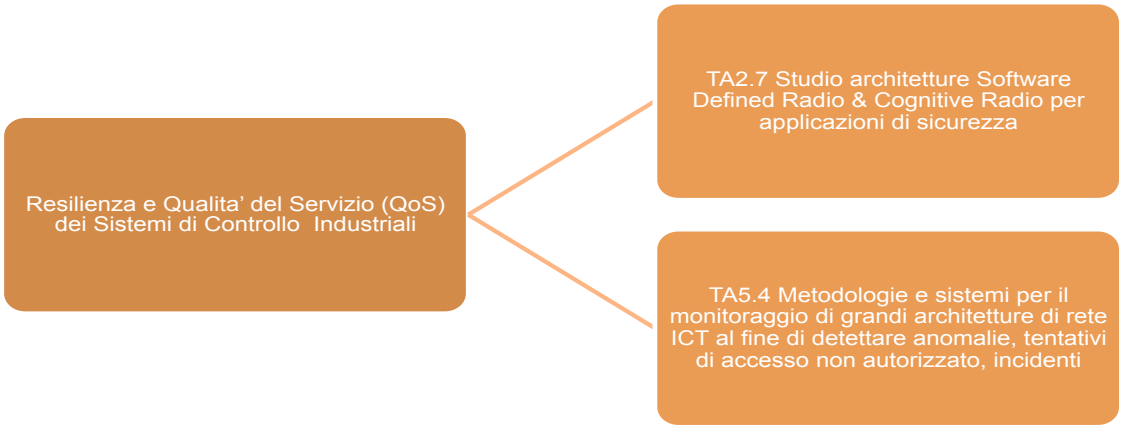
<2014-2016> migliorare la Resilienza e la QoS delle CI rispetto agli attacchi cyber mediante sistemi di supporto alle decisioni, distribuiti e basati sulla predizione del rischio.

<2014-2016> realizzare un test bed per la valutazione della security dei sistemi ICS. Ciò nell'ottica europea di creazione di test beds europei e di un European Computer Emergency Response Team che fronteggi incidenti cyber di larga scala.

Costo associato per arrivare a TRL +1

Anni: 3.5
Investimento: 14 M€

TA di riferimento TA5



High Performance Computing, Hybrid Computing

Descrizione dello Stato dell'arte

Il concetto che sta alla base dell'High Performance Computing consiste nel fatto che l'esecuzione di un dato job computazionale complesso è ottimizzabile suddividendo il problema in tanti task più semplici che possano essere eseguiti in parallelo su CPU differenti. Questo

concetto semplice, che è stato applicato per la prima volta negli anni 90 con l'avvento dei supercomputer, ha permesso di sviluppare tecnologie utilizzate da supercomputer o da computer cluster per creare sistemi di elaborazione in grado di fornire prestazioni molto elevate nell'ordine dei petaflops (un petaflop al secondo significa in una capacità di calcolo in virgola mobile di 10 seguito da 15 zero). I sistemi di elaborazione progettati per ottenere potenze di calcolo estremamente elevate, sono state impiegati sino ad oggi per la risoluzione di algoritmi complessi spesso in ambito scientifico, caretterizzati da un pesante utilizzo di CPU (CPU-bound) o da grossi volumi di dati (Io-bound). I campi di applicazioni più comuni in ordine cronologico sono stati dalla prime modellazione 2D del plasma per poi passare alla modellazione 3D oppure le previsione meteorologiche dalle 48h alle 72h. Sino ad oggi, quindi quando ci si riferisce all'High Performance Computing ci si riferisce ad architetture di calcolo, spesso concepite come pezzi unici, fatte per affrontare un problema o una categoria di problemi computazionali che richiedono potenze di calcolo elevatissime, dedicate e confinate in aree di ricerca o aree industriali ed applicative ben note e definite. Ma gli analisti prevedono, nei prossimi ambiti, una sensibile crescita di queste tecnologie in contesti differenti. L'IDC Worldwide Technical Server Revenue Forecast 2008-2013, per esempio, prevede un mercato in crescita con un business complessivo che passerà da 8,25 miliardi di dollari del 2009, in calo rispetto al 2008, ai 10,5 miliardi nel 2013. Parte di questo mercato, se alcuni gap tecnologici verranno colmati in questi anni, è rappresentato dal mercato security in particolare per l'elevato numero di dati che deve elaborare in real time. Tipiche applicazioni che potrebbero avvantaggiarsi di un sistema HPC sono la decriptazione delle password in real time, trattamento di big data sia per fraud detection in rete che per trattamento di immagini per estrazione di informazioni security relevant, etc.

Descrizione dei Gap tecnologici

Per poter diffondere le tecnologie HPC hanno la necessità di slegare l'infrastruttura HPC caratterizzata da forti investimenti al concetto cioè alla possibilità di avere prestazioni sufficientemente elevate compatibili con il real-time. Cioè si ha la necessità di utilizzare i concetti HPC nel cloud e di semplificare e automatizzare la parallellizzazione del software, con un intervendo ridotto da parte degli esperti. È importante sottolineare che l'HPC sarà fortemente influenzato dai risultati e dalla diffusione del cloud computing (si veda scheda a riguardo).

Trend evolutivi

I trend evolutivi sono caratterizzati da:

- Modelli di programmazione parallela (ad esempio Shared Memory, Multi Thread, Message Passing, Data Parallel);
- CPU-GPU hybrid computing system in grado di accellerare l'esecuzione di un dato algoritmo attraverso l'allocazione dei tasks fra CPU e GPU per la parallel cooperate execution
- Embarrassingly parallel workload in parallel computing ingrado di permettere l'esecuzione di tante tasks parallele senza dipendenze o comunicazione fra tasks parallele.

Livello attuale di TRL

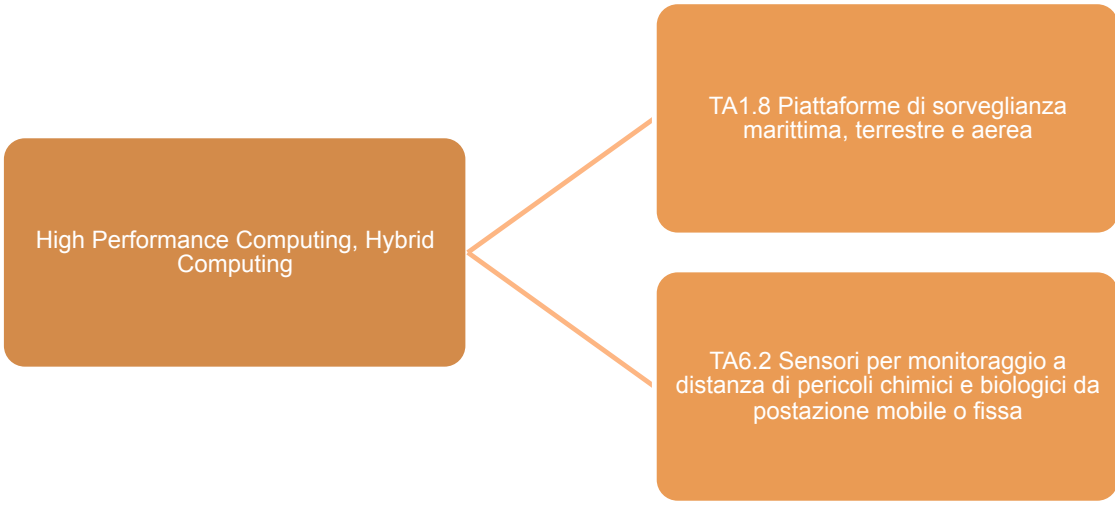
TRL è valutato intorno al 3-4 per le tecnologie abilitanti

Step Necessari per arrivare a TRL + 1 (road-map)

<2013-2015> <sviluppo di nuovi modelli di programmazione parallela>
<2013-2015> <hybrid computing system>

Costo associato per arrivare a TRL +1
Anni: 2.5
Investimento: 10Meuro

TA di riferimento TA5



- **IT Authentication technologies**

Descrizione dello Stato dell'arte

Le tecnologie per l'autenticazione e la gestione dell'identità e degli accessi hanno lo scopo di gestire le identità individuali, la loro autenticazione, l'autorizzazione, i ruoli, i privilegi e i permessi all'interno di un sistema o tra confini aziendali con l'obiettivo di aumentare la sicurezza complessiva del sistema, garantendo al contempo la tracciabilità delle operazioni effettuate. Un modello generale di *identità* assume che tutte le identità in un determinato spazio dei nomi siano uniche e distinguibili e che queste identità abbiamo una specifica relazione alle entità corrispondenti nel mondo reale. In generale, l'entità può avere più identità, e ogni identità può consistere di più attributi o identificatori, alcuni dei quali sono condivisi e alcuni dei quali sono unici all'interno di un certo spazio dei nome. Nella maggior parte dei modelli di identità digitale, un oggetto identità è costituito da un insieme finito di proprietà. Queste proprietà possono essere usate per registrare informazioni relative all'oggetto, sia per scopi esterni al modello stesso o in modo da aiutare il modello operativo, per esempio per la classificazione e il recupero. Il paradigma dell'*accesso degli utenti* in ambito IT prevede che ogni utente assuma un'unica "identità digitale" tra le applicazioni e le infrastrutture di rete, per permettere controlli di accesso da valutare verso questa identità. Tecnicamente, l'uso di un'identità unica tra tutti i sistemi facilita il monitoraggio e la verifica del potenziale accesso non autorizzato, e consente ad un'organizzazione IT di mantenere traccia di eccessivi privilegi concessi a persone all'interno dell'infrastruttura stessa.
Un'identità digitale è articolata in due parti:

- chi uno è (identità);
- le credenziali che uno possiede (gli attributi di tale identità).

Le credenziali possono essere numericamente e qualitativamente molto variegate e hanno differenti utilizzi. L'identità digitale più semplice consiste in un identificativo (username) unico e una parola di identificazione segreta (password). In questo caso lo username è l'identità, mentre la password è chiamata credenziale di autenticazione. Esempi di applicazioni e tecnologie relative all'autenticazione e alla gestione dell'identià e degli accessi sono le Active Directories, Service Providers, Identity Providers, Web Services, Access control, Digital Identities, Password Managers, Single Sign-on, Security Tokens, Security Token Services (STS), Workflows, OpenID, WS-Security, WS-Trust, SAML 2.0, OAuth, and RBAC.

Descrizione dei Gap tecnologici

La gestione dell'identità crea principalmente problemi di *privacy*, come i rischi legato al furto di identità. In particolare, il crescente sviluppo di servizi di social networking online, nei quali la gestione delle identità dei membri rappresenta un elemento fondamentale per la credibilità di questi sistemi, ha sollevato problemi legati alla divulgazione dei dati personali e, quindi, alla perdita della privacy di un individuo. Attualmente i sistemi per la gestione delle identità digitali soffrono dei seguenti problemi:

- costi alti per le suite commerciali di gestione delle identità digitali;
- le soluzioni opensource non soddisfano tutti i requisiti funzionali delle organizzazioni;
- difficoltà per la maggior parte delle organizzazioni creare soluzioni ad hoc per la gestione delle identità digitali.

In particolare, ogni sistema sicuro per la gestione delle identità digitale deve offrire:

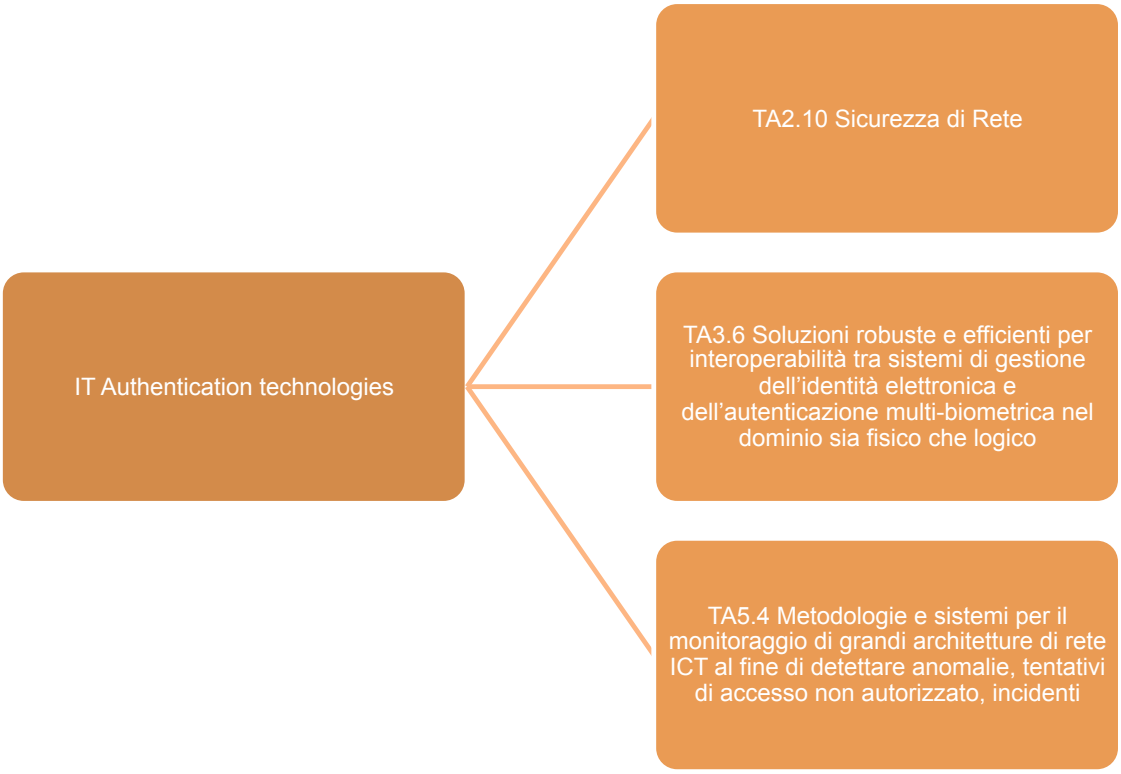
1. storage sicuro delle identità, recupero e provisioning;
2. meccanismi per il policy enforcement dell'autenticazione, autorizzazione, single sign-on, e della federazione delle identità;
3. storage sicuro delle attività effettuate, monitoraggio e recupero;
4. utilità di amministrazione e configurazione per gestire i componenti e i dati.

Trend evolutivi

Vi è un crescente interesse da parte delle organizzazioni verso l'uso delle federazioni per la gestione intra-istituzioni di gruppi di lavoro per evitare di dover creare nuove identità per ogni persona in ogni istituzione. C'è anche un aumento della domanda per la gestione delle identità degli affiliati e l'integrazione di tali utenti nelle strutture di autorizzazione usate dai dipendenti stessi. Inoltre, visto il crescente utilizzo di risorse e dati in ambienti cloud computing che possono essere condivisi da istituzioni e individui diversi, queste si baseranno sulla gestione delle identità federate per la loro infrastruttura di autenticazione e autorizzazione. La situazione attuale vede l'utente/utilizzatore come unico custode e garante delle chiavi di accesso ai sistemi informativi in contraddizione con il fatto accertato che 'l'uomo è vulnerabile e non patchablè. Dalla tecnologia l'uomo si aspetta di avere dei benefici, senza subirne i problemi. Una prossima tappa obbligata dell'informatica deve essere la rivisitazione concettuale dell'accesso ai sistemi e conseguentemente alle informazioni, eliminando l'arcaica necessità di impostare, ricordar-

si e cambiare continuamente complesse credenziali d'accesso (Dlgs 196/2003). Le tecniche biometriche di identificazione possono essere applicate sia al controllo dell'accesso a luoghi e informazioni, sia all'autenticazione di informazioni, in sostituzione di sistemi nome username/password, o di dispositivi elettronici o meccanici aventi funzione di chiave. L'utilizzo delle tecniche biometriche avviene attraverso un sistema di riconoscimento biometrico; attualmente questi sistemi si stanno espandendo in diversi settori, ma con costi ancora abbastanza elevati.

TA di riferimento TA5



- **Intrusion detection technologies**

Descrizione dello Stato dell'arte

La sicurezza delle informazioni deve essere diretta anche a garantire la riservatezza delle informazioni acquisibili nell'ambiente, quali colloqui tra persone o semplici comportamenti concludenti (ad es.: leggere la combinazione all'apertura di una cassaforte). Inoltre esistono altri generi di informazioni che scaturiscono dall'uso di tecnologie (ad es.: telefono) che sono comunque fortemente connesse alla vulnerabilità delle persone e verso le quali è necessario aumentare la protezione dagli strumenti di spionaggio. Debbono quindi essere adottate contromisure elettroniche idonee a individuare eventuali sistemi di intercettazione (*Technical Surveillance Counter Measures* - TSCM). Le tecnologie TSCM intendono localizzare sistemi di attacco quali dispositivi di audio/video clandestini, localizzatori, o altri strumenti di spionaggio elettronico, allo scopo di proteggere gli interessati dalle intercettazioni. La tecnologie di ricerca sono basate su tre direttrici: individuazione diretta delle device, ovvero individuazione delle stesse attraverso la ricerca delle fonti di alimentazione o dei sistemi di trasmissione dei dati. Peraltro il grande

sviluppo dell'elettronica da consumo e a basso costo degli ultimi anni ha consentito l'accesso al mercato degli strumenti di intercettazione entry level, a volte discretamente efficaci, anche a soggetti improvvisati o addirittura digiuni di qualsiasi competenza tecnica e quasi sempre per scopi illegali. Le tecnologie TSCM richiedono di un alto grado di flessibilità in relazione all'enorme variabilità dei sistemi di attacco che sfruttano le vulnerabilità della Information security. Queste ultime debbono essere individuate attraverso adeguate target e risk analysis. Le tecnologie di individuazione e localizzazione dei sistemi di trasmissione radio possono essere costituite sia da apparecchi scanner dedicati e dotati di sofisticati e specifici software di analisi (ad esempio per individuare trasmissioni digitali come i burst), sia scanner tradizionali di alta qualità, sicuramente meno versatili ma insostituibili in condizioni particolari. Esistono poi tecnologie in grado di individuare o analizzare i sistemi di alimentazione elettrica, ad esempio attraverso l'individuazione e classificazione di interruzioni o giunzioni sulla rete. L'utilizzo del NLJD (*Non Linear Junction Detector*), che consente di individuare transistors o altre componenti elettriche, ha raggiunto un elevato grado di maturità e integrazione con altre tecnologie, esaltandone la qualità (ad es. integrando funzioni avanzate di metal detection) e non sono prospettabili rilevanti sviluppi nel futuro. Vanno poi tenute in considerazioni molte tecnologie di detection più specializzate ma assolutamente necessarie per garantire una adeguata sicurezza, quali la protezione da sistemi di trasmissione a onde convogliate, infrarosso, laser e ultrasuoni.

Descrizione dei Gap tecnologici

La saturazione dello spettro delle radiofrequenze rende sempre più difficile l'individuazione dei segnali radio e soprattutto l'esclusione dei segnali non nocivi, anche perché non esiste una campionatura delle frequenze soggette a vulnerabilità. La nuova tecnologia di trasmissione a banda ultra-larga (ultra wideband) risulta scarsamente intercettabile sulla base delle tecnologie oggi disponibili, oltre alle altre, continue, novità nel campo della trasmissione digitale (ad es sovrapponendosi alle frequenze per cellulari. Anche la diffusione di apparecchiature elettriche nelle abitazioni e soprattutto nei luoghi di lavoro ha reso meno utilizzabile per la detection delle microspie il rilevatore di giunzioni non lineari, che pure resta uno strumento fondamentale per alcuni contesti. Pertanto risulta difficile individuare una microspia in un computer da tavolo o in altre apparecchiature elettroniche complesse, posto che non sono state sviluppate tecnologie idonee a questo scopo. In questo caso la ricerca di microspie si dirige verso le fonti di alimentazione e soprattutto di trasmissione del segnale. Anche le altre apparecchiature illustrate debbono misurarsi con i continui sviluppi delle tecnologie di intercettazione. In sostanza, manca la capacità di gestire in forma efficiente ed equilibrata le nuove vulnerabilità e di garantire per ognuna di essa lo sviluppo di best practice e tecnologie di contrasto.

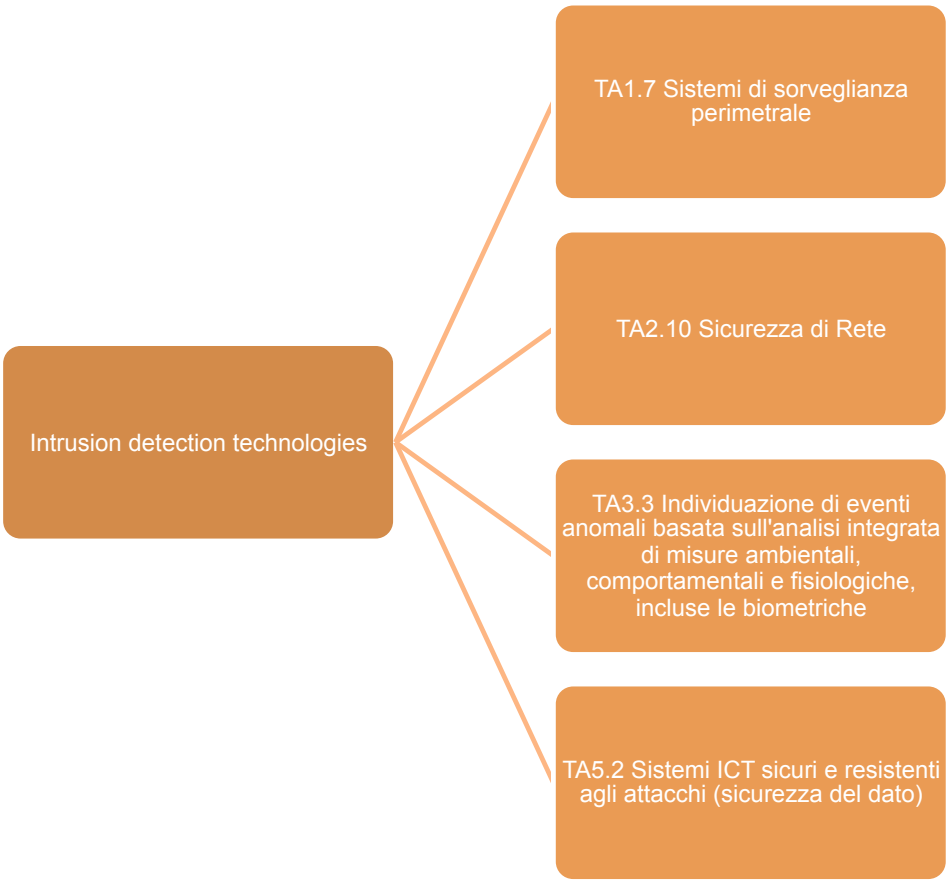
Trend evolutivi

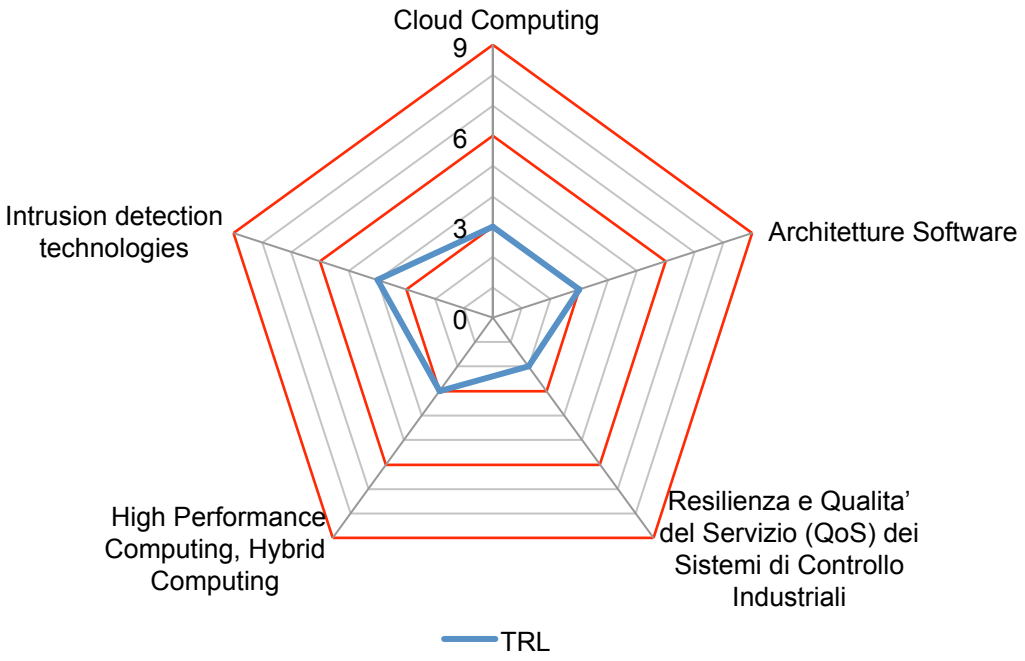
Prioritariamente va sviluppata una piattaforma software gestionale che, sulla base di best practice di gestione dell'intero processo di countersurveillance, consenta l'individuazione e la riduzione delle vulnerabilità. Sono in corso di sviluppo tecnologie in grado di individuare microspie in ambienti tecnologicamente avanzati, ad esempio attraverso l'analisi dei campi magnetici dispersi (le c.d. frequenze di clock). A questo riguardo è ipotizzabile effettuare una campionatura degli spettri dei campi magnetici dispersi emessi delle apparecchiature di spionaggio per lo sviluppo di appositi filtri a supporto degli apparati di analisi di dette emissioni. Infine la

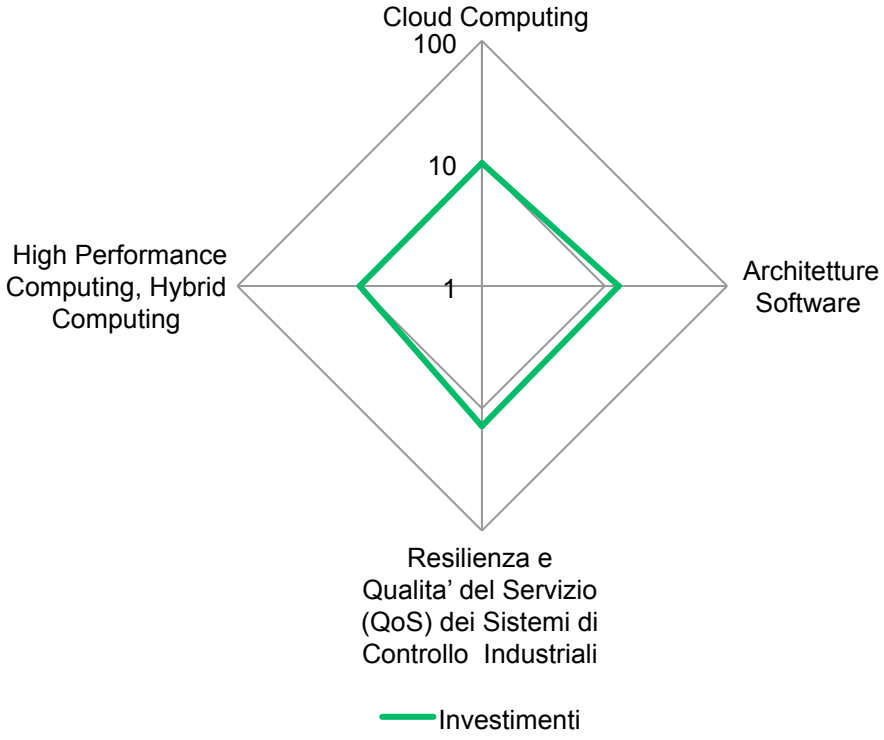
classificazione dell'analisi vettoriale dei segnali da microspia coperti dalle frequenze telefoniche cellulari può consentire lo sviluppo di appositi tool in materia.

Livello attuale di TRL TRL 4

I TA di riferimento TA3




Cloud Computing
9
6
3
0
Architetture Software
Resilienza e Qualita' del Servizio (QoS) dei Sistemi di Controllo Industriali
High Performance Computing, Hybrid Computing
Intrusion detection technologies
TRL


Cloud Computing
100
10
1
Architetture Software
Resilienza e Qualita' del Servizio (QoS) dei Sistemi di Controllo Industriali
High Performance Computing, Hybrid Computing
Investimenti

4.1.4 Biotechnology

Ambiti prioritari di ricerca

- Biomaterials and nanofabrication
- Rapid analysis of biological agents and of human susceptibility to diseases and toxicants
- Food testing and control techniques

- **Biomaterials and nanofabrication**

Descrizione dello Stato dell'arte

I biomateriali possono essere modellati per assumere forme desiderate, e come parte di un sistema complesso, applicate al controllo delle interazioni con componenti dei sistemi complessi. Si parla della progettazione di biomateriali, la sintesi di polimeri e la caratterizzazione, l'autoassemblaggio di biopolimeri (acidi nucleici, proteine, lipoproteine o proteine legati a zuccheri, polisaccaridi, altri composti con caratteristiche specifiche). Per i biopolimeri, sequenze specifiche negli acidi nucleici o di ammino acidi forniscono caratteristiche specifiche (interazione e legame con molecole bersaglio) quindi un approccio combinatorio SELEX viene largamente usato per identificare le sequenze che meglio interagiscono con i bersagli desiderati. I biomateriali possono essere sintetizzati in laboratorio utilizzando una varietà di approcci chimici usando componenti metalliche, ceramiche, o materiali compositi su nanoscala / nancompositi. I biomateriali possono avere proprietà di autoassemblaggio e gerarchia strutturale. La funzionalizzazione delle superfici polimeriche possono fornire le proprietà desiderate di uno strato sottile: la tecnica consente il controllo delle proprietà di "gating", come l'apertura e la chiusura di canali che controllano il flusso di ioni tra due lati di una superficie. Tecnologie per fabbricare microprocessori, capaci di creare oggetti minori di 100 nm, sono applicate alla nanofabbricazione. La nanotecnologia molecolare è particolarmente associate all'assemblatore molecolare, una macchina che può produrre una struttura o uno strumento desiderato aggiungendo unità singole di biomateriali a formare uno strato sulla superficie. Altre prestazioni possono essere ottenute mediante lo sfruttamento delle architetture gerarchiche, presentando diversi biomateriali e/o strutture organizzate a livelli e scale diverse. La stabilità è stata considerata sia migliorando la qualità dei materiali (es. Riducendo la presenza di difetti che possono indurre deriva nel tempo e ridotta riproducibilità) sia con lo sviluppo di protocolli diversi (es fotoattivazione di reazioni chimiche).

Descrizione dei Gap tecnologici

Lo sviluppo di metodi adatti a integrare biomateriali in strumenti funzionali con costi e tassi di produzione accettabili. Una ulteriore sfida riguarda lo sviluppo di metodi adatti a usare tali biomateriali come blocchi di costruzione per preparare architetture con proprietà innovative o migliorate; per un dato biomateriale, la capacità di produrre un gran numero di unità quasi identiche; adattare una appropriata interfaccia per scambi di trasportatori di carica; mantenere la dimensione e organizzazione nano delle nanostrutture, evitando fenomeni di autoassemblaggio o modificazione.

Trend evolutivi

Sviluppo di tecniche capaci di lavorare in parallelo, manipolando (orientando) biomateriali su più substrati allo stesso tempo. Analogamente, altre tecniche sono state dedicate a crescere direttamente i biomateriali sui substrati funzionali (tecniche di autoassemblaggio). L'assemblaggio di materiali forti e flessibili con capacità ottiche ed elettroniche che portano a superfici e sensori ripiegabili. Questi possono essere usati per rilevare le molecole singole di gas. Sensibilità e selettività dei materiali nanofabbricati devono essere testate. Il 'DNA origami' è stato sviluppato come mezzo di produrre strutture plasmoniche che contengono nanoparticelle con strutture chirali sistemate in eliche, con una risposta ottica modulabile, con precisione nanometrica. La

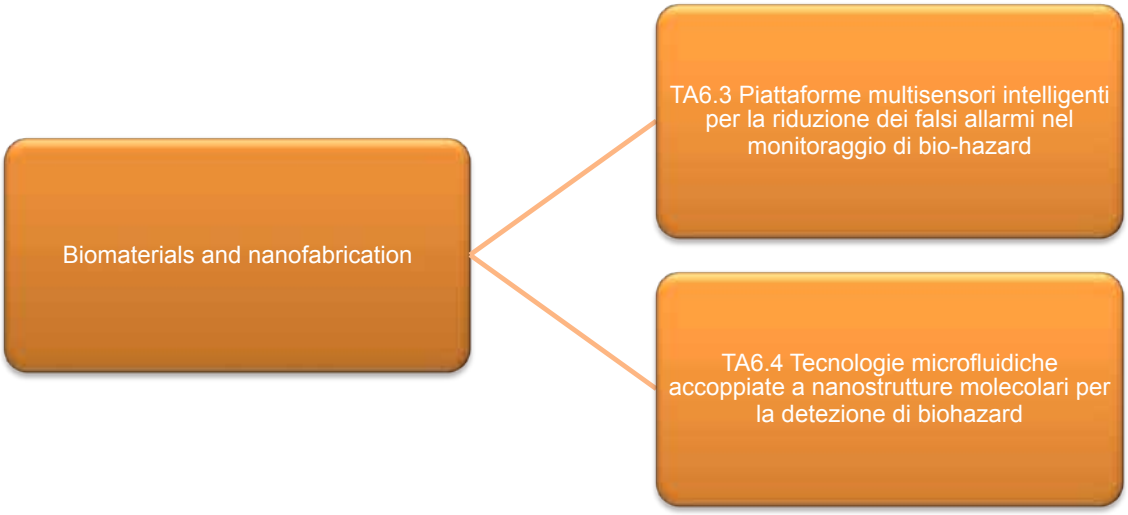
risposta ottica di questi assemblaggi può essere razionalmente modulata per chiralità, colore e intensità, sottolineando il valore del DNA origami come strumento valido per guidare l'auto-assemblaggio di nanoparticelle in materiali con le desiderate proprietà elettriche e magnetiche.

Livello attuale di TRL

TRL 1 - Studi su strutture e superfici basate su nanomateriali a livello di base: comunicazioni richieste tra bisogni e applicabilità di prototipi per focalizzarsi su caratteristiche specifiche.

Costo associato per arrivare a TRL +1 (anni ed investimento economico)
0.5 Meuro/anno

I TA di riferimento TA6



- **Rapid analysis of biological agents and of human susceptibility to diseases and toxicants**

Descrizione dello Stato dell'arte

I rischi biologici e chimici sono comuni nei paesi industrializzati. I rischi biologici sono costituiti da organismi o sostanze prodotte da organismi che pongono minacce alla salute umana e provocano malattie di origine alimentare, anche se si pensa saranno in aumento a causa di attacchi terroristici e contaminazioni in massa per scopi criminali. D'altra parte, i rischi chimici e le sostanze tossiche possono essere gassosi, liquidi o solidi e comprendono materiali chimici e radioattivi (comunemente definiti HazMats) che si possono trovare nell'ambiente ma possono anche rappresentare armi di distruzione di massa, perché il loro rilascio provoca molte vittime e esaurisce le risorse disponibili. Rilevazione, identificazione e quantificazione dei rischi biologici si possono eseguire con diversi tipi di approcci e tecniche basate sul riconoscimenti di specifiche macromolecole diagnostiche, solitamente acidi nucleici (DNA, RNA) e proteine. Un diagramma di flusso dell'approccio metodologico in caso di rischi biologici comprende: (i) estrazione di acidi nucleici da campioni ambientali, in diverse matrici (suolo, piante, animali); (ii) quantificazione e caratterizzazione di acidi nucleici; (iii) scelta di bersagli molecolari per l'identifi-

cazione diagnostica dell'agente di interesse; (iv) applicazione della Polymerase Chain Reaction (PCR) per l'amplificazione selettiva dei marcatori diagnostici; (v) applicazione di protocolli PCR modificati per il miglioramento del rilevamento (es. quantificazione, reazioni multiplex, genotipizzazione). Queste analisi si possono classificare come dirette e indirette. Sono dirette, quando il rilevamento del bersaglio indica la presenza dell'agente di rischio: ad esempio, il rilevamento di un frammento genico appartenente a un organismo patogeno indica la presenza di quell'organismo. Sono indirette, se il rilevamento del bersaglio suggerisce la presenza dell'agente di rischio: es., il rilevamento di un gene che codifica per una tossina suggerisce la presenza dell'organismo produttore della tossina, ma non può dare informazioni sulla presenza della tossina stessa. Agenti chimici tossici sono identificabili con diversi sensori nell'atmosfera, che sono descritti in altri documenti. L'effetto degli agenti tossici di natura chimica o biologica sulla salute umana può essere diverso nei diversi individui secondo la specifica suscettibilità. Le componenti deboli della popolazione sono le più sensibili. Un esempio recente è stato fornito dalla infezione di Escherichia coli in Germania (primavera 2011) dovuta alla contaminazione da semi di fieno greco: Le vittime non sono state causate solo dal livello di esposizione, ma anche dalla sensibilità degli individui. Studi su questi aspetti sono ancora nelle fasi iniziali.

Descrizione dei Gap tecnologici

I gap tecnologici per l'analisi e la risposta agli agenti tossici (biologici e chimici) sono rappresentati da due aspetti principali:

- la mancanza di un sistema coordinato a livello europeo per l'identificazione di rischi e protocolli armonizzati per le procedure analitiche;
- la mancanza di una procedura comune per risposta e contromisure. Anche questo è stato esemplificato nell'epidemia da Escherichia coli in Germania, dove la mancanza di flusso di informazioni e mancanza di comunicazione hanno contribuito alla disseminazione della malattia.

I gap tecnologici per gli agenti biologici sono rappresentati dalla difficoltà nell'identificare l'evento, difficoltà nell'identificare l'agente (I sistemi sensoriali non stanno in un piccolo veicolo, e pochi sono disponibili fuori dall'ambito militare. Inoltre i sensori sono molto costosi), difficoltà nella protezione (messa in atto per i militari e non per i cittadini comuni), mancanza di preparazione che è minore di quella esistente per le sostanze chimiche e radiologiche, e infine mancanza di condivisione di informazioni. Un altro gap è l'assenza di informazioni relative agli esempi di suscettibilità verso specifici agenti chimici o biologici.

Trend evolutivi

Come già descritto nel caso del controllo sugli alimenti, l'identificazione rapida di agenti biologici si sta evolvendo con l'uso di sensori e analizzatori da applicare in pieno campo, adattando strumenti usati in ambiente medico a un utilizzo in situazioni disagevoli. La miniaturizzazione di strumenti e lo sviluppo di saggi che usano pochi reagenti è un altro trend evolutivo in questo ambito. Riguardo i rischi chimici e biologici, l'autocampionamento e l'analisi automatica delle matrici (aria, acqua) e un altro trend recente. Qualunque programma per le emergenze è potenzialmente molto costoso perché richiede attrezzature e forniture specializzate, e molte unità di personale addestrato a livelli sofisticati. Lo sviluppo di strumenti che non richiedano personale specializzato è quindi una soluzione. Riguardo la produzione di sensori, ci sono molte propo-

ste, come i minisensori per uso civile prodotti specialmente da industrie Americane. Questi nuovi sensori usano tecniche di analisi cromatografiche, analisi del DNA, PCR e classici ligandi anticorpali, fornendo una gestione totale delle reti complesse di sensori, sistemi che integrano rilevatori CBRNE, sistemi di fotocamere analogiche o digitali, modelli di dispersione e reazione ad attacchi bioterroristici.

Livello attuale di TRL

TRL6
Il livello presente di TRL è quello dell'esistenza di alcuni tipi di sensori efficienti per agenti biologici che tuttavia sono usati specialmente per uso militare. Per quanto riguarda le intossicazione chimiche, l'identificazione di sostanze chimiche è più facile ma la ricerca si concentra su alternative terapeutiche.

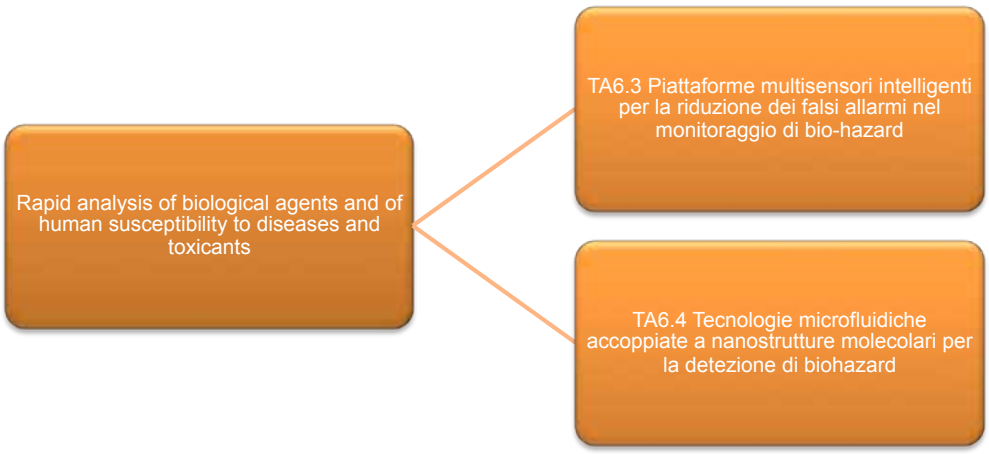
Step Necessari per arrivare a TRL + 1

Mentre il bersaglio delle minacce si è allargato al pubblico in generale, le tecnologie disponibili devono essere adattate e semplificate per creare strumenti da applicare in campo, che offrano identificazione di agenti biologici allo stesso livello dei laboratori, sul posto e con minimi ritardi. Entrambi i tipi di incidenti, chimici e biologici, soffrono della scarsa coordinazione da parte delle autorità competenti basata essenzialmente sulla mancanza di informazioni condivise.

Costo associato per arrivare a TRL +1 (anni ed investimento economico)

3-5 anni
5-10 milioni di Euro

I TA di riferimento TA4, TA6



- **Food testing and control techniques**

Descrizione dello Stato dell'arte

"Tecniche di analisi e controllo degli alimenti" è una definizione che copre una vasta gamma di

tecnologie. Entro questa possiamo considerare: (i) analisi sensoriali eseguite da esperti, basate sull'esperienza personale; (ii) tecniche analitiche convenzionali, chimiche e microbiologiche; (iii) applicazioni innovative di tecniche di biologia molecolare; (iv) piattaforme high-throughput che vanno dai microarray alla spettrometria di massa, Lab-on-chip e raggi X. Perciò, lo stato dell'arte dipende dalla tecnologie prescelta. Nella UE e in altri paesi, il controllo della sicurezza alimentare è incluso nelle leggi, e l'esecuzione dei controllo deve seguire metodi standardizzati (ISO, Codex, AOAC, ecc.). Il controllo della qualità degli alimenti è lasciato a standard volontari e alla certificazione; in questo caso ogni azienda può scegliere parametri specifici, lavorando su tecniche innovative per la valutazione rapida e affidabile della qualità. Spesso, associazioni di produttori possono partecipare nel definire standard e regolamenti. La UE ha finanziato negli ultimi 12 anni diversi progetti di ricerca per migliorare e innovare il controllo degli alimenti a tutti i livelli, iniziando dal Libro Bianco sulla Sicurezza Alimentare che poi originò la General Food Law del 2002. I progetti hanno prodotto notevoli avanzamenti in questo campo, riassunti di recente nella conferenza "What's for Lunch?" (Bruxelles, Settembre 2011) e nel libro "Food chain integrity. A holistic approach to food traceability, safety, quality and authenticity." (Hoorfar, J., Jordan, K., Butler, F., and Prugger, R. (eds.) Woodhead Publishing Series in Food Science, Technology and Nutrition No. 212. Woodhead Publishing, Cambridge). Un inventario di tutte le tecnologie che si possono applicare all'analisi degli alimenti non è lo scopo di questo documento, ma si possono elencare i principali punti di interesse per la sicurezza delle filiere alimentari, che comprendono frodi e contraffazione, terrorismo alimentare, adulterazione, contaminazione. Questi punti riguardano la presenza negli alimenti di agenti chimici o biologici non desiderati o nocivi, ma gli agenti biologici sono più significativi per la sicurezza in caso di terrorismo o di contaminazione intenzionale. Le tecnologie per la rilevazione degli agenti biologici vanno dalle analisi microbiologiche, a metodi basati su analisi di acidi nucleici, proteine e metaboliti che possano essere diagnostiche di organismi specifici. I metodi di rilevazione che possono essere molto utili nel contesto della sicurezza alimentare dovrebbero rivolgersi a bersagli specie-specifici, solitamente con la Polymerase Chain Reaction, o invece a classi di contaminanti, usando tecniche analitiche (es naso elettronico, o spettrometria) accoppiate con la Artificial Intelligence per il riconoscimento di pattern.

Descrizione dei Gap tecnologici

Alcuni argomenti devono essere affrontati per le applicazioni relative ad aspetti di sicurezza.
Il monitoraggio e la sorveglianza dei punti critici lungo la filiera alimentare richiedono lo sviluppo delle strategie di campionamento e di strumenti per il campionamento automatico. La gestione delle situazioni di crisi richiede lo sviluppo di metodi per la preparazione dei campioni da applicare fuori dai laboratori. I metodi dovrebbero essere "extraction-less", per fornire alle analisi il materiale senza lunghi passaggi di purificazione. Per lo stesso motivo, le tecnologie di chimica analitica e di biologia molecolare dovrebbero essere organizzate in piattaforme da applicare il più vicino possibile al punto di interesse (point of concern), anche in condizioni disagevoli. Si devono perciò sviluppare strumenti miniaturizzati e sistemi robusti. Come ha dimostrato la recente crisi con Escherichia coli nei germogli, la conoscenza tecnologica è tale che l'identificazione dell'agente biologico contaminante può essere ottenuta in poche ore. Le perdite di tempo critiche avvengono tuttavia quando si cerca di ricostruire la filiera e di tracciare i contaminanti alla loro origine. Questo è essenziale per proteggere i cittadini da una ulteriore dispersione dell'agente, e anche a scopi forensi. I gap critici qui riguardano i sistemi per archiviare e scambiarsi informazioni tra i diversi attori, rispettando confidenzialità e segretezza.

Trend evolutivi

I trend evolutivi in questo campo riguardano la sorveglianza e la "preparedness". La sorveglianza è considerata mediante lo sviluppo di metodi per il campionamento automatico, di metodi extraction-less per la preparazione di campioni, di strategie per l'identificazione di punti di controllo critici e per lo sviluppo di biosensori.
La preparedness si considera attraverso lo sviluppo e l'applicazione di una serie di tecnologie validate per l'applicazione ad agenti biologici e chimici di interesse per la sicurezza alimentare, lavorando in particolare sulle applicazioni in campo, sulla rapidità delle analisi, su multiplexing e high-throughput. Reti di comunicazione , database, sistemi di supporto alla decisioni sono tutti critici per gli approcci di preparedness, necessari per la gestione delle crisi.
Anche la tracciabilità nella filiera alimentare è necessaria per proteggerne l'integrità, e le tendenze in questo campo si muovono verso l'integrazione della tracciabilità basata su documenti con le tecnologie ICT e il monitoraggio obiettivo dei punti critici.

Livello attuale di TRL TRL 5

Step Necessari per arrivare a TRL + 1

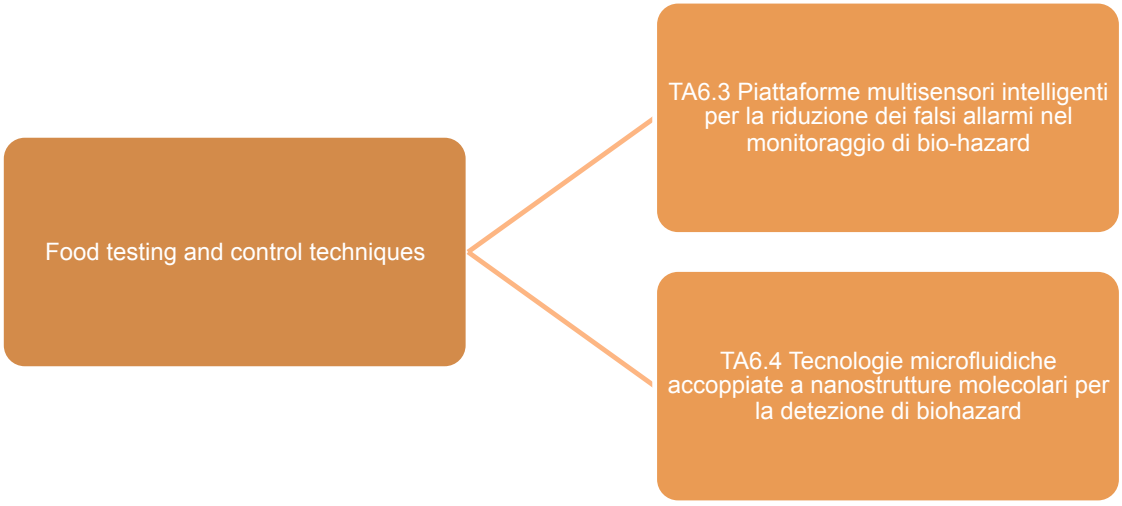
I passaggi successivi richiedono l'applicazione delle tecnologie a problemi realistici su piena scala e l'integrazione con i sistemi esistenti. Si richiedono sforzi a livello multidisciplinare per combinare dati analitici e tecnologie ICT, sistemi di comunicazione e supporto alle decisioni.

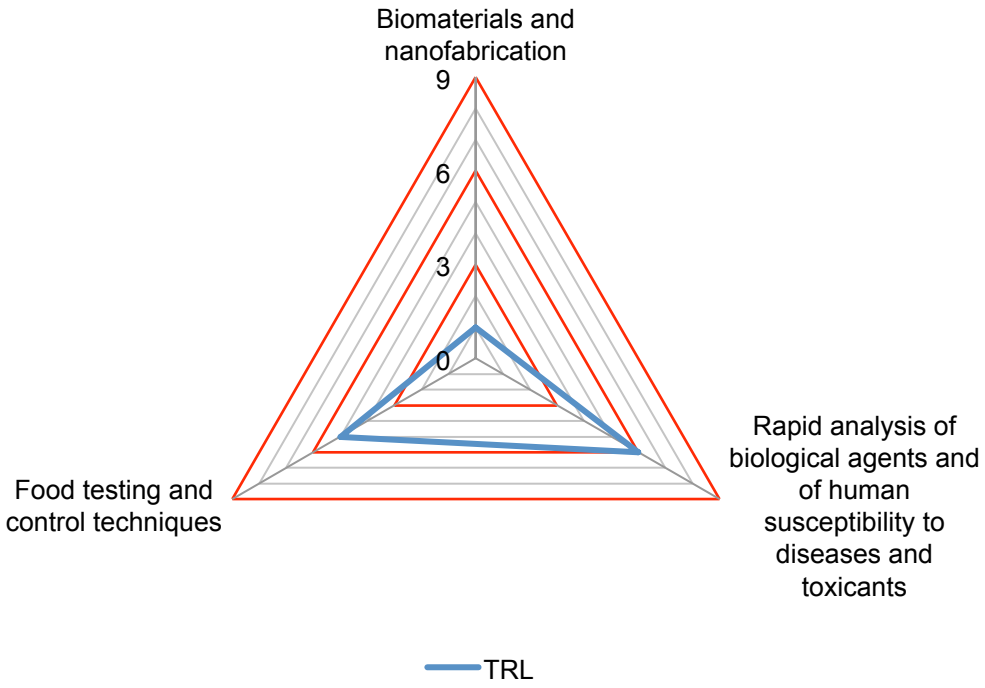
Costo associato per arrivare a TRL +1 (anni ed investimento economico)

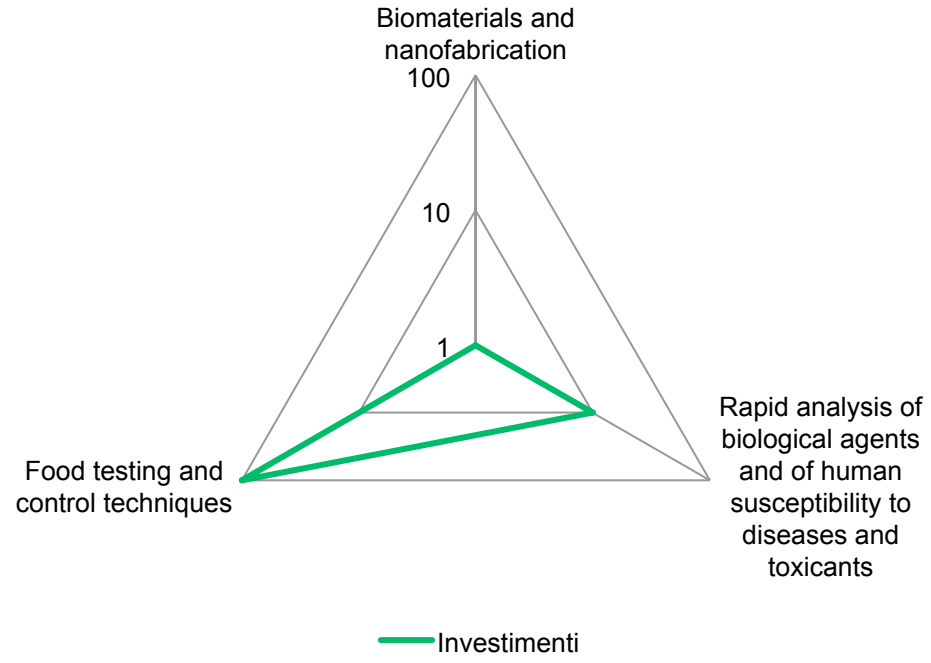
Il prossimo step si può raggiungere nei prossimi 3 anni, con un piano robusto di investimenti stimato a centinaia di M€ a livello mondiale.

I TA di riferimento

TA6, anche TA2 per l'integrazione con ICT

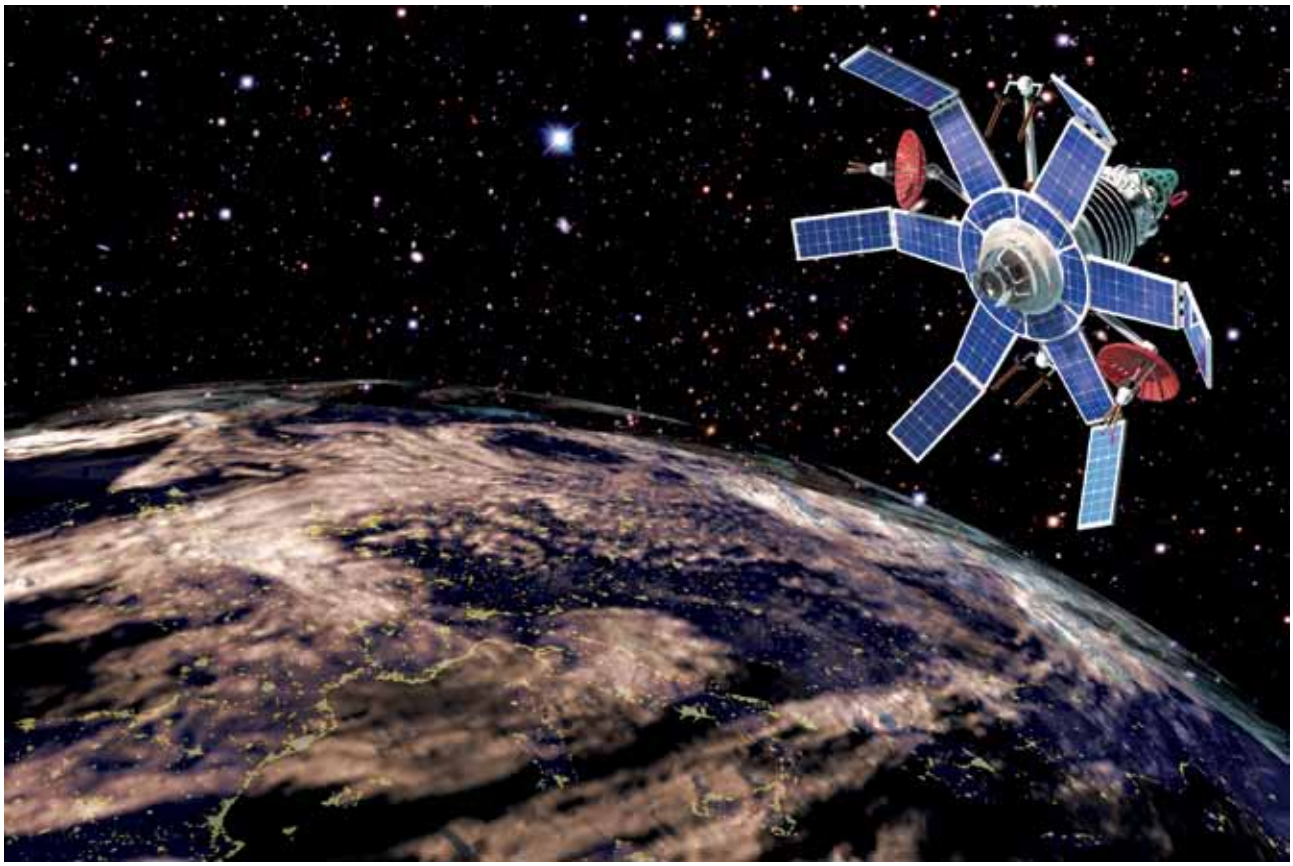



Biomaterials and nanofabrication
9
6
3
0
Rapid analysis of biological agents and of human susceptibility to diseases and toxicants
Food testing and control techniques
TRL


Biomaterials and nanofabrication
100
10
1
Rapid analysis of biological agents and of human susceptibility to diseases and toxicants
Food testing and control techniques
Investimenti

4.2 Equipments and sub systems

4.2.1 Sensor Equipments and signal protection



Ambiti prioritari di ricerca

- Advanced MIMO MTI techniques for Spaceborne Radars
- Mm-wave sensors equipments
- LADARs, LIDARs equipments
- Mobile sensors networks info collection
- Advanced ELINT Capabilities for Spaceborne Radars
- Chemical, Biological, Radiological and Nuclear (CBRN) protection and decontamination equipment - Biotechnology-based systems

- **Advanced MIMO (Multiple-Input-Multiple-Output) MTI (Moving Target Indicator) techniques for Spaceborne Radars**

Descrizione dello Stato dell'arte

Gli attuali radar satellitari hanno conseguito un ben definito, maturo e verificato quadro ingegneristico in funzione di mappature SAR. Al contrario le tecniche MTI sono ancora a livello sperimentale e basate sull'impiego di di tecniche data-independent come la DPCA e la ATI. Inoltre tecniche MTI avanzate, basate su coppie di trasmettitori MIMO (multiple-input-multiple-output), che potrebbero impiegare approcci multicanale con maggiore diversità e strutture di covarianza, risultano onerose e quindi non sono realizzabili rapidamente su payloads SBR.

Descrizione dei Gap tecnologici

Risultano evident i seguenti gap tecnologici:
Necessità di scelte e sviluppi sulle tecniche di processamento e sugli algoritmi
Sviluppi sui payload che trattano la multichannel diversity e le future funzioni di data download
Tecnologie disponibili a qualifica spaziale per utilizzare gli ITAR free components and promuovere una indipendenza europeanell'ambito di queste tecnologie abilitanti.

Trend evolutivi

Il radar MIMO è un argomento di ricerca di grande interesse. La ricerca sui MIMO per MTI satellitari richiede ulterior studi ed investigazioni.

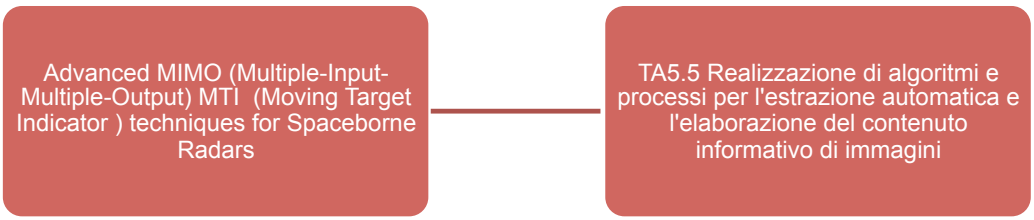
Livello attuale di TRL

Gli attuali radar satellitari non implementano capacità di tipo MIMO. Il range va pertanto da TRL 1 a TRL 3.

Step Necessari per arrivare a TRL + 1

La definizione degli step è attualmente condizionata da un preliminare progresso delle tecnologie abilitanti.

I TA di riferimento TA 1



- **Mm-wave sensors equipments**

Descrizione dello Stato dell'arte

La protezione delle infrastrutture critiche, come nei trasporti di massa, è un bisogno che diventa

sempre più importante dopo i diversi attentati suicidi nelle principali città cosmopolite (Mosca, Londra, Parigi e Oslo). I terroristi con la cintura esplosiva nascosta sotto i panni o nello zaino rappresentano al giorno d'oggi una terribile minaccia. Il successivo rilevante numero di morti e feriti e le conseguenze economiche per le infrastrutture della città, pone la questione di avere una nuova strategia nel problema di sicurezza di trasporto di massa. Tra le diverse tecnologie per contrastare questo pericolo, le onde millimetriche sono interessanti a causa della intrinseca capacità di rilevare i cambiamenti dielettrici passando attraverso i tessuti. In particolare, il corpo umano ha una risposta dielettrica unica (firma) che è differente da qualsiasi firma degli esplosivi. Un sensore di potenziale millimetrico può rilevare e confrontare i valori dielettrici degli oggetti nel campo delle microonde a valori noti (ad esempio, valori del corpo umano) ed è in grado di distinguere zone anomale in cui le proprietà dielettriche sono differenti. Pertanto il sensore dielettrico cosiddetto permette di rilevare un volume sufficiente che è diverso dal corpo umano o da altro materiale in questione. I principali vantaggi della tecnologia millimetrica risiedono essenzialmente nell'utilizzo di un campo a microonde di basse energie per irradiare oggetti e non causare alcun rischio per la salute.
A sostegno di questa tecnologia vi sono ulteriori vantaggi:

- Sicurezza delle radiazioni. La misura dielettrica utilizza energia a microonde a basso livello di dosaggio e quindi radiazioni non ionizzanti possono fornire un'indicazione automatica della presenza di una minaccia;
- Questi sistemi possono operare a frequenze più elevate;
- La modalità attiva o passiva di funzionamento. In modalità stand-off la rilevazione è possibile (fino a 100 m);
- La possibilità di avere più visualizzazioni. Questa tecnologia di misurazione richiede l'accesso a tutte le parti intorno all'oggetto. Il portale esplora tutti i lati in una sola volta scansionando tutto il corpo;
- Protegge la privacy del singolo analizzato. Il display mostra un generico modello umano per visualizzare la posizione di eventuali anomalie rilevate.

Gli inconvenienti della tecnologia millimetri sono:

- Rivelazione non specifica. Si rilevano anomalie, non esplosivi;
- Apparecchiature mobili. Le preoccupazioni circa le questioni etiche (bambini, donne ecc.). Viceversa, immagini di armi nascoste possono essere ottenute ad alta risoluzione utilizzando due scansioni dimensionali olografiche. Tecnologie a onde millimetriche attive e passive sono attualmente utilizzate in body scanner commerciali. Pochi sistemi sono disponibili sul mercato, ma sono in fase di sviluppo sia sistemi attivi che passivi.

Descrizione dei Gap tecnologici

Anche se la tecnologia concettualmente è conosciuta da molti anni, l'applicazione nella sicurezza è stata introdotta solo di recente e un buon livello di maturità è tutt'altro che raggiunto, sia per i sensori attivi che passivi. Diverse lacune sono ancora presenti in molti aspetti della tecnologia. Le firme dei materiali da discriminare tra diversi tipi di oggetti non vengono approfondite. Inoltre, la capacità di determinare la profondità degli oggetti è ancora scarsa, anche se la scansione in polarizzazione viene utilizzata. La forma delle antenne e dei trasmettitori a favore di approcci attivi e passivi deve essere riesaminato, al fine di ottimizzare la rivelazione

ravvicinata o a distanza. Array di antenne per la ricezione devono essere migliorate nelle loro capacità di rilevamento, insieme con l'integrazione di sistemi veloci di scansione elettronici. In generale il concetto di un nuovo radar attivo ad immagine deve essere rivisto. Il riconoscimento automatico delle minacce si basa sullo sviluppo di algoritmi di analisi dell'immagine per rilevare la presenza di oggetti anomali. Le problematiche etiche diventano sempre meno importanti con lo sviluppo di nuovi strumenti software.

Trend evolutivi

Solo poche aziende al mondo sono coinvolte nello sviluppo di questo tipo di sensori, principalmente per il mercato dei body scanner. Solo pochi prototipi pionieristici stanno emergendo nel mercato per sensori attivi stand-off. D'altra parte, le richieste degli uffici di sorveglianza e sicurezza degli aeroporti o delle stazioni metropolitane stanno richiedendo con forza di dotarsi di questa strumentazione. Molti aeroporti internazionali (USA) ed europei (Schipol, Londra, Roma) sono già dotati di questi sensori. Dall'altro lato, i body scanner L3 sono stati testati negli aeroporti e recentemente ENAC e CISA hanno deciso di installare negli aeroporti italiani alcuni di questi sistemi sulle linee di imbarco verso gli Stati Uniti.

Livello attuale di TRL

TRL 7 per i body scanners aeroportuali
TRL5 for stand-off

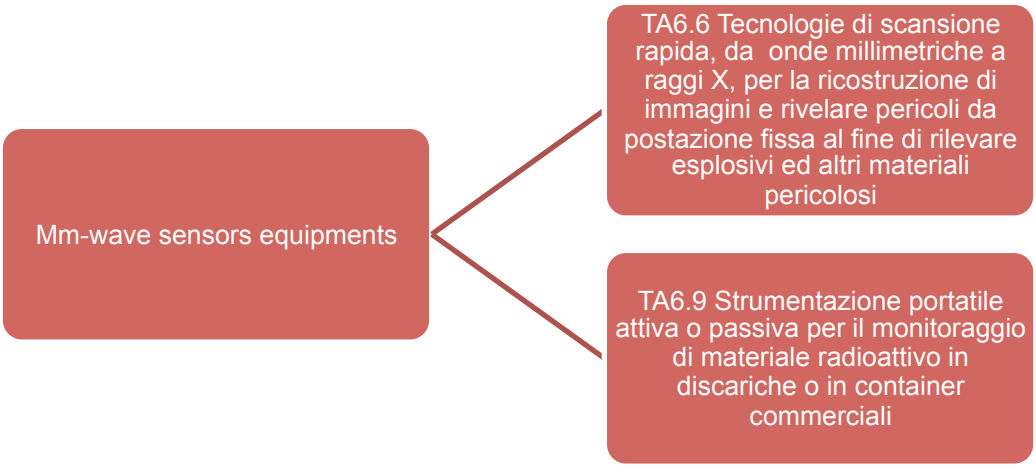
Step Necessari per arrivare a TRL + 1

Forti miglioramenti sono attesi per adattare questi apparati ad ambienti reali. Gli sforzi sono necessari per progettare nuovi apparati per il funzionamento di rilevamento stand-off.

Costo associato per arrivare a TRL +1 (anni ed investimento economico)

Il prossimo passo potrebbe essere raggiunto nei prossimi 3-5 anni, con un piano di investimenti robusto che può essere stimata nell'ordine di diverse centinaia M € a livello mondiale

I TA di riferimento TA1, TA3, TA4, TA6



- **LADARs, LIDARs equipments**

Descrizione dello Stato dell'arte

Un ladar o lidar è essenzialmente un radar laser per la misura a distanza e in tempo reale di parametri chimicofisici dell'oggetto investigato (superficie solida, corpo idrico, strato atmosferico…). Tipicamente è composto da un trasmettitore (laser e ottiche di "beam shaping") e un ricevitore (telescopio ed elettronica di rilevamento del segnale). Comunemente, se il bersaglio è solido (edificio, ostacolo, veicolo…) si usa l'acronimo ladar ("laser detection and ranging"), se il bersaglio è aeriforme (inquinante, particolato, vapore…) si preferisce l'acronimo lidar ("light detection and ranging"). In generale, questi sistemi hanno raggiunto un grado elevato di maturità tecnologica e sono ormai commercializzati da ditte specializzate. Ad esempio, il ladar è utilizzato correntemente nel campo della difesa per misurare la distanza di potenziali obiettivi e il lidar è un potente strumento per studi atmosferici dall'aria urbana alla mesosfera. Per quanto riguarda la security sarebbe auspicabile trasferire alle applicazioni connesse le tecnologie "ladar topografico" e "lidar DIAL". Il ladar topografico permette la ricostruzione di un territorio e potrebbe essere utilizzato con successo alla restituzione tridimensionale di una scena di potenziale interesse. Il lidar DIAL ("differential absorption lidar") è basato sull'assorbimento differenziale di impulsi laser a due lunghezze d'onda leggermente differenti per rilevare molecole specifiche e loro profili lungo il percorso del fascio nell'atmosfera. La lunghezza d'onda ON viene scelta per essere assorbita solo dalla sostanza chimica in esame e la lunghezza d'onda OFF non è assorbita da tale sostanza e, preferibilmente, da altri gas atmosferici, fornendo così un riferimento che caratterizza la risposta ottica del sistema nelle condizioni reali. Comparando la misura dell'attenuazione dei fasci ON e OFF si può calcolare la concentrazione della sostanza chimica in esame lungo il percorso degli impulsi laser. Se il lidar permette il puntamento del fascio, si può ottenere una mappa tridimensionale di concentrazione. Nel campo della security le sostanze da monitorare sono quelle utilizzate per la preparazione di ordigni esplosivi improvvisati (IED), ad esempio acetone. La mappa locale di vapori sospetti mostrerà dove cercare il luogo di fabbricazione di IED.

Descrizione dei Gap tecnologici

Le attuali tecnologie ladar topografico e lidar DIAL per utilizzi civili sono già una buona base per un ulteriore sviluppo verso un design più compatto e robusto, ottimizzato per scenari terroristici e/o per la rilevazione dei precursori di IED. Per alcuni precursori (ad esempio l'acetone) esistono sorgenti laser potenti e affidabili, per altri (ad esempio il perossido di idrogeno, probabilmente uno dei precursori "emergenti") le sorgenti non permettono ancora un dispiegamento "sul campo".

Trend evolutivi

L'innovazione principale a breve termine sarà l'utilizzo di ladar topografici e lidar DIAL al di fuori del laboratorio per caratterizzare scenari terroristici e/o rivelare precursori di IED in tempo reale. Quindi è prevedibile l'utilizzo di una piattaforma mobile: dapprima minivan e, infine, UAV ("unmanned aerial vehicle"). Nel frattempo, il campo delle sorgenti laser accordabili nel medio infrarosso è in piena ebollizione, grazie al costante sviluppo dei QCL ("quantum cascade laser").

Livello attuale di TRL

Nel campo della security: ladar topografico TRL6, lidar DIAL TRL4.

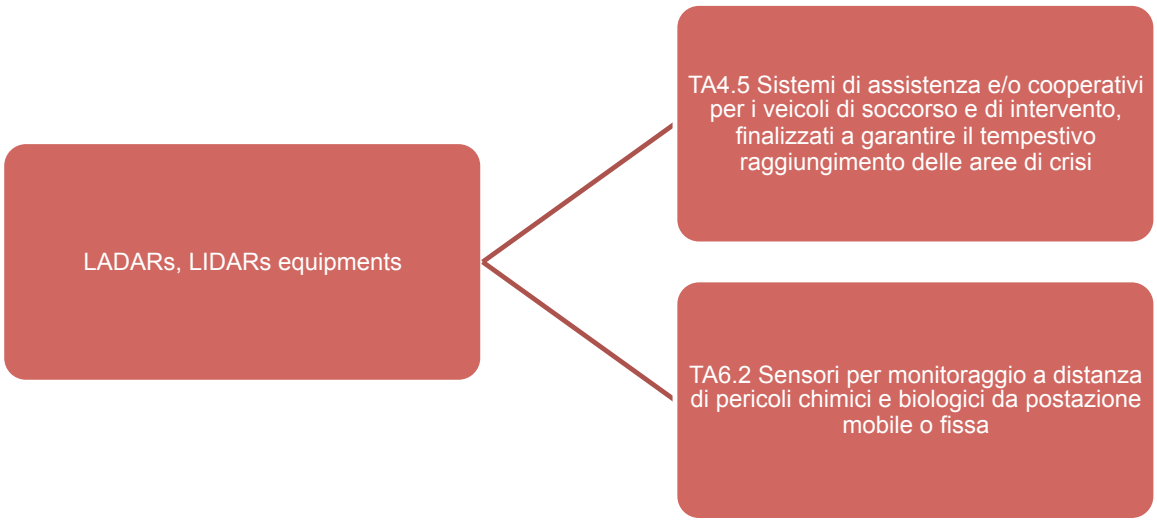
Step Necessari per arrivare a TRL + 1

Il primo obiettivo è quello di creare sistemi i più compatti possibile. A questo riguardo, è fondamentale un accurata progettazione dello schema ottico, in generale, e dell'ottica di puntamento, in particolare.
Per il lidar DIAL è importante che si rendano disponibili sorgenti laser accordabili nel medio infrarosso potenti.
Un ulteriore passo avanti rispetto allo stato della dell'arte riguarda il sottosistema di rilevamento e acquisizione dati. Le prestazioni critiche da affrontare sono la sensibilità del rivelatore e la linearità del sistema di rivelazione.

Costo associato per arrivare a TRL +1 (anni ed investimento economico)

Per ogni tipo di sistema, è ragionevole ritenere che per arrivare a TRL + 1 occorra un investimento pari a un progetto FP7 medio (3 anni, 5 m€).

I TA di riferimento TA1,TA6



- **Mobile sensors networks info collection**

Descrizione dello Stato dell'arte

Le wireless sensors networks sono reti che permettono di creare nuovi strumenti a supporto di attività di monitoraggio apportando un notevole valore aggiunto costituito, da una parte, dalla delocalizzazione dell'attività di misura e, dall'altra, dalla resistenza ai guasti dell'intero complesso. Tali reti si propongono quindi anche come efficace strumento di intelligence, la loro presenza potendo essere facilmente dissimulata in ambienti critici per la sicurezza come, ad esempio, gli aeroporti, ma addirittura nel cosiddetto arredo urbano. Queste reti devono avere le seguenti caratteristiche:

- **Scalability**: trattandosi di reti caratterizzate da un elevato numero di nodi-sensori (dal centinaio sino addirittura al milione) che trasmettono prevalentemente in broadcast, protocolli e algoritmi devono essere adeguati alla situazione e quindi "leggeri" e "scalabili". Lo stesso vale per "naming and addressing";
- **Real time**: il requisito è dettato dal tipo di applicazione. Si va dalla reazione entro qualche ora (es. in agricoltura, rilascio controllato di un pesticida a fronte di una rilevata situazione di vulnerabilità) all'"ingegneria dei secondi" delle reti di early warning sismico (es. blocco dei semafori sul rosso entro 2 secondi dalla ricezione dell'allarme);
- **Data fusion**: la capacità di elaborazione locale su ciascun nodo-sensore e di aggregazione di misure direttamente rilevate con misure ricevute dai nodi-sensori vicini deve avere l'effetto di consentire la propagazione di messaggi di contenuto semantico significativo, piuttosto che di miriadi di dati singoli, alcuni dei quali anche potenzialmente fuorvianti;
- **Narrowband**: date le caratteristiche dei nodi, la potenza in trasmissione è ridotta e ridotte sono le esigenze di banda tipiche delle reti di sensori/attuatori;
- **Routing** idoneo ad "assorbire" le variazioni nel tempo della topologia della rete (nodi che vanno fuori servizio, periodicamente o definitivamente, ritardi variabili di propagazione dei segnali che possono rendere la rete "disconnessa" per un certo lasso di tempo).

Descrizione dei Gap tecnologici

Si elencano di seguito le principali criticità di ordine tecnologico, che si oppongono ad un utilizzo pervasivo delle wireless sensor networks.

- **Manutenibilità/Accessibilità**. Il numero di nodi (elevato) e/o la collocazione di questi (tipicamente "in situ" rispetto al fenomeno da osservare) causano l'impossibilità materiale o comunque l'estrema difficoltà nella manutenzione della rete, intesa soprattutto come manutenzione HW (es. sostituzione di batterie esauste, rimpiazzo di nodi in avaria) e in parte come manutenzione SW (es. riconfigurazione da remoto, ecc.). La rete quindi deve avere marcate caratteristiche di struttura ad alta sopravvivenza con algoritmi, protocolli e procedure studiati appositamente per il risparmio energetico;
- **Connettività intermittente**. È insito nella natura delle wireless sensors network il fatto che i nodi della rete possano trascorrere parte della loro vita utile nello stato di nodi "ibernati" e quindi non connessi al resto della rete ;
- **Multihop**. Data la ridotta potenza in trasmissione dei nodi, dettata sia da criteri di power budget, sia da necessità di reusability spaziale delle frequenze, le reti si troveranno ad operare in multi-hop. Questo pone dei problemi di raggiungibilità dei nodi e di affidabilità della rete;
- **Difficoltà** nello stabilire un **sincronismo di rete** (in alcuni casi, impossibilità materiale) e conseguente necessità di algoritmi ad-hoc per il recupero del sincronismo dai messaggi ricevuti;
- **Naming and addressing**. La scelta di una convenzione di naming and addressing è di importanza cruciale e dipende fortemente dal singolo contesto applicativo. In alcuni casi potrebbe infatti avere senso decidere che ciascun nodo di rete abbia un proprio identificativo unico; in altri casi potrebbe invece convenire che il nodo x ospitante un sensore per la sostanza y possa essere identificato come "uno degli n sensori per la sostanza y"; in altri casi ancora, può convenire fare prevalere un criterio geografico e quindi indirizzare, per esempio "tutti i nodi di una determinata regione/cluster", o indirizzare il solo nodo "capo cluster", oppure indirizzare secondo un criterio funzionale, quindi ad esempio "tutti i nodi che hanno

dati da trasmettere" o infine utilizzare un criterio tipo publish and subscribe (o semantic addressing), e quindi disseminare messaggi del tipo "offresi misura della sostanza y" oppure "cercasi nodo con a bordo un sensore della sostanza y" piuttosto che indirizzare i singoli nodi. Ovviamente le soluzioni miste sono in numero ancora più elevato. Questa vastità di possibilità di scelta condiziona fortemente la scelta dei protocolli di MAC, di routing e gli schemi di data fusion;

- **Sicurezza.** I protocolli 802.11, basati inizialmente sulla crittografia WEP, hanno visto numerosi sviluppi, ad esempio il passaggio dalla crittografia WEP delle chiavi alla tecnica WPA, che rimuoveva la maggior parte dei problemi di sicurezza rendendo le reti wireless discretamente sicure. Nel 2004 venne sviluppato il WPA2 che abbandona l'RC4 come algoritmo di codifica per passare al più sicuro Advanced Encryption Standard - AES. Le varie opzioni di sicurezza disponibili comportano però livelli di complessità crescente per la configurazione e l'adeguamento del firmware e di drive di sistema operativo di Access Point e schede di rete wireless. Il problema di sicurezza principale delle reti ad-hoc è l'intercettazione, che mette a rischio per la privacy degli utenti (potrebbero ad esempio essere sottratti segreti industriali o dati bancari). L'accesso abusivo alla rete è rischioso anche perché non è possibile rintracciare a posteriori gli autori di comportamenti pericolosi o illegali. La sicurezza nelle WMNs è gestita soltanto in modo peer-to-peer tra coppie di nodi (uso del protocollo 802.11i). 802.11s definisce, comunque, autenticazione per password e scambio di chiavi. IEEE802.15.4 e Zigbee offrono elevato livello di sicurezza che viene supportata a livello di link, ma anche a livello rete ed applicativo. Reti basate su 6lowPAN potrebbero ereditare meccanismi di sicurezza di livello di rete (ed esempio IPsec o simili). Sia gli algoritmi di Zigbee che soluzioni come IPsec su 6LowPAN potrebbero essere troppo onerosi in dispositivi a basse capacità di batteria e di processing. ROLL, come definito nel *draft-ietf-roll-rpl-19* del 2011, utilizza meccanismi di livello di link se esistenti o i propri ma in questo caso utilizza chiavi pre-installate o si affida ad autorità di certificazione esterne non definite nella specifica.

Trend evolutivi

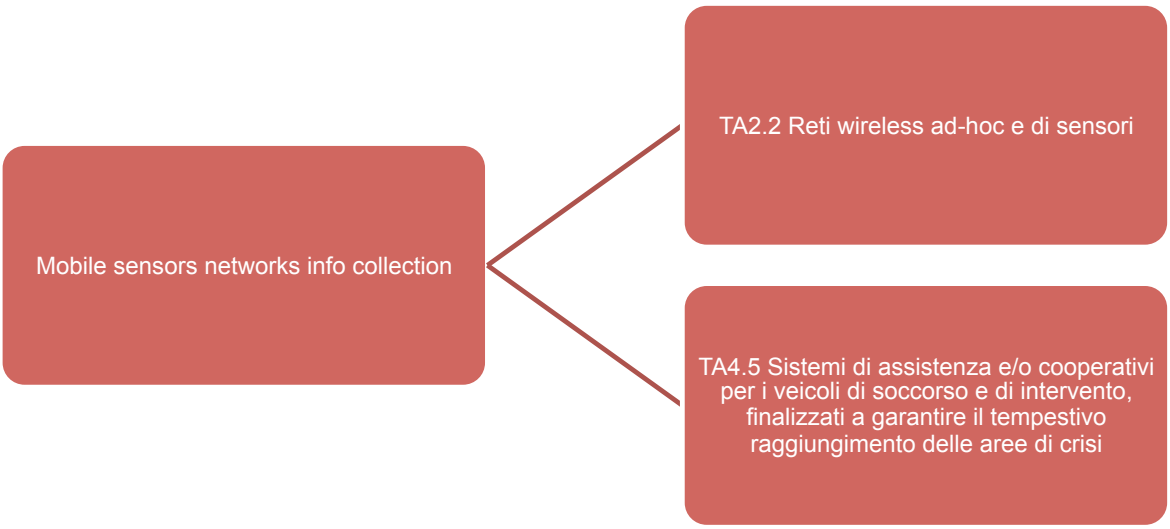
Gli sviluppi della sicurezza nell'ambito delle reti di sensori ad-hoc riguardano in particolare lo sviluppo del protocollo 802.11ad. I trend evolutivi principali nelle reti di sensori riguardano le scarse capacità computazionali dei nodi e consistono nella definizione di tecniche di crittografia più efficienti in termini energetici e di risorse computazionali. Inoltre, un miglioramento tecnologico in grado di fornire un forte incentivo all'adozione e alla diffusione del protocollo IETF ROLL in reti formate da sensori caratterizzati da batteria, memoria e capacità di processing limitati, si prevede essere l'integrazione di tali reti con autorità di certificazione esterne per ottenere un livello di sicurezza complessivo ottimale in queste tipologie di scenario.
Le principali criticità tecniche relative all'applicazione della suite TCP/IP su base "as is" a questo tipo di reti sono:

- IP funziona se c'è continuità (cioè se il percorso è mantenuto) tra tutti i nodi intermedi tra sorgente e destinazione durante il trasferimento del singolo pacchetto
- TCP è inefficiente in caso di disconnessioni di breve durata e di jitter sul ritardo di trasmissione
- UDP è intrinsecamente "unreliable", non prevedendo acknowledge, ed inoltre non supporta il meccanismo "store and forward".

Queste tematiche sono attualmente oggetto di analisi, studio e specificazione dei relativi algoritmi e metodi presso il Delay Tolerant Networking Research Group (DTNRG) dell'IRTF e i partecipanti al programma Disruption Tolerant Networking del DARPA. Molti dei protocolli di networking proposti derivano da studi per reti ad alto ritardo, da impiegarsi nelle comunicazioni terra-bordo-terra per le missioni spaziali.

Livello attuale di TRL TRL 6-7

I TA di riferimento TA2 ,TA6



- **Advanced ELINT Capabilities for Spaceborne Radars**

Descrizione dello Stato dell'arte

Gli attuali radar da satellite sono particolarmente orientati verso le funzioni di Osservazione della Terra. Ulteriori servizi di sorveglianza possono essere previsti tramite l'impiego di funzionalità di ELINT (Electronic Intelligence) per il monitoraggio dello spettro elettromagnetico (EM) e l'identificazione delle sorgenti EM specialmente in termini di DOA (Direction of Arrival).
Al momento queste funzionalità sono sviluppate nel segmento di terra e sull'equipment aviotrasportato mentre la loro applicazione sui sistemi satellitari viene vista come una capability secondaria nonostante le grandi potenzialità che potrebbe apportare. Sono pertanto necessari studi analitici e sviluppi tecnologici preliminari per svilupparne le prestazioni a partire dall'attuale livello embrionale di questa tecnologia sul sistema satellite.

Descrizione dei Gap tecnologici

I radar satellitari con caratteristiche ELINT possono beneficiare di evoluzioni della tecnologia delle antenne phased array di tipo multichannel; un'altra tematica di particolare interesse riguarda le architetture transceiver di tipo supereterodina basate su core digitali partizionati sia in software che in hardware. Tali miglioramenti potrebbero consentire tecniche di processamento avanzate di tipo ELINT.

Trend evolutivi

I radar satellitari devono potenziare i modi di misura (ovvero i modi con i quali acquisiscono dati per il processing di tipo SAR) con ulteriori funzioni orientate alla sorveglianza ed alla intelligenza elettronica allo stesso modo di quanto già avviene per i sistemi di sorveglianza aerea che implementano molte modalità di tipo watch-dog.
In questa prospettiva, sono in via di svolgimento delle ricerche preliminari per identificare le tecniche ELINT più adatte all'implementazione satellitare e per definire le caratteristiche architetturali necessarie per un radar satellitare. L'accento è posto soprattutto sulla condivisione delle risorse (ad esempio la condivisione della stessa apertura di antenna per assolvere sia ai task di tipo imaging che alle applicazioni di tipo ELINT)

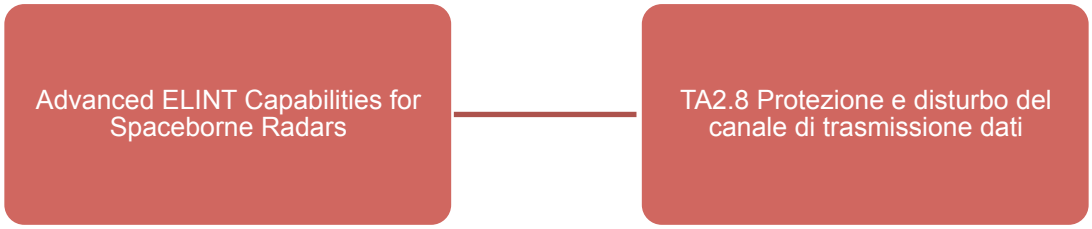
Livello attuale di TRL

Gli attuali radar satelitari non implementano capacità di tipo ELINT. Quindi la TRL ELINT si attesta sul livello 1 in qualche caso estendibile fino al livello 3.

Step Necessari per arrivare a TRL + 1

Gli step necessary sono:
- Consolidamento delle Enabling technologies.
- Chiarificazione dello scenario Operativo.

I TA di riferimento TA 1



- **Chemical, Biological, Radiological and Nuclear (CBRN) protection and decontamination equipment - Biotechnology-based systems**

Descrizione dello Stato dell'arte

Gli agenti per una potenziale contaminazione biologica delle filiere alimentari includono organismi responsabili di malattie per uomini, animali e piante, da tutti i gruppi biologici: virus, batteri, funghi, protozoi e piccoli invertebrati. Inoltre, le tossine prodotte da alcuni di questi organismi possono essere usate come contaminanti. Gli agenti biologici possono essere usati per contaminare prodotti alimentari, o per colpire raccolti e aziende agricole, o possono essere dispersi in aria e in acqua. Tutte le entità biologiche coinvolte nella produzione e nel processamento di alimenti, e anche molti contaminanti, possono essere riconosciute analizzando gli acidi nucleici o le proteine presenti nel prodotto, usando sistemi basati sulle biotecnologie. I metodi per identificare i contaminanti richiedono che si distinguano le componenti o gli ingredienti accettati dalle componenti non volute o nocive. Attività di ricerca recenti si sono concentrate sullo svilup-

po e sull'analisi di metodi analitici innovativi e affidabili per identificare le componenti biologiche presenti negli alimenti. L'identificazione delle componenti biologiche anomale o non desiderate nei prodotti alimentari può essere eseguita mediante la identificazione e la classificazione del materiale genetico (fingerprint) appartenente ad animali, piante o microrganismi utilizzati nella produzione o nel processamento del prodotto alimentare. La ricerca dei contaminanti patogeni negli alimenti comporta convenzionalmente l'isolamento dei microrganismi dal prodotto, la loro crescita o arricchimento su terreni selettivi e la loro identificazione con saggi biochimici o immunologici. Il processo può essere lungo e alterato da falsi negativi. Un approccio diverso è l'analisi degli acidi nucleici, DNA o RNA, dei microrganismi che si credono essere contaminanti. L'uso della Real-time PCR quantitativa (qtRT-PCR) può consentire la quantificazione dei batteri, e l'identificazione non ambigua della specie batterica. Alternativamente, metodi basati sul riconoscimento delle proteine mediante anticorpi possono essere adottati, ad esempio Enzyme linked assays (ELISA). Molti diversi metodi sono disponibili per la rilevazione rapida di componenti patogene multiple in modo simultaneo. Uno dei più avanzati è l'uso dei DNA microarray per la rilevazione dei patogeni. Il vantaggio dell'approccio microarray è l'analisi simultanea di diversi bersagli in un solo esperimento, in cui l'ibridazione dei DNA bersaglio a sonde specifiche conferma l'identità e perciò consente il riconoscimento del contaminante. Il mercato per questi sistemi si sovrappone al mercato della diagnostica in campo medico, nel controllo degli alimenti, nel monitoraggio ambientale. Naturalmente, il potenziale è molto alto, ma una stima non è possibile.

Descrizione dei Gap tecnologici

Il rilevamento precoce è il principale gap nella tecnologia per contrastare gli attacchi alla sicurezza degli alimenti. In questo, i sistemi basati sulle biotecnologie possono dare un contributo. Il tempo richiesto per l'identificazione dei patogeni o dei composti chimici è un punto critico, perché definisce la velocità e l'efficacia nel ritiro del prodotto dalla disponibilità dei consumatori. In particolare, è l'identificazione dei prodotti alimentari colpiti che provoca i ritardi maggiori. Una risposta sta negli approcci che possano essere applicati in campo. L'interesse nella qtRT-PCR per indagini di sicurezza dipende proprio dalla sua applicabilità in condizioni di campo, con alcuni sistemi portatili per RT-PCR. Uno di questi è il termociclatore R.A.P.I.D. (Ruggedized Advanced Pathogen Identification Device) che è stato applicato con successo in campo per la rilevazione di patogeni quali Francisella tularensis. Un altro passo essenziale vero l'applicazione in campo per la rilevazione precoce è lo sviluppo di sistemi rapidi per la rilevazione di DNA o proteine nell'ambiente, di metodi RT-PCR senza estrazione del DNA, o di sistemi di estrazione su stato solido, per evitare lunghe procedure prima di una PCR diagnostica o di analisi immunologiche.
Un completo sistema integrato che colleghi le informazioni sulla storia e sul movimento dei prodotti lungo la filiera, con parametri obiettivi di qualità e sicurezza misurati in punti critici, aumenterebbe sicuramente la preparazione verso minacce intenzionali o accidentali.

Trend evolutivi

Diverse piattaforme innovative basate sul campionamento automatico e sull'analisi di acidi nucleici o proteine sono state sviluppate di recente per il monitoraggio di luoghi ad alto rischio, specialmente per la difesa contro il bioterrorismo. Perciò un trend riguarda il campionamento per la sorveglianza e il trattamento dei campioni, che deve essere ridotto al minimo prima dell'analisi. Per aumentare la velocità dell'analisi, i lab-on-chip sono le applicazioni più avanzate

di biosensori portatili, riproducendo complesse tecniche analitiche su piccoli vetrini di pochi centimetri quadrati. Ad oggi, molte tecniche analitiche sono state integrate o associate su sensori Lab-on-chip, comprese PCR, RT-PCR e microarray. Accoppiare la microfluidica per l'ibridazione del DNA con letture colorimetriche può fornire soluzioni innovative per l'applicazione delle piattaforme "near-line" in punti critici della filiera alimentare e per strumenti veloci per il monitoraggio in caso di attacchi terroristici. Di recente, il DNA applicato ai biosensori è stato sfruttato come componente attiva nella generazione di un segnale elettrico. Infine, l'analisi e integrazione dei dati con altre informazioni, al fine di un efficiente supporto alle decisioni è uno degli argomenti che la ricerca attuale sta studiando. Questi trend sono stati chiaramente espressi negli ultimi bandi per progetti di ricerca Europei (2011).

Livello attuale di TRL TRL 5

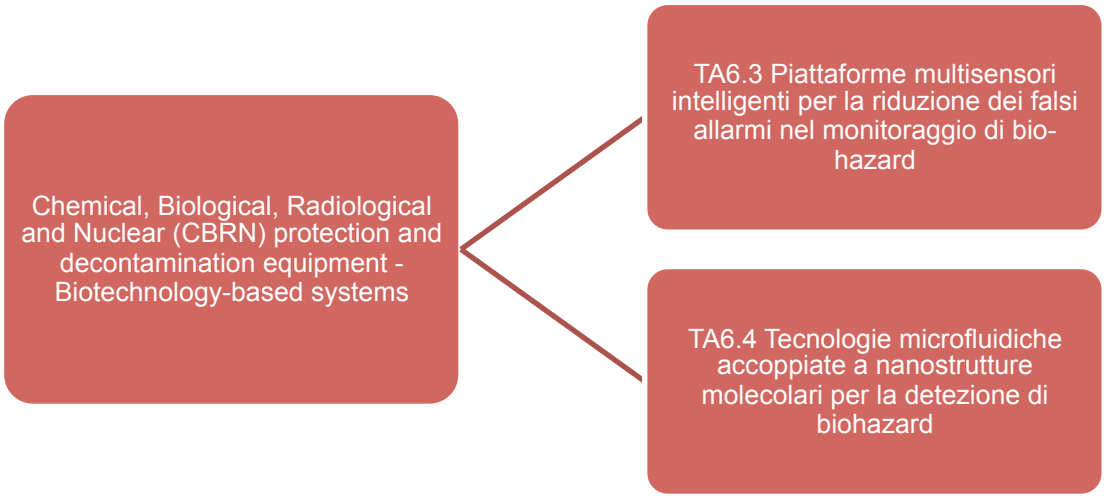
Step Necessari per arrivare a TRL + 1

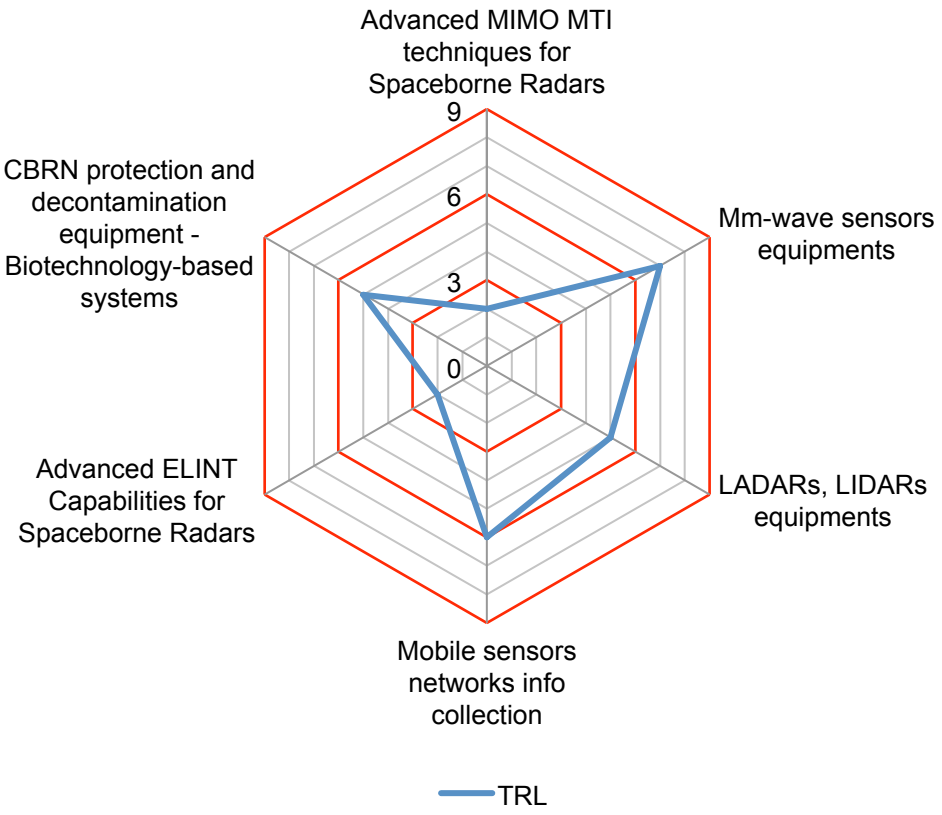
Il passaggio successivo richiede la miniaturizzazione delle piattaforme analitiche con portabilità sul campo e interoperabilità; nuovi approcci strategici per l'identificazione simultanea degli agenti; definizione delle strategie di campionamento e trattamento; interconnessione con sistemi ICT per l'acquisizione automatica e l'analisi di dati.

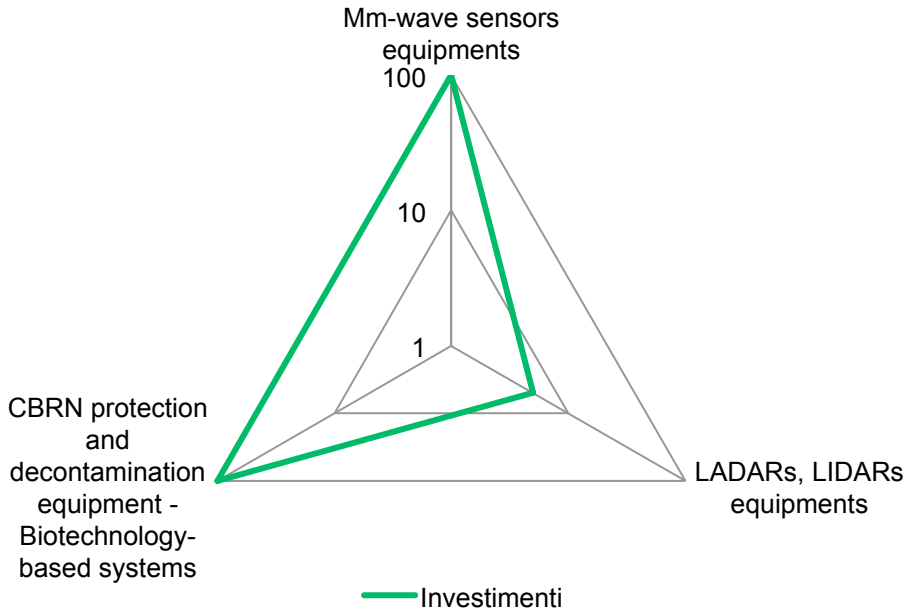
Costo associato per arrivare a TRL +1 (anni ed investimento economico)

Il prossimo passaggio potrebbe essere raggiunto nei prossimi 3 anni, con un robusto piano di investimenti che si stima nell'ordine di diverse centinaia di M€ a livello mondiale.

I TA di riferimento TA6, anche TA2 per le integrazioni con ICT.




Advanced MIMO MTI techniques for Spaceborne Radars
9
6
3
0
Mm-wave sensors equipments
LADARs, LIDARs equipments
Mobile sensors networks info collection
Advanced ELINT Capabilities for Spaceborne Radars
CBRN protection and decontamination equipment - Biotechnology-based systems
TRL


Mm-wave sensors equipments
100
10
1
LADARs, LIDARs equipments
CBRN protection and decontamination equipment - Biotechnology-based systems
Investimenti

4.2.2 Forensic technologies

Con Scienze Forensi viene generalmente indicato un ampio spettro di Scienze e competenze di interesse sia per il sistema legale che per il settore della Sicurezza, essendo in relazione con azioni criminali e/o terroristiche. Le Scienze Forensi comprendono molte discipline, quali antropologia, biologia, geologia, chimica, ingegneria, genetica, medicina, patologia, fonetica, informatica, psichiatria e tossicologia. Esse fanno riferimento all'analisi di molti tipi di materiali complessi, comprendenti sia materiali inorganici che organici e biologici, che possono essere ad esempio parte costituente di munizioni, GSR, DNA, impronte digitali, cosi come metalli, munizioni, frammenti di bombe, tracce chimiche e biologiche, droghe ed esplosivi da individuare ai check point. Tale area risulta quindi molto complessa e dinamica, a causa della confluenza di esigenze e bisogni propri della Società, così come da bisogni e richieste provenienti dal sistema legale ed istituzionale.La domanda per una diagnostica di alta qualità è generalmente in crescita e gli avanzamenti tecnologici degli ultimi anni sono stati di particolare rilevanza, incluso il design e la produzione di apparecchiature portatili e banche dati per una rapida ed affidabile diagnostica e una precisa identificazione di particolari e caratterizzanti specificità.

Ambiti prioritari di ricerca

- Ballistics
- Fire Arms and projectiles identification
- Drug Analysis
- Explosion investigation
- Ballistics

Descrizione dello Stato dell'arte

La balistica è la scienza che in particolare analizza le modalità d'uso delle armi in azioni criminali e terroristiche, tenta di identificare utili correlazioni ed esamina tutte le fasi del processo di sparo dall'espulsione dell'ogiva dopo essere stato accelerata lungo la canna dell'arma, alle interazioni che essa subisce sino allo studio dell'effetto dell'impatto. Le indagini balistiche hanno lo scopo di determinare alcune caratteristiche dell'ogiva e del suo tragitto dall'arma al bersaglio quali l'angolo di incidenza e la direzione di provenienza oltre alle tracce che l'interazione la canna dell'arma impartisce all'ogiva. Tale interazione lascia infatti caratteristiche tracce evidenti sull'ogiva soprattutto ad opera delle rigature a spirale create in fase di produzione dell'arma per impartire una direzione precisa ed una migliore accuratezza al proiettile. Poiché le rigature delle canne o altri segni lasciati dalle lavorazioni meccaniche sulle componenti dell'arma possono essere differenti, le tracce risultanti sull'ogiva e sul bossolo possono essere considerate uniche e permettono quindi di associare un ogiva espulsa ad una canna di una arma e quindi, fornire indicazioni utili per la ricostruzione di una scena del crimine o di una azione terroristica, facendo corrispondere striature del proiettile (o strie) con la canna rigata attraverso il quale è stato licenziato, o facendo corrispondere segni sul bossolo di marchi in camera, e altre parti.

Descrizione dei Gap tecnologici

È generalmente accettato che due armi anche se dello stesso calibro e modello producono tracce sull'ogiva differenti in quanto micro-differenze nelle rigature della canna producono micro-difetti casuali che permettono una correlazione diretta fra arma e ogiva. Lo studio di tali micro-difetti si basa sulla loro osservazione mediante microscopia ottica, generalmente condotta valutando comparativamente l'aspetto di tali tracce, ma che, assistita da adatti software di analisi delle immagini, potrebbe essere più accurata e fornire migliori e più dettagliate informazioni. Il gap tecnologico esistente risiede nel miglioramento dell'attendibilità della valutazione che deve essere oggettiva e non frutto di una valutazione personale, anche se di un esperto; inoltre, lo studio si dovrebbe estendere anche ai micro- e nano-difetti o tracce per associare con certezza una ogiva connessa ad un evento criminale o terroristico ad una arma.

Trend evolutivi

Un problema che potrebbe presentarsi è la possibile alterazione delle tracce considerate come un'impronta digitale di un'arma che potrebbero essere alterate dall'utilizzo di particolari accorgimenti come pure si deve incrementare l'oggettività delle valutazioni anche mediante l'utilizzo di software di analisi delle immagini dedicati.

Livello attuale di TRL TRL6

Attualmente gli esperti di balistica identificano l'arma utilizzata dallo studio delle tracce lasciate sull'ogiva rinvenuta sulla scena del crimine o di una azione terroristica. Lo studio di tali micro-difetti si basa sulla loro osservazione mediante microscopia ottica generalmente condotta valutando comparativamente l'aspetto di tali tracce, ma che assistita da adatti software di analisi delle immagini potrebbero essere più accurate e fornire migliori e più dettagliate informazioni.

Step Necessari per arrivare a TRL + 1

Gli step necessari per migliorare l'attuale stato dell'arte riguardano sia la rilevazione delle tracce che dovrebbe estendersi anche agli aspetti nano sia il miglioramento dell'attendibilità della

valutazione che deve essere oggettiva e non frutto di una valutazione personale anche se di un esperto ma frutto diuna comparazione comparativamente assistita da adatti software di analisi delle immagini 3D, che potrebbero risultare più dettagliate fornendo informazioni più accurate e precise.

I TA di riferimento TA3, TA6

- **Fire Arms and projectiles identification**

Descrizione dello Stato dell'arte

Le armi da fuoco collegate o collegabili ad un crimine o ad una azione terroristica, possono essere rinvenute sulla scena del crimine, su elementi sospetti, in autoveicoli o mezzi di trasporto sia perché esse siano già state utilizzate, o perché lo potrebbero essere, per condurre azioni terroristiche e criminose. Dal punto di vista della sicurezza sono quindi, elementi da sottoporre a controllo e verifica considerando anche il grande numero di potenziali informazioni ottenibili riguardo il loro uso e provenienza; medesimo interesse riveste il munizionamento ed i materiali inerenti (inneschi, residui di sparo etc.), le caratteristiche balistiche delle armi da fuoco e le informazioni collegabili ad azioni condotte con finalità criminali o terroristiche. Tutte queste informazioni possono confluire e costituire una o più banche dati che, dotate di un adatto sistema esperto permettano una loro agevole e finalizzata analisi ed elaborazione, capacità sempre più importante considerando il rapido sviluppo e la produzione di nuove armi, munizionamento ed inneschi che vengono prodotti sia con finalità legali e environmentally friendly (inneschi privi di piombo) ma anche criminali (inneschi in grado di non essere monitorati e rintracciati) e che necessitano quindi per essere identificati di nuove conoscenze ed approcci come pure di normative aggiornate.

Descrizione dei Gap tecnologici

Le metodologie per la definizione di un sistema esperto in grado di riconoscere la presenza di osservabili utili all'identificazione di eventi dolosi o potenzialmente dolosi collegati all'uso delle armi è di grande interesse per la ricostruzione degli eventi e l'identificazione di aspetti significativi per azioni di sicurezza preventiva. L'attività dovrebbe prevedere l'acquisizione e la creazione di banche dati riguardanti informazioni chimiche, morfologiche e strutturali di osservabili utili all'identificazione di eventi dolosi o potenzialmente dolosi e la partecipazione alla definizione di un sistema esperto diagnostico-informatico. Si ricorda che la precisa identificazione di materiali legati all'uso di armi da fuoco potrebbe essere affetto da limitazioni quali l'utilizzo di armi sconosciute o modificate, di inneschi e munizionamento inusuale, di particolato atmosferico con caratteristiche simili ai GSR e contributi esogeni di varia natura e provenienza, anche considerando che alcuni inneschi e materiale propellente potrebbero essere stati modificati per renderli non identificabili e tracciabili.

Trend evolutivi

Il metodo più utilizzato e validato negli ultimi decenni per accertare l'utilizzo, il maneggaiamento o il trasporto di armi da fuoco è il monitoraggio della presenza di residui di sparo (GSR). I GSR sono particelle micrometriche la cui morfologia e composizione chimica sono caratteristiche e per essere identificate devono essere confrontate con quelle delle varie tipologie di GSR note

che fungono da standards e sono state raccolte e studiate secondo una precisa metodica. Nonostante l'ampio lavoro fin qui svolto permangono incertezze dovute a falsi positivi, contaminazioni o GSR ignoti generati da inneschi e munizionamenti "esotici" ignoti alla forze dell'ordine e alla sicurezza che giungono sino a noi per effetto della globalizzazione. Anche per ovviare a tali situazioni la creazione di una banca dati dedicata potrebbe essere di grande utilità, i risultati attesi da tale sistema prevedono la capacità di individuare la natura e la provenienza di materiali incogniti potenziali indicatori di reato o di pericolo criminale o terroristico, distinguendo le evidenze dirette ed indirette di un evento doloso e di discriminare materiali artefatti o modificati.

Livello attuale di TRL TRL6

L'utilizzo di una arma da fuoco da parte di un criminale o di un terrorista produce la combustione dell'innesco e della polvere da sparo contenuti in una cartuccia e la conseguente formazione dei residui di sparo che possono comprendere anche elementi proveniente dall'arma, dall'ogiva e dal bossolo.
I GSR sono comunemente studiati mediante microscopia elettronica a scansione e analisi chimica a dispersione di energia (SEM-EDS) e l'attribuzione della natura di una particella alla classe dei GSR deve rispettare alcune specifiche riguardanti composizione chimica e morfologia che deve essere confrontata con i risultati delle indagini micro-chimiche e morfologiche condotte su particelle note come GSR e prelevate durante test di sparo condotti secondo metodiche standard e riproducibili.

Step Necessari per arrivare a TRL + 1

Alcuni miglioramenti sono possibili per migliorare l'identificazione e la tracciabilità:

- creazione di una banca dati e di un sistema esperto;
- l'aggiunta intenzionale di elementi "esotici" agli inneschi o alla polvere da sparo quali il neodimio o il praseodimio per la sicura identificazione della natura GSR di una particella di sparo;
- l'utilizzo di microinserti con variabile composizione chimica in una arma o in una cartuccia;
- l'utilizzo di micro-marchi invisibili (tipo codice a barra) su cartuccie, incamiciatura e arma da fuoco per una sicura tracciabilità.

I TA di riferimento TA03

- **Drug Analysis**

Descrizione dello Stato dell'arte

L'analisi delle droghe d'abuso è finalizzata all'identificazione dei principi attivi stupefacenti contenuti in una matrice illegale e alla loro quantificazione, cioè la determinazione del grado di purezza nella matrice. Attraverso la misura del grado di purezza si perviene alla definizione del numero di dosi ricavabili dal materiale in sequestro, alla sua potenzialità intossicante e alla stima del valore economico del materiale sequestrato. Le legislazioni nazionali che adottano un sistema tabellare necessitano delle informazioni qualitative e quantitative sulla droga sequestrata per poter applicare le sanzioni penali, la cui entità può dipendere dalla tipologia delle droghe e dai quantitativi di principio attivo ricavabili. Le droghe d'abuso non rappresentano una categoria omogenea di sostanze chimiche, pertanto l'approccio metodologico dell'analisi chimica può variare di molto da sostanza a sostanza. La maggior parte di tecniche d'analisi utilizzate

è di tipo cromatografico, infatti difficilmente si può prescindere da un momento separativo del principio attivo dalla matrice. Spesso a queste sono associate tecniche spettroscopiche (spettrometria di massa), utili per identificare e costruire dei profili di composizione delle sostanze illegali.

Descrizione dei Gap tecnologici

Il problema dell'identificazione certa di una droga d'abuso è molto sentito per l'applicazione della legge penale sugli stupefacenti. Molte sostanze stupefacenti presentano degli isomeri di struttura o degli stereoisomeri che hanno diverso potere drogante o diversi livelli di tossicità. Non sempre è facile distinguere questi isomeri, così come anche certi analoghi strutturali e spesso è necessario applicare molteplici tecniche analitiche alla stessa matrice con aggravio di costi e allungamento dei tempi di analisi. Un miglioramento nelle capacità di distinzione di queste sostanze è auspicabile, anche per evitare che le legislazioni nazionali siano portate ad ampliale il numero delle sostanze vietate includendo anche isomeri e analoghi di struttura non stupefacenti o scarsamente rilevanti dal punto di vista tossicologico. Una ulteriore difficoltà è quella di ottenere comparazioni tra stupefacenti, tramite costruzione di banche dati dinamiche, per valutare una origine comune del materiale sequestrato in contesti diversi con un buon grado di attendibilità.

Trend evolutivi

Una delle tematiche più rilevanti dal punto di vista investigativo è quello della comparazione di droghe. La comparazione chimica (chemical profiling) può contribuire a identificare i canali di traffico e a stabilire collegamenti fra diversi gruppi criminali. Queste analisi possono anche servire ad associare una partita di droga alle sue origini in termini di sito produttivo o di laboratorio clandestino. Sono analisi già in parte sviluppate per le principali sostanze stupefacenti (cocaina, eroina, amfetamina), ma è necessario migliorare il loro livello di attendibilità ed estenderle a un maggior numero di sostanze.

Livello attuale di TRL

TRL6. Le tecnologie di riferimento sono gascromatografia, HPLC, spettrometria di massa. Sono tecniche mature e largamente applicate in campo chimico analitico. Attualmente non si può prescindere da tecniche separative (cromatografiche), che isolino l'analita dalla matrice, mentre è auspicabile lo sviluppo di tecniche dirette su matrice che operino anche in presenza di sostanze interferenti con le tecniche tradizionali

I TA di riferimento TA3, TA6

- **Explosion investigation**

Descrizione dello Stato dell'arte

La diffusione di eventi terroristici in tutto il mondo nell'ultimo decennio ha sottolineato l'importanza della individuazione degli esplosivi nascosti ed ha portato a richieste di nuove ed avanzate tecnologie per proteggere il pubblico. Poiché la maggior parte degli esplosivi rilascia poco vapore, non è possibile rilevarli in modo efficace mediante l'uso di metodi che sono am-

piamente utilizzati per altri prodotti chimici. Rilevare esplosivi è un compito molto complesso e costoso a causa di una serie di fattori, quali la grande varietà di composti che possono essere impiegati come esplosivi, il vasto numero di mezzi di distribuzione, e la mancanza di sensori economici che forniscano insieme una elevata sensibilità e selettività. Un'alta sensibilità assieme alla selettività, combinate con la capacità di abbassare i costi di produzione e distribuzione di tali sensori, risultano fattori essenziali per vincere la battaglia sugli esplosivi utilizzati dai terroristi. Tra i congegni esplosivi gli IED rappresentano bombe fatte in casa costruite e distribuite in modi diversi da quelli convenzionali e tipici delle azioni militari. Essi possono essere costruiti da esplosivi militari convenzionali, come un tutto artiglieria, attaccato ad un meccanismo detonante. Essi sono estremamente diversificati nel design e possono contenere molti tipi di iniziatori, detonatori, penetratori e cariche esplosive. Inoltre, esiste il rischio che sostanze chimiche tossiche, biologiche o materiali radioattivi possano essere aggiunti ad un dispositivo, creando così altri effetti letali, al di là delle conseguenze classiche attribuibili all'esplosione stessa e normalmente associate all'uso di bombe. Inoltre, una volta avvenuta l'esplosione è di fondamentale importanza capirne l'origine e le cause.

Descrizione dei Gap tecnologici

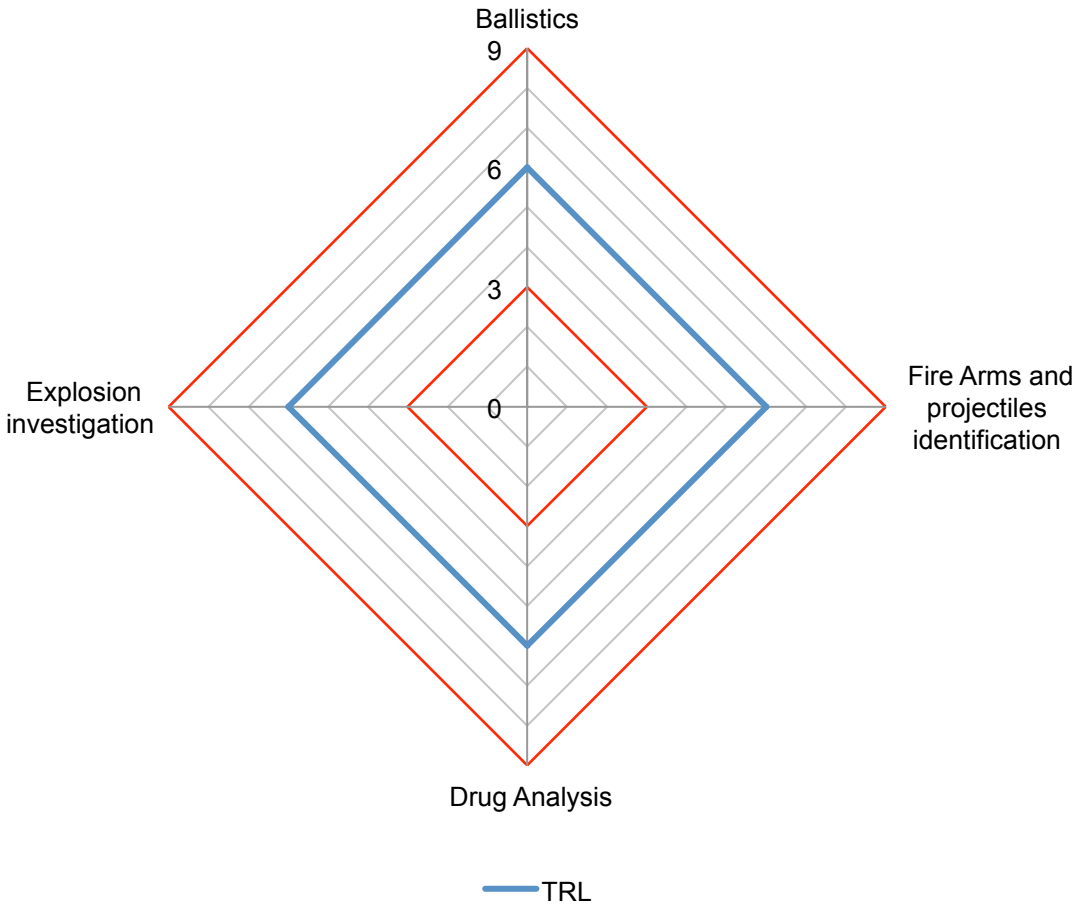
Il settore delle esplosioni, a causa della sua natura in parte investigativa ed in parte forense, coinvolge un grande numero e una grande varietà di competenze ed expertises. Inoltre va considerato il fatto che le bombe possono essere esse stesse oggetto di grande variabilità, da molto semplici a molto sofisticate, in funzione di quante competenze chimiche abbia il sospetto in questione.

Trend evolutivi

Generalmente gli esplosivi vengono rilevati sulla base delle proprietà fisiche dei loro vapori, e molte ricerche sono indirizzate verso l'impiego di dispositivi micromeccaniche

Livello attuale di TRL TRL6

I TA di riferimento TA3, TA6


Ballistics
9
6
3
0
Fire Arms and projectiles identification
Drug Analysis
Explosion investigation
TRL

4.3 Systems & Services functions

4.3.1 Human behaviuor and Identity Management

Ambiti prioritari di ricerca

- Behavioural analyses
- Identity management
- Biometrics

- **Behavioral Analysis**

Descrizione dello Stato dell'arte

L'analisi video in tempo reale è un settore in ampio sviluppo nella comunità scientifica dato il suo risvolto pratico in molti ambiti applicativi. L'ambito applicativo di maggiore interesse è quello della videosorveglianza.In tale applicazione l'obiettivo principale è il controllo, ai fini della sicurezza, di aree sensibili come stazioni, aeroporti, zone di particolare interesse turistico, etc. Un sistema di videosorveglianza intelligente ha l'obiettivo di individuare gli eventi della scena, interpretarli e segnalare quelli di interesse all'operatore. Ci sono necessità immediate di sistemi di videosorveglianza intelligente in applicazioni commerciali, ma soprattutto militari e di sicurezza. Montare telecamere, infatti, è abbastanza semplice ed economico, ma trovare le risorse umane disponibili ad analizzarne i contenuti è costoso. Anche se le telecamere di sorveglianza sono già molto presenti in banche, negozi e parcheggi, i dati video sono attualmente utilizzati come strumento legale a posteriori, perdendo così il suo vantaggio principale di essere un mezzo di analisi attiva e real-time. Quello che è necessario è il continuo monitoraggio per allertare gli operatori di sicurezza di un furto in corso, o un vagabondaggio sospetto, e così via. La videosorveglianza ha ottenuto, nell'ultimo decennio, un crescente interesse sia dal punto di vista scientifico che commerciale. Grandi progetti di ricerca dedicati alla ricerca di videosorveglianza sono stati condotti negli Stati Uniti (DARPA e VSAM), Europa (ESPRIT PASSWORDS, AVS-PV, VIEWS) e Giappone (CooperativeDistributed Vision project). La videosorveglianza sta diventando molto importante anche dal punto di vista scientifico come dimostrato da recenti workshop e conferenze internazionali (come ad esempio le conferenze Advanced Video and Signal-BasedSurveillanceAVSS e Performance Evaluation of Tracking and SurveillancePETS) e special issue su riviste (come per esempio l'International Journal of Computer Vision).

Descrizione dei Gap tecnologici

L'analisi video in tempo reale, nella comunità scientifica, ha avuto uno sviluppo molto ampio negli ultimi anni. Un sistema di videosorveglianza, tipicamente, si basa sull'analisi delle traiettorie degli oggetti in movimento, dalle quali viene effettuata l'analisi comportamentale. Esistono ad oggi, nella comunità scientifica, moltissimi algoritmi per l'analisi delle traiettorie. D'altra parte, però, mancano i risvolti tecnologici e pratici dei risultati ottenuti a livello scientifico. Infatti, esistono molte società che operano nella sicurezza e diversi sistemi commerciali che rivendicano una serie di risultati in termini di efficacia dell'analisi comportamentale. Il motivo principale di questa mancanza è dovuto al fatto che i ricercatori che hanno lavorato nell'ambito dell'analisi video e comportamentale, hanno proposto nuovi algoritmi che risultavano efficaci su video di prova, ma che non risolvono bene i problemi che si presentano nell'applicazione reale di tali sistemi. Nell'uso quotidiano di questi sistemi, infatti, sorgono molti più problemi di quanti sono stati esaminati dalla comunità scientifica. I principali problemi non affrontati sono i seguenti: segnale rumoroso (telecamere a basso costo), ambiente non controllato (variabilità della scena, non idealità delle traiettorie, etc.), complessità delle interazioni nella scena.

Trend evolutivi

Oggi i principali sistemi di videosorveglianza si limitano all'analisi monocamera, ed uno dei trend evolutivi di tali sistemi è l'analisi di aree molto vaste attraverso l'uso di più telecamere.

In questo contesto la ricerca si sposta dall'analisi delle traiettorie su singola telecamera, alla ricostruzione della traiettoria di un soggetto che transita dal punto di vista di una telecamera ad un altro. Inoltre si aggiungono le problematiche di calibrazione delle telecamere, al fine di avere gli stessi punti di riferimento tra le varie viste, e problematiche di sincronizzazione tra gli eventi riconosciuti nelle varie inquadrature. Un altro trend di tali sistemi, nasce dall'esigenza di catalogare la ingente mole di dati che risultano dall'utilizzo della funzionalità di registrazione video. Oggi è molto semplice memorizzare una grande quantità di materiale, ma risulta molto difficile recuperare da questi dati delle sequenza video utili agli operatori. Si pensi che, in occasione degli attentati di Londra del 2005, tutte le scene di interesse erano memorizzate negli archivi della sicurezza inglese, ma ci sono voluti circa 4 mesi per estrarre le immagini utili al riconoscimento degli attentatori. In questo ambito, dunque, le attività di ricerca e sviluppo si sposteranno su sistemi di retrieval delle informazioni multimediali.

Livello attuale di TRL TRL 5

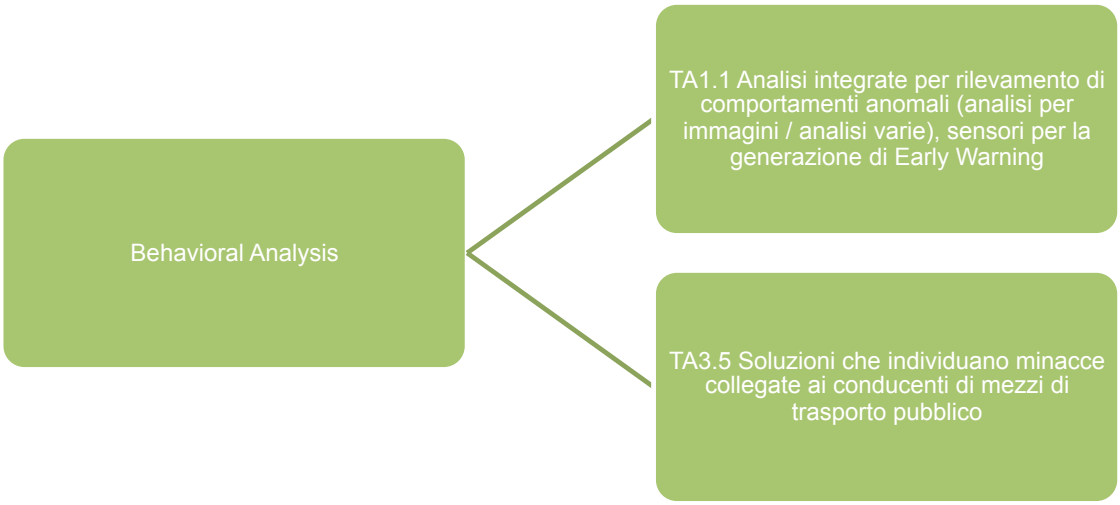
Step Necessari per arrivare a TRL + 1

Per poter iniziare a superare i gap tecnologici sopra descritti e raggiungere un nuovo livello di TRL è necessario:
Installare dei sistemi pilota e usarlo in ambienti reali di grandi dimensioni
Avviare un'ampia sperimentazione di tali sistemi, definendo le esigenze funzionali e prestazionali dei grandi player della sicurezza

Costo associato per arrivare a TRL +1 (anni ed investimento economico)

2 anni, € 2000000

I TA di riferimento TA1 e TA3



- **Identity management**

Descrizione dello Stato dell'arte

Con il termine "Identity Management (IM)" si intende una vasta area tecnologica basata su sistemi integrati e tecnologie che permettono a specifici sistemi informatici di controllare l'identità

degli utenti che accedono ad un servizio o a un luogo definendone i criteri di autenticazione, le autorizzazioni, i ruoli e i previlegi attribuiti ad ogni utente. Negli ultimi tempi, con l'arrivo sul mercato di tecnologie sempre più sofisticate, il termine Identity Management si è esteso anche al dominio degli oggetti.Nel contesto degli individui, il concetto di Identity Management appare sempre più legato all'area delle tecnologie biometriche mentre, per ciò che attiene agli oggetti, un settore fortemente emergente è quello degli RFID (Radio Frequency IDentifier). Con particolare riferimento ai due contesti tecnologici citati (tecnologie biometriche e RFID), il livello tecnologico raggiunto dall'area dell'Identity Management, può essere senz'altro definito soddisfacente ed in continua evoluzione grazie ai forti investimenti assegnati al settore in questi ultimi anni. Purtroppo, a causa anche di difficoltà di tipo giuridico, soprattutto in tema di protezione dei dati personali e, con specifico particolare riferimento al quadro europeo, l'uso di strumenti di identificazione avanzati, come le tecnologie biometriche, è per il momento praticamente monopolizzato da applicazioni di tipo "governativo". Il settore invece degli RFID, grazie ai minori implicazioni dal punto di vista della protezione dei dati personali, è invece in forte ascesa anche nel settore privato con particolare riferimento a quello dell'automazione industriale.

Descrizione dei Gap tecnologici

Pur essendo difficile analizzare i gap tecnologici in una area così vasta ed eterogenea, un fattore inibitore che comunque caratterizza in maniera trasversale tutta l'area dell'Identity Management è la parziale mancanza di standard. Nonostante gli sforzi dei comitati internazionali preposti, la standardizzazione nel settore dell'Identity Management procede infatti ad un ritmo meno sostenuto degli avanzamenti tecnologici con prevedibili conseguenze sul mercato. Ulteriori gap sono riscontrabili in alcuni negli aspetti a cavallo tra tecnologia e contesto giuridico, etico e sociale. Con particolare riferimento infatti alle tecnologie biometriche, ad esempio, manca probabilmente ancora una visione chiara del quadro normativo applicabile e la legislazione è desumibile spesso solo attraverso singoli pareri dati di volta in volta su specifiche applicazioni. Ancora con riferimento alle tecnologie biometriche, esiste un importante gap legato al problema della accessibilità. È un dato di fatto che alcuni utenti, a causa dei deficit fisici e/o cognitivi possono trovare difficile se non addirittura impossibile usare un sistema di autenticazioni su base biometrica. Questi problemi investono soprattutto il settore della terza età che, come già avviene per altri aspetti della vita sociale, rischia una ulteriore emarginazione. Per il settore degli RFID potrebbero essere citate, come gap, le preoccupazioni potenzialmente sollevate da alcuni utenti in merito ai limiti di esposizione alle radiazioni elettromagnetiche soprattutto nelle applicazioni inerenti i luoghi di lavoro.

Trend evolutivi

Il trend evolutivi più significativi nel contesto delle biometriche riguarderanno probabilmente alcuni settori legati alle tecnologie emergenti quali (i) il riconoscimento biometrico del volto in condizioni ambientali impegnative (ad esempio in condizioni di scarsa illuminazione), (ii) l'acquisizione le caratteristiche dell'iride a distanza e (iii) l'uso di tecnologie molti spettrali nelle riconoscimento dattiloscopico. Per ciò che attiene agli RFID, i trend si concentrano sulla riusabilità e sull'incremento della performance tecnica (ad esempio memoria a bordo e/o distanza di lettura/scrittura). In una visione a medio lungo termine, gli RFID avranno l'obiettivo di massima di ridurre sostanzialmente il loro costo al fine di assicurare una maggiore occupazione dei settori di mercato di competenza.

Livello attuale di TRL

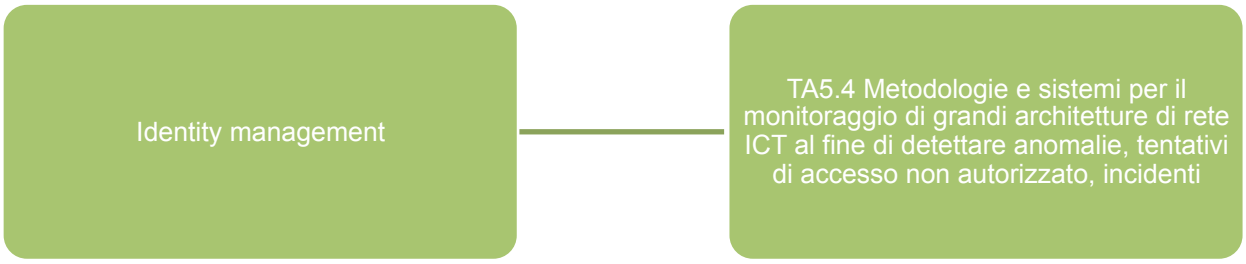
TRL n/a

Essendo il settore dell'Identity Management estremamente vasto ed eterogeneo, appare veramente complesso assegnare un livello generalizzato di readness tecnologica. Esso dovrebbe essere valutato infatti tecnologia per tecnologia. In ogni caso, è opinione ormai consolidata che la maggioranza delle tecnologie appartenenti al settore dell'Identity Management è da posizionarsi nelle fasce più alte di una scala tarata sulle readness tecnologica.

Step Necessari per arrivare a TRL + 1

Gli step necessari per un innalzamento del livello di rilevanza tecnologica del settore dell'Identity Management potrebbero essere caratterizzati dalle keywords "performance", "reliablity" e "resistance" e cioè incremento generalizzato delle prestazioni, dell'affidabilità a della resistenza agli attacchi.

I TA di riferimento TA3, TA6, TA7



- **Biometrics**

Descrizione dello Stato dell'arte

Le tecnologie biometriche, e cioè quelle orientate all'identificazione automatica o verifica di identità degli individui sono entrate ormai in maniera costante nella vita di ogni giorno e gli esperti concordano su di un ulteriore progressiva acquisizione di nuove importanti fette di mercato del cosiddetto "Identity Management". Sebbene, comunque, il trend delle tecnologie biometriche, in uno scenario temporale a medio lungo termine, sia previsto assolutamente in crescita in virtù soprattutto del ruolo fondamentale giocato nella catena della sicurezza, agli ottimi risultati fatti riscontrare nel settore delle applicazioni "pubbliche" non corrispondono, purtroppo, quelli riscontrati nel mercato commerciale privato. Con specifico riferimento, infatti, allo scenario europeo, il numero delle applicazioni "commerciali" è infatti, davvero particolarmente esiguo e su questo dato dovrebbe concentrarsi l'attenzione degli esperti del settore per tentare di determinare le motivazioni di questo risultato inaspettatamente negativo. Sicuramente uno dei fattori inibitori della biometria commerciale consiste nelle difficoltà a correlare, in alcuni casi, tecnologie emergenti e rispetto della privacy. In vari paesi infatti, inclusa l'Italia, allo stato attuale, l'impiego delle tecnologie biometriche è strettamente legato al concetto della proporzionalità e cioè della esistenza di un presupposto cogente, ad esempio la sicurezza di una collettività di utenti. In questo quadro abbastanza definito, le motivazioni imperniate sulla oggettiva semplificazione di procedure di accesso o su fattori economici, almeno allo stato attuale, in varie giurisdizioni nazionali, non vengono considerate sufficienti per l'installazione di sistemi biometrici. Esistono inoltre fondati dubbi in merito al problema della cosiddetta "accessibilità" e cioè

del presupposto di permettere indistintamente a tutti gli utenti di fruire in maniera agevole dei servizi offerti dalle procedure biometriche. Non tutti gli utenti infatti godono delle condizioni fisiche e/o cognitive in grado di assicurare un agevole ed efficace uso dei sistemi biometrici. Il problema dell'accessibilità comporta intrinsecamente la discriminazione di alcune categorie di utenti, per esempio quelli appartenenti alla terza età. Dal momento che le soluzioni proposte per assicurare la massima accessibilità ai sistemi biometrici, ad esempio attraverso l'impiego di tecnologie multi-biometriche, prevedono investimenti particolarmente ingenti e, considerato il difficile momento economico presente, è facile prevedere che il mercato delle tecnologie biometriche continuerà il suo trend espansionistico soprattutto nel settore governativo che, allo stato attuale, sembra l'unico a possedere i requisiti economici per sostenere lo sviluppo delle tecnologie biometriche.

Descrizione dei Gap tecnologici

Le tecnologie biometriche hanno ormai raggiunto un livello tecnologico che ne permette un uso ormai costante in settori estremamente delicati quali, ad esempio, l'attraversamento delle frontiere. Pur tuttavia non si può non parlare di gap tecnologici in quanto, ancora lo stato attuale, esistono ancora gap tecnologici che possono agire da importanti agenti inibitori per quanto riguarda la diffusione di tali tecnologie. Se da una parte, infatti, alcune tecnologie, come ad esempio quella basata sul riconoscimento dattiloscopico, sembrano ormai consolidate e gli sforzi si vanno ad orientare verso aspetti collaterali della tecnologia, quali ad esempio la resistenza a possibili tentativi di frode (anti-spoofing), altre tecnologie sono oggetto di forti investimenti per superare significativi gap tecnologici. I sistemi basati sul riconoscimento biometrico del volto, ad esempio, possono fare registrare un decremento delle prestazioni all'aumentare del tempo intercorrente tra la registrazione iniziale nel sistema del dato biometrico di riferimento e quello acquisito al momento della transazione. Sempre con riferimento al riconoscimento biometrico del volto inoltre alcuni fattori ambientali, come ad esempio l'illuminazione, giocano ancora un ruolo particolarmente importante sulle prestazioni. È lecito quindi annoverare, per alcune tecnologie biometriche, la dipendenza dai fattori ambientali come uno dei gap tecnologici più significativi da colmare.

Trend evolutivi

L'evoluzione delle tecnologie biometriche è da vedersi sotto due profili e cioè quello tecnologico e quello legato a fattori etici legali e sociali. Se è lecito infatti aspettarsi una sempre maggiore accuratezza nell'identificazione o nella verifica di entità degli individui associata ad una robusta residenza come trend delle tecnologie biometriche, è ragionevole comunque ipotizzare che passi in avanti significativi saranno misurabili in una sempre maggiore accettazione di tali tecnologie da parte degli utenti. Partendo, infatti, dalla considerazione che le tecnologie biometriche sono le uniche in grado di poter rendere certa, per quanto possibile, un'attribuzione di identità, è ragionevole ipotizzare che, in un mondo sempre più globalizzato è caratterizzato da transazioni di tipo elettronico, le peculiarità vantabili dalle tecnologie biometriche diventino così importanti da far passare in secondo piano alcune perplessità legate a possibili derive in tema di privacy

Livello attuale di TRL TRL 8 (complessivo)

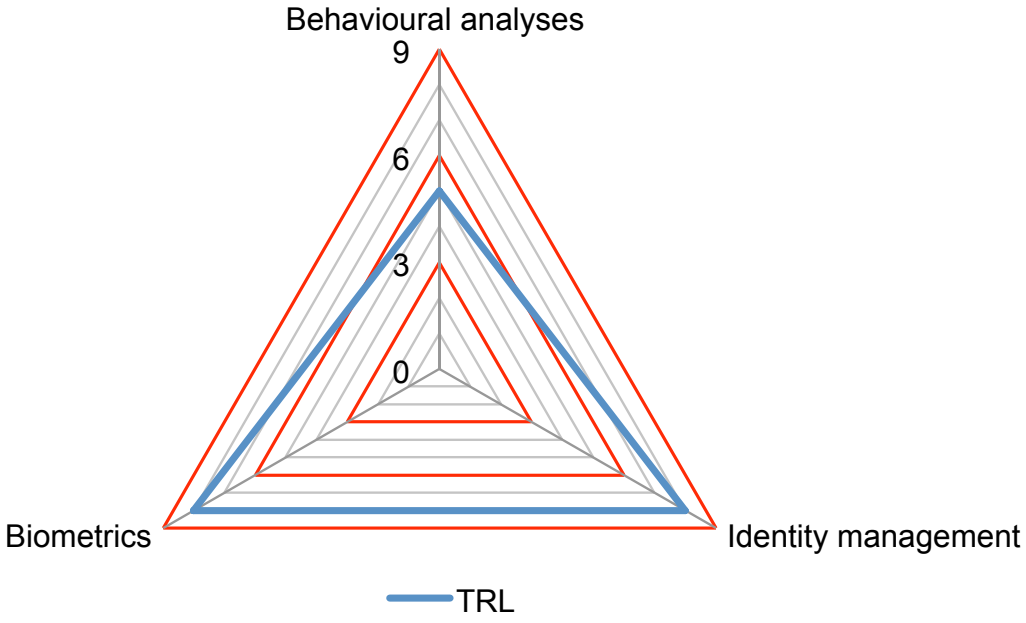
Le tecnologie biometriche sono ormai da considerarsi ragionevolmente consolidate anche se il

TRL può oggettivamente variare in funzione delle diverse tecnologie. Se, infatti, alla riconoscimento dattiloscopico può essere assegnato un TRL 9, ad altre tipologie, ad esempio, quelle inerenti il riconoscimento dell'iride distanza, andrebbe assegnato un TLR minore, ad esempio di valore 7, perché solo recentemente si sta passando da una fase dimostrativa ad una regolarmente applicativa.

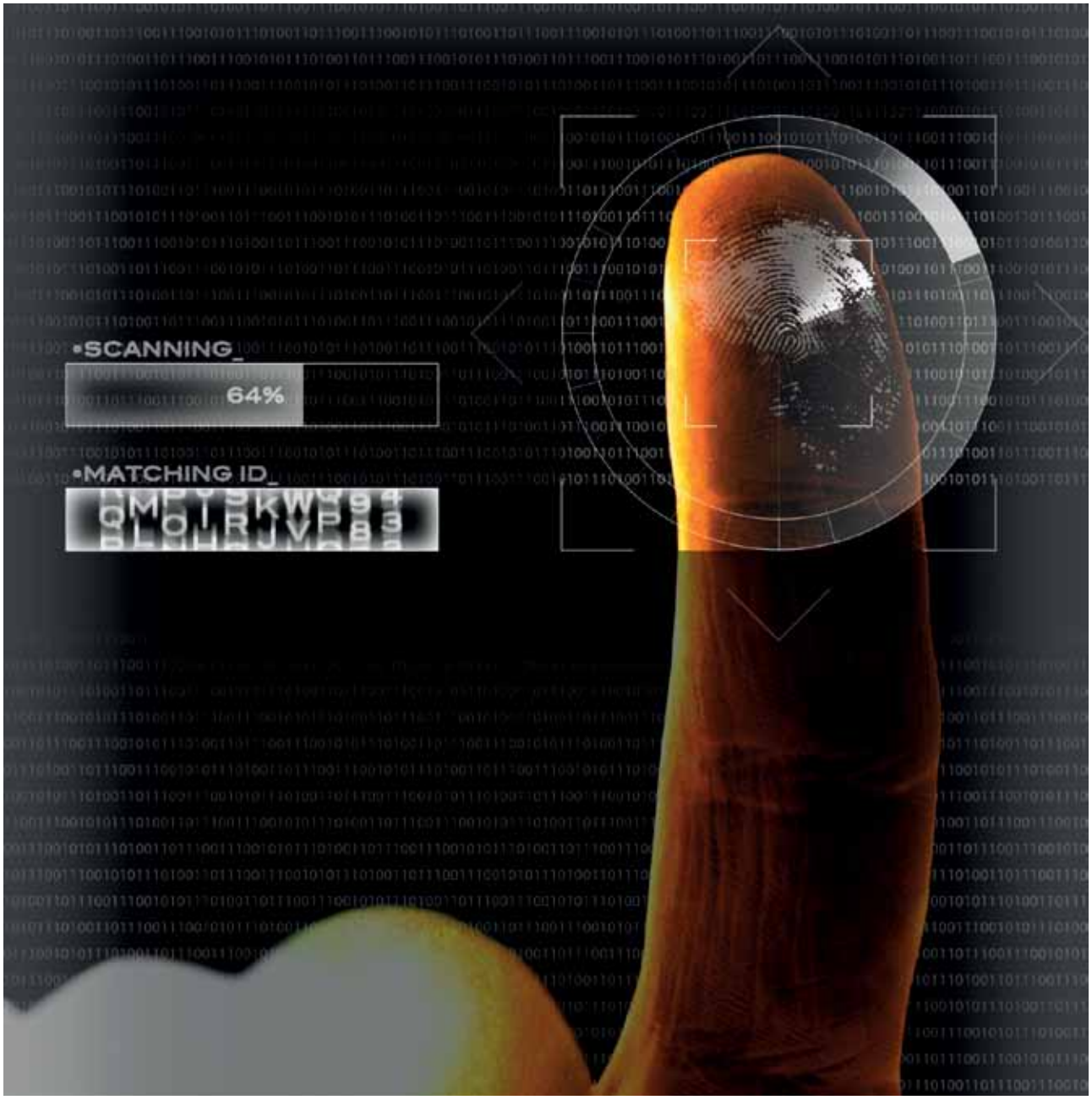
Step Necessari per arrivare a TRL + 1

Con riferimento alle tecnologie ancora in evoluzione gli step necessari consistono soprattutto nel miglioramento e nel mantenimento delle prestazioni in tema di accuratezza, specialmente al variare le condizioni ambientali.

I TA di riferimento TA 3, TA 6, TA 7



4.3.2 Simulation and Design tools, including Ergonomics and Human Factor



Ambiti prioritari di ricerca

- Sensors Simulation
- Advanced Analysis & Simulation Software Tool for Spaceborne Radars
- Methods, tools and processes to support the integration of people in security systems

- **Sensor Simulation**

Descrizione dello Stato dell'arte

Recentemente, le reti di sensori intelligenti sono state largamente utilizzate per scopi molteplici in sistemi orientati alla sicurezza e alla protezione. Applicazioni militari e civili che vanno dalla sorveglianza dei confini e il monitoraggio di spazi pubblici all'intelligenza d'ambiente e la sicurezza stradale rappresentano questa grande varietà di applicazioni. Molti studi recenti hanno proposto l'applicazione delle funzionalità intelligenti direttamente alle video-camere e alle reti di sensori al fine di passare dal riconoscimento degli oggetti alla comprensione degli eventi e delle situazioni [1]. Per sfruttare in maniera efficiente le potenzialità cognitive in una rete di sensori intelligenti, il ruolo degli algoritmi di fusione dati è cruciale [2]. In letteratura molti lavori considerano il problema della fusione dati applicato a sensori eterogenei per la sicurezza [3, 4]. Nel corso degli ultimi anni molte ricerche si sono concentrate sul problema della sorveglianza (e.g., [5], [6]). Lo scopo dei sistemi di sorveglianza moderni è quello di rilevare, riconoscere e classificare situazioni di interesse attraverso una rete di sensori eterogenei per prevenire gli incidenti e proteggere un determinato ambiente dalle minacce esterne. Il lavoro presentato in [7] considera l'introduzione di telecamere intelligenti attive e l'analisi dei modelli di comportamento a lungo termine. Secondo gli autori, una particolare rilevanza di questo tipo di sistemi consiste nella capacità di consentire una diminuzione dell'impegno degli operatori addetti alla sicurezza di un ambiente, poiché sono in grado di generare e gestire in maniera automatica opportuni segnali di allarme. Recentemente, l'integrazione delle caratteristiche dei sistemi di video-sorveglianza e di intelligenza d'ambiente sta portando allo studio e allo sviluppo di soluzioni innovative che sono in grado di modellare ed analizzare le interazioni uomo-macchina, rilevare e classificare i comportamenti umani anche a fini assistenziali e di supporto. Esempi di tali applicazioni sono rappresentati dal lavoro di Appiah et al. [8], secondo i quali un sistema automatico è in grado di imparare le zone di riposo per le persone anziane, monitorare le attività di tutti i giorni e rilevare specifici eventi di interesse. Inoltre Zhang et al. [9] hanno introdotto un metodo basato sulla trasformata di Haar per il riconoscimento e la classificazione delle interazioni tra persone. In [10] Garcia et al. si descrive l'applicazione di metodi con auto-accrescimento per supportare i compiti di video-sorveglianza e di interazioni uomo-macchina. L'approccio proposto è in grado di inseguire i soggetti di interesse ma anche di interpretare i gesti e le posture, ovvero le interazioni con altri device.

[1] Valera, M., Velastin, S.: Intelligent distributed surveillance systems: a review. Vision, Image and Signal Processing, IEEE Proceedings 52(2), 192–204 (2005)
[2] Foresti, G.L., Regazzoni, C.S., Varshney, P.K.: Multisensor Surveillance Systems: The Fusion Perspective. Kluwer Academic, Boston (2003)
[3] Smith, D., Singh, S.: Approaches to multisensor data fusion in target tracking: A survey. IEEE Transactions on Knowledge and Data Engineering 18(12), 1696–1710 (2006)
[4] Chang, B.R., Tsai, H.F., Young, C.P.: Intelligent data fusion system for predicting vehicle collision warning using vision/gps sensing. Expert Systems with Applications 37(3), 2439 – 2450 (2010).
[5] Plataniotis, K.N., Regazzoni, C.S.: Visual-centric surveillance networks and services. IEEE Signal Processing Magazine 22(2), 12–15 (2005)
[6] Collins, R.T., Lipton, A.J., Kanade, T.: Introduction to the special section on video surveillance. IEEE Trans. Pattern Analysis and Machine Intelligence 22(8), 745–746 (2000)

[7] Hampapur, A., Brown, L., Connell, J., Ekin, A., Lu, M., Merkl, H., Pankanti, S., Senior, A., Tian, Y.: Multi-scale tracking for smart video surveillance. IEEE Signal Processing Magazine 22(2), 38–51 (2005)
[8] Appiah, K., Hunter, A., Waltham, C.: Low-power and efficient ambient assistive care system for elders. In: IEEE Computer Vision and Pattern Recognition Workshop, CVPR 2011
[9] Zhang, H., Liu, Z., Zhao, H.: Human activities for classification via feature points. Information Technology Journal 10 (2011)
[10] José García-Rodríguez and Juan Manuel García-Chamizo. 2011. Surveillance and human-computer interaction applications of self-growing models. Appl. Soft Comput. 11, 7 (October 2011), 4413-4431

Descrizione dei Gap tecnologici

Tra le molte discipline che sono coinvolte nella progettazione dei sistemi di sicurezza e protezione di prossima generazione, le scienze cognitive sono sicuramente tra le più interessanti dal punto di vista delle possibilità, che offrono di consentire miglioramenti rispetto allo stato dell'arte. L'applicazione di modelli bio-inspired ai task legati alla sicurezza rappresenta un valore aggiunto importante anche se può essere visto come un gap tecnologico rispetto all'attuale stato dell'arte. La possibilità non solo di rilevare un intruso in un'area proibita o di riconoscere una traiettoria di un oggetto in uno scenario urbano (e.g. una valigia in una stazione o un'auto sulla strada), ma anche di interpretare il comportamento dell'entità nella scena considerata o di rilevare un evento di interesse rispetto a situazioni di normalità, può essere ottenuta attraverso ulteriori attività di ricerca e sviluppo di tali sistemi ispirati alle capacità cognitive umane. I ricercatori in questo campo dovrebbero quindi essere in grado di sviluppare una struttura generale che rappresenti il modello comune per progettare un sistema di sicurezza cognitivo.

Trend evolutivi

Uno dei trend evolutivi più promettenti considera i modelli di ragionamento umani e la formazione della coscienza. Le teorie di A.Damasio descrivono le entità cognitive come sistemi complessi in grado di apprendere in maniera incrementale basandosi sull'esperienza delle relazioni tra se stessi e il mondo esterno. Due sistemi specifici del cervello possono essere definiti per formalizzare tale concetto: proto-self e core-self. Tali sistemi sono specificamente delegati alla gestione e al monitoraggio dello stato interno dell'entità (proto-self) e delle relazioni dell'entità con il mondo esterno (core-self). Quindi, un aspetto cruciale per modellare le entità cognitive è rappresentato dalla possibilità di aver accesso allo stato interno delle entità e, d'altro canto, dalla conoscenza e dall'analisi dell'ambiente esterno. Questo approccio può essere messo in corrispondenza con una struttura sensoriale che divide tra endo-sensori (sensori proto) ed eso-sensori (sensori core) che monitorano rispettivamente gli stati interno ed esterno delle entità che interagiscono. Rispetto alla descrizione precedente, gli oggetti interagenti possono essere rappresentati, per esempio, da una guardia che sorveglia alcune infrastrutture critiche, da un soggetto che guida un veicolo intelligente ovvero da un operatore che opera in un centro di controllo. Per esempio, considerando uno scenario di guardianaggio intelligente, gli eso-sensori potrebbero monitorare l'ambiente dal punto di vista della guardia, mentre i sensori-endo potrebbero fornire informazioni su alcuni parametri della guardia legati alla sua postura, posizione, velocità, etc.

Livello attuale di TRL TRL2

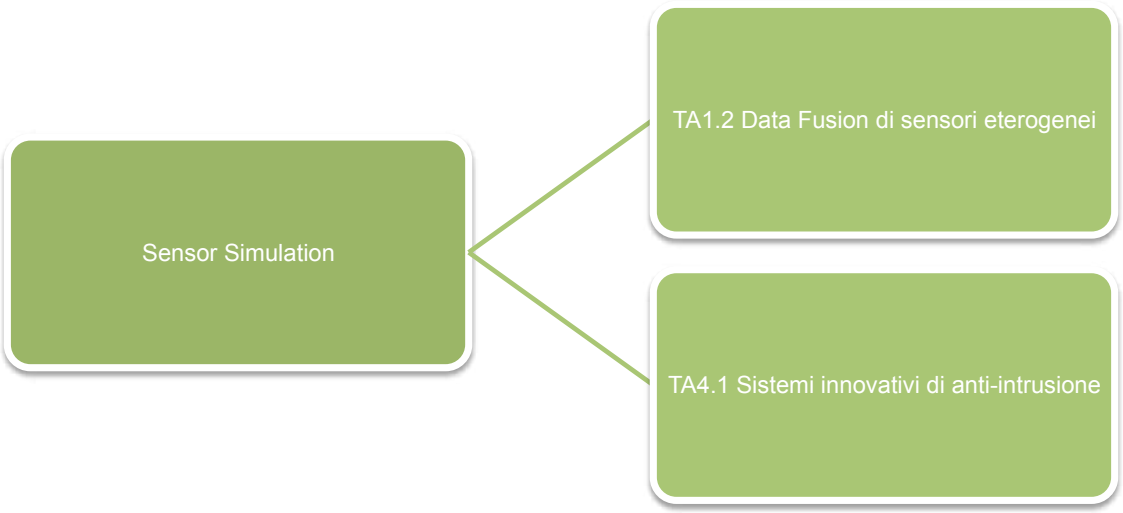
Step Necessari per arrivare a TRL + 1

Le attività di ricerca e sviluppo devono essere indirizzate verso i sistemi cognitive di tipo bio-inspired.

Costo associato per arrivare a TRL +1 (anni ed investimento economico)

Il costo associato per il prossimo livello di sviluppo tecnologico può essere stimato in 7 anni/uomo circa.

I TA di riferimento TA1, TA4



• Advanced Analysis & Simulation Software Tool for Spaceborne Radars

Descrizione dello Stato dell'arte

L'attuale ingegneria per i radar spaziali si basa su strumenti software di analisi e simulazione come supporto per la previsione delle performance dei radar, ma anche come strumento di innovazione per le attivita di ricerca e sviluppo. In Italia si sono prodotti un ampia gamma di strumenti di simulazione, che tuttavia richiedono ulteriori attività per l'integrazione e per successive implementazioni basate su metodi di modellazione sempre più avanzati. A tale scopo i simulatori di radar spaziali dovranno essere progettati e sviluppati tenendo presente una varietà di modalità operative e di modi di controllo remoto (mappatura SAR, sorveglianza RAR, funzioni di intercettamento di tipo ELINT e così via). È di particolare interesse la progettazione di un simulatore modulare costituito da differenti sottosistemi che possano essere aggiornati in modo flessibile e con livelli di dettaglio sempre maggiori. Gli attuali sforzi sono concentrati sullo sviluppo di uno schema di message passing di tipo non real time e xml-based che garantisca la comunicazione tra i diversi moduli che coprono aspetti di ingegneria aerospaziale, elettronica nonché di geofisica. Più in dettaglio vanno trattati aspetti di meccanica orbitale dei veicoli, aspetti ambientali che prendono in esame i pattern di clutches dei terreni e delle superfici marine, la gestione di target statici o dinamici, le condizioni atmosferiche, le tecnologie dei radar moderni con con treni di impulsi sia coerenti che incoerenti in diverse bande operative, curando le acquisizioni di dati elementari, la formazione delle immagini SAR, le tecniche MTI

con gli approcci SISO e MIMO, le funzionalità di intercettamento ELINT e le sorgenti EM. Infine le prestazioni di misura del simulatore software saranno validate anche tramite il confronto dei risultati analitici con i risultati forniti da simulazioni Monte Carlo ogni volta che ciò sia realizzabile.

Descrizione dei Gap tecnologici

Essendo un simulatore SW, i GAP tecnologici non sono propri del Simulatore ma è esso stesso uno strumento di analisi come evidenziato nella precedente sezione "Descrizione dello Stato dell'arte".

Trend evolutivi

Le attuali infrastrutture software devono alle metodiche standard di progetto e sviluppo di sistema quali la Flessibilità, la Modularità, l'Interoperabilità e l'Efficienza. È ovvio che l'Efficacia costituisce pure uno degli elementi di base dell'ingegneria di questi sistemi, influenzati anche in senso più generale dallo stato dell'arte delle tecniche di modeling e dal livello delle tecnologie abilitanti di tipo spaziale.

Livello attuale di TRL

Non è possibile una definizione precisa del livello di TRL del software.

Step Necessari per arrivare a TRL + 1

Come detto, non è possibile una definizione precisa del livello di TRL del software di analisi e simulazione ma nonostante ciò, questo rappresenta un elemento indispensabile per supportare lo sviluppo di radar spaziali innovativi e per accelerare l'implementazione di concetti avanzati nell'ambito dei sistemi di volo.L'innovazione degli strumenti software richiede un progresso sulle assunzioni di modeling dei sottosistemi radar per lo spazio e del relativo ambiente operativo. È inoltre richiesta il miglioramento dell'infrastruttura software che consente di istanziare tali modelli.

I TA di riferimento TA 1

- **Methods, tools and processes to support the integration of people in security system**

Descrizione dello Stato dell'arte

Attualmente esistono svariate metodologie, tecnologie e framework (molti all'avanguardia, alcuni ancora in fase di consolidamento) per la integrazione efficace di persone, mezzi e processi (operativi) in sistemi di sicurezza, consistenti in apparati centralizzati che operano un "comando e controllo" da remoto di sensori, *device* radiomobili, videocamere, etc. e preposti alla gestione di situazioni critiche, di emergenza (terremoti, alluvioni, etc.) o nelle quali "semplicemente" debbano essere erogati – comunque in tempi molto rapidi e con pochi margini di errore - servizi di sicurezza (es: eventi "speciali" quali ad esempio il G8, il giubileo, gli europei di calcio, manifestazioni, etc.). In ogni caso, la comunicazione (soprattutto quella fra sistemi radiomobili di differenti tecnologie, ad esempio TETRA, DMR, VHF…) ha un ruolo fondamentale, e l'orchestrazione di differenti applicativi (con annesse "procedure operative") nonché l'integrazione (in tempo reale e con la "certificazione" dell'autenticità delle fonti informative) di database eterogenei (e contenenti dati non strutturati e multimediali) sono elementi qualificanti dei migliori prodotti / ser-

vizi (solitamente denominati Crisis Management Systems, Emergency Warning Systems, Mass Notificaton Platforms, etc.) attualmente in fase di lancio o già commercializzati. La maggior parte di questi sistemi prevede quasi sempre, come detto, che il "comando e controllo" sia effettuato da una sala operativa, spesso ospitata all'interno di strutture preposte (ad esempio le Sale Crisi della Protezione Civile), all'interno della quale personale specializzato gestisce, con competenza e capacità decisionale, le varie situazioni critiche, di emergenza, etc. Infine, detti sistemi fanno un sempre più massiccio ricorso, da un lato, a tecnologie di radiolocalizzazione attraverso il GPS, la "triangolazione" fra celle radiomobili, l'RFID, etc. (per il *positioning* di persone ed oggetti) e, dall'altro, ad architetture di Cell Broadcasting (per l'invio - in modalità *broadcast* – di informazioni destinate sia alla popolazione civile sia agli operatori sul campo).

Descrizione dei Gap tecnologici

Il gap è notevole non tanto con rispetto alle tecnologie (laddove l'*offerta* è, al contrario spesso superiore alla effettiva *domanda*) ma, piuttosto, quando si tratta di prevedere un'efficace integrazione fra differenti componenti infrastrutturali o, ciò che è ancor più problematico, fra differenti attori e processi (es: il coordinamento sul territorio, durante la gestione – prima, durante e dopo - di un evento catastrofico, come ad esempio un terremoto, di gruppi appartenenti a differenti corpi – polizia, 118, vigili del fuoco, etc. – ed organizzazioni, spesso no profit e quindi con pochi strumenti a disposizione, quali i volontari della protezione civile, della croce rossa, etc.). Oltre a ciò, la flessibilità nel ri-progettare autonomamente e dinamicamente (in base alle mutate esigenze) le modalità di comunicazione nonché lo scambio di informazioni (fra i differenti "nodi" di questo network di persone ed oggetti) è sicuramente un *gap* che i paradigmi di progettazione ed erogazione dei servizi quali, fra tutti, il Cloud Computing stanno, in questo momento, tentando di colmare.

Trend evolutivi

I trend evolutivi sottendono l'utilizzo, sempre più frequente e strutturato, di prodotti di *social networking* (soprattutto quando si tratta di mettere a disposizione - in maniera tempestiva, sicura e profilata – informazioni e/o contenuti, spesso anche multimediali, fra i differenti attori coinvolti), di *data mining* (vedansi tutte le problematiche legate alla gestione dei cosiddetti Big Data, la cui efficace interpretazione aumenta la *situational awareness* di chi prende le decisioni) e, soprattutto, del *Cloud Computing*, che consente di erogare – in *real time* ed in maniera resiliente e sicura - servizi da una piattaforma centralizzata. Una enfasi particolare viene poi sempre più riposta nell'utilizzo combinato, in seno a sistemi cooperanti, dei vari standard dedicati alla gestione delle emergenze, quali l'Emergency Data Exchange Language (EDXL) o il Common Alerting Protocol.

Livello attuale di TRL TRL6

Step Necessari per arrivare a TRL + 1

Setup di un testlab aperto e distribuito (con disponibilità di strumenti avanzati di *Service Creation*, di *Cloud Simulation,* etc.). Stipula di accordi di partnership con ambienti di ricerca, universitari, etc. e anche Service Provider (es: Telecom Italia)

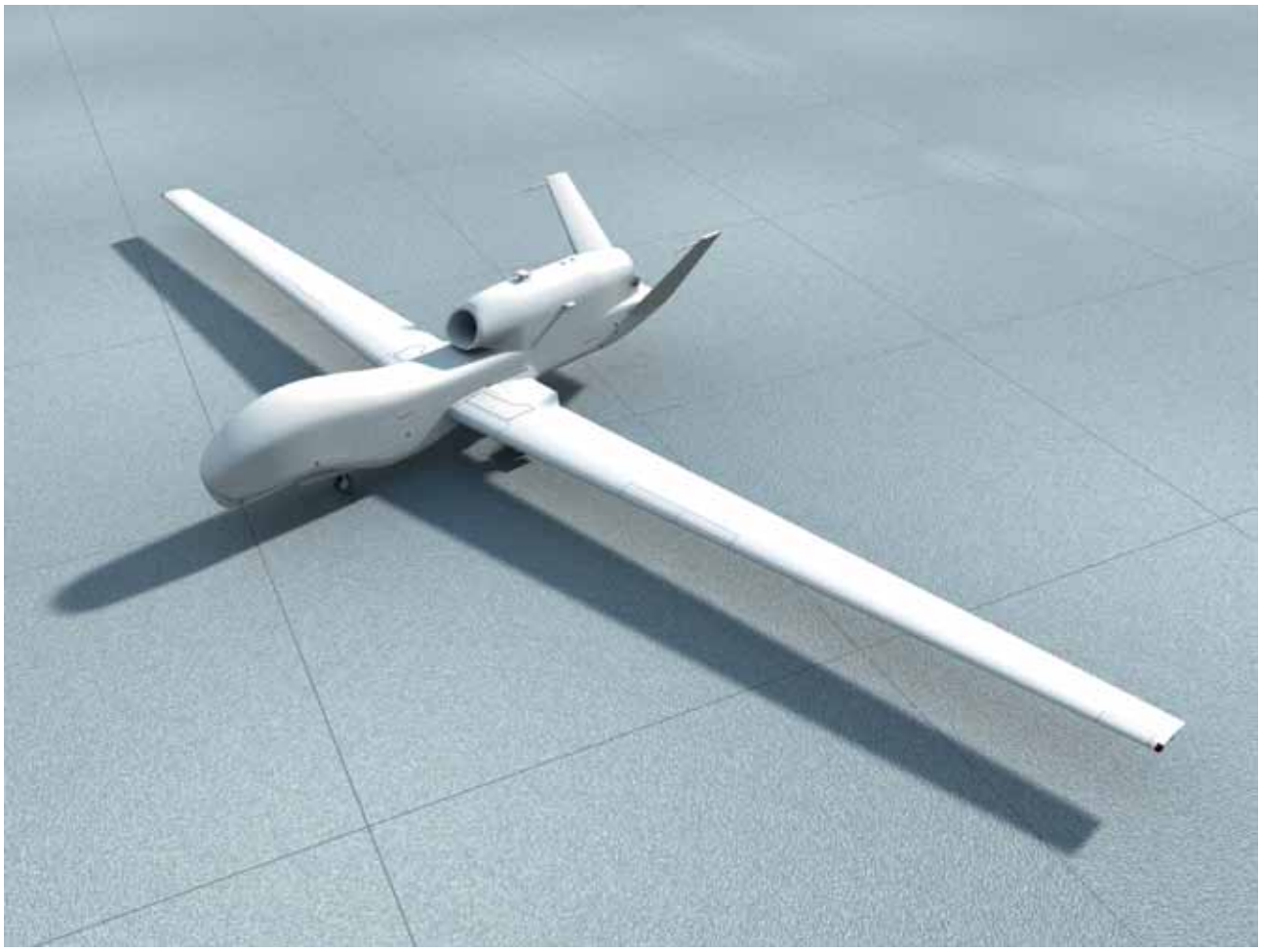
Costo associato per arrivare a TRL +1 (anni ed investimento economico)

Anni: 2 anni. Investimento economico: c.a. 6 milioni di euro

I TA di riferimento TA1,TA4

4.4 Integrated platforms and systems

4.4.1 Platforms



Ambiti prioritari di ricerca

- Space platforms - Infrastruttura di Navigazion Multi-funzione (INM) per la Security
- Ground platforms - Unmanned ground vehicles
- Air platforms - Unmanned Aerial Vehicles

- **Space platforms - Infrastruttura di Navigazione Multi-funzione (INM) per la Security**

Descrizione dello Stato dell'arte

Una piattaforma comune multi-funzione che mette a disposizione i dati di base indispensabili per posizionarsi con accuratezza e sicurezza sia in termini di safety e sia di security. La piattaforma intende rendere disponibili ad opportuni utenti finali (non sono da considerarsi le applicazioni avioniche), anche in modalità protetta e sicura, le tecnologie proprie della navigazione satellitare, come la generazione di dati per il miglioramento della accuratezza di posizionamento (augmentation), attraverso protocolli e formati standard (utilizzati per le correzioni differenziali di codice o di fase, dati SISNeT, ecc.), le informazioni di tempo, o quelle legate alla qualità ed integrità del dato e le risorse di utilità comune come mappe o dati meteorologici al fine di migliorare la qualità complessiva del servizio di navigazione anche per movimentazione indoor. Il tutto anche nel caso di applicazioni critiche. Concettualmente, primi fruitori delle informazioni elaborate e messe a disposizione dalla INM sono dei "Centri Servizi". Il singolo Centro adegua le informazioni acquisite dalla INM alle necessità specifiche degli utenti terrestri (siano essi cittadini normodotati o diversamente abili aventi esigenze riconducibili alla pura navigazione commerciale o utenti che presentino esigenze molto più particolari di tipo anche governativo), oppure abilita gli utilizzatori all'uso diretto delle informazioni, monitorandone e gestendone qualità ed affidabilità. L'accuratezza, la protezione ed il suo livello di robustezza sono da ricondursi alle specifiche esigenze dell'applicazione finale che viene presa in considerazione. La piattaforma proposta aspira a soddisfare le più stringenti esigenze governative garantendo i livelli di protezione richiesti.
Le funzioni principali della INM sono raggruppabili in quattro aree:

1. Funzioni di potenziamento del dato di posizione (gli utenti, abilitati a ricevere le informazioni dalla INM, possono migliorare l'informazione di posizionamento, ottenere più rapidamente la propria posizione [tecnologia Assisted GPS o Assisted Galileo], fruire del dato di correzione del sistema EGNOS tramite interfacciamento con il SISNeT data server [SDS], fruire di informazioni cartografiche tramite server GIS operante nel caso di applicazioni non governative con mappe commerciali ed interfacciabile tramite server Web Feature Service)
2. Funzioni di Comunicazione (a seconda delle esigenze e degli scenari operativi si prevedono diverse soluzioni che vanno da un supporto wireless per erogazione delle informazioni tramite tecnologia WiFi in aree attrezzate, a soluzioni di trasmissione ad-hoc opportunamente protette).
3. Strumenti per la gestione ed il monitoraggio delle informazioni
4. Gestione dell'accesso agli elementi locali di differenti tipologie (Stazioni di riferimento, ecc);

La protezione dell'informazione e la sua distribuzione all'utente anche in situazione di interferenza elettromagnetica può essere garantita con diverse tecniche tra cui quelle che si basano sulla Geo- Encryption o su innovativi algoritmi e tecniche di protezione tipo GREAT (GNSS Regenerative Encryption Algorithm and Techniques).
Nota: gli aspetti concernenti l'adeguamento dei terminali-utente al fine di soddisfare i requisiti di security incluso l'utilizzo di tecniche di geo-encryption esulano dal perimetro di interesse di questa scheda.

Descrizione dei Gap tecnologici

Includere nella piattaforma INM sviluppata, nel rispetto delle esigenze e dei requisiti di security, le soluzioni basate sulle tecniche e gli algoritmi di geo-encryption in modo da garantire i livelli di protezione adeguati alle varie esigenze (anche le più stringenti). Includere, quindi, in modo opportuno i principi ed i benefici della geo-encryption per rendere robusta la protezione e la generazione delle chiavi di cifratura. Considerare le soluzioni tipo GREAT per integrarle ove opportuno nella piattaforma.

Trend evolutivi

Generalizzare la piattaforma in modo da raggiungere livelli di multi-funzionalità tali da coprire un ampio spettro di esigenze sia in ambito safety e sia di security.

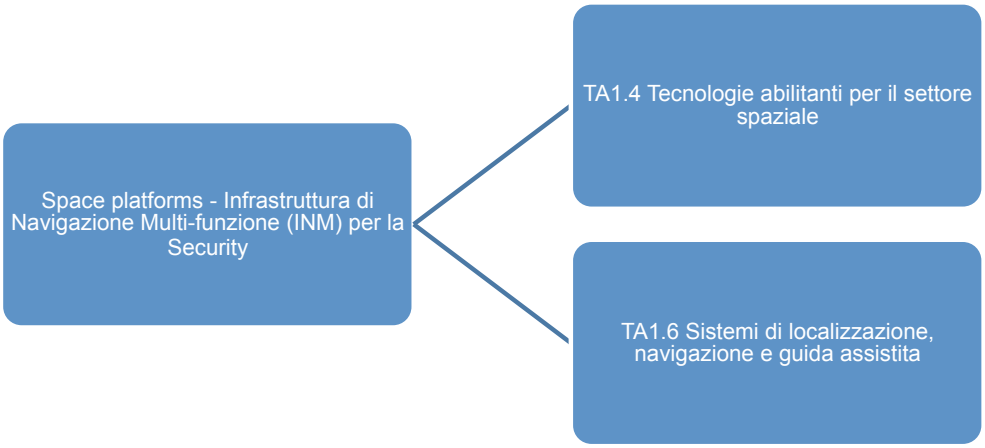
Livello attuale di TRL

La piattaforma INM per le applicazioni Safety ha raggiunto una maturità TRL-6 (Dimostratore tecnologico). L'estensione alle applicazioni Security è ad un livello inferiore paragonabile ad un TRL-3 o TRL-4

Step necessari per arrivare a TRL+1

- Le principali attività per portare tutta la piattaforma al livello successivo possono suddividersi nei seguenti due filoni principali:
- adeguare la parte associata alle applicazioni security allo stesso livello di maturità della piattaforma INM per la safety
- innalzare tutta la piattaforma (includente la parte attinente la security) al livello successivo di sviluppo

TA di riferimento TA1, TA4



- **Ground platforms - Unmanned ground vehicles**

Descrizione dello Stato dell'arte

L'impiego di piattaforme robotiche mobili nella gestione di eventi critici – siano essi di origine

umana (incidenti industriali, attacchi terroristici) o calamità naturali – è strettamente correlato alla possibilità di operare in collaborazione o in sostituzione di squadre di operatori umani (First Responder Team). I soccorritori devono infatti abitualmente operare in ambienti particolarmente ostili, dal punto di vista della stabilità strutturale - variabile anche in modo repentino (terremoti; chiusura vie di fuga), della temperatura (incendi), della presenza di sostanze tossiche o radioattive (Seveso, Fukushima). Inoltre le condizioni di visibilità, come pure le comunicazioni radio, possono essere seriamente deteriorate, con conseguenze negative sulla possibilità di orientamento. Infine la stessa possibilità di impiego di operatori umani è subordinata alla verifica di determinate condizioni di sicurezza, che a sua volta richiede la "visibilità" dell'area interessata. Appare evidente, anche da un punto di vista puramente intuitivo, che un robot autonomo dotato delle opportune caratteristiche permetterebbe di far fronte a tutte le problematiche evidenziate, riducendo in maniera sostanziale i rischi di ferimento o di morte per i soccorritori e aumentandone contemporaneamente, grazie anche ad una adeguata dotazione sensoriale, l'efficienza e l'efficacia. Allo stato dell'arte attuale l'impiego di robot nella gestione di crisi è però fortemente limitato, a causa di vari fattori, e nonostante la disponibilità sul mercato di un gran numero di piattaforme mobili. Si possono citare la limitata mobilità su terreni accidentati, sulle macerie conseguenti a un terremoto o su scale; le ancora insufficienti capacità di navigazione e, più in generale, di autonomia, che non consentono di operare efficientemente in ambienti non strutturati, specialmente in caso di mancanza di comunicazioni adeguate; la scarsa efficienza delle attuali interfacce uomo-robot, che impegnano eccessivamente l'operatore, distraendolo da altri compiti, a scapito anche della sicurezza. Illuminanti sono in proposito le osservazioni raccolte, in differenti occasioni, fra alcuni end-users (vigili del fuoco), che lamentano la macchinosità del controllo delle piattaforme robotiche attualmente disponibili e affermano con convinzione la superiorità, in termini di capacità e di efficienza – e della stessa possibilità di compiere determinate operazioni - dell'uomo sul robot.

Descrizione dei Gap tecnologici

- Limitata mobilità su terreni accidentati, macerie, scale; limitata adattabilità a differenti tipologie di terreno.
- Pesi eccessivi (ideale sarebbe la possibilità di trasporto da parte di uno o due operatori); dimensioni eccessive e standardizzazione insufficiente dei payload.
- Limitate capacità di comunicazione in aree schermate; limitate capacità di ripristino comunicazione.
- Capacità sensoriale migliorabile; miniaturizzazione migliorabile (per consentire l'installazione di più sensori su veicoli mobili di limitate dimensioni); condivisione dati fra robot e operatori limitata o assente.
- Limitate capacità di comprensione autonoma della situazione e di autoapprendimento, limitata cognitività.
- Capacità di autolocalizzazione e di navigazione autonoma ancora insufficienti, specie in ambienti non strutturati; assenza di funzioni di rientro autonomo e di inseguimento autonomo dell'operatore.
- Interfacce uomo-robot non sufficientemente "user-friendly", che comportano ancora un eccessivo impegno mentale da parte dell'operatore. Mancanza di funzioni di cooperazione automatica con l'operatore.
- Insufficiente livello di cooperazione fra robot diversi.

Trend evolutivi

- Miglioramento della mobilità – inclusa la velocità di movimento - su differenti tipi di terreno accidentato (macerie, scale).
- Miglioramento delle prestazioni dei sistemi sensoriali, inclusa la miniaturizzazione e la standardizzazione delle interfacce verso il robot.
- Sviluppo e integrazione di capacità cognitive e di autonomia, sia per quanto riguarda l'autolocalizzazione e la navigazione che per l'individuazione di vittime e di situazioni ambientali di pericolo.
- Sviluppo di interfacce uomo-robot evolute.
- Studio e realizzazione di swarm di robot.

Livello attuale di TRL

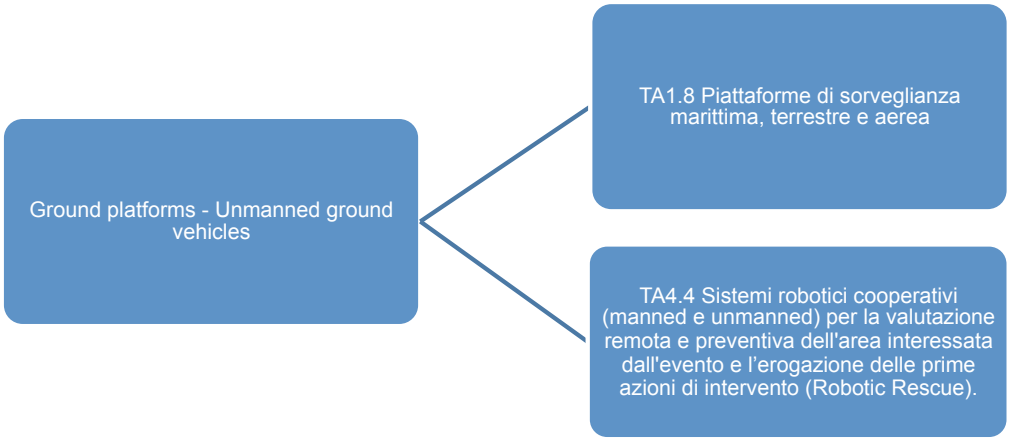
Per le differenti tecnologie indicate si valuta un TRL di livello 3 – 5 (technology development)

Step Necessari per arrivare a TRL + 1 (road-map)

Per il raggiungimento del livello superiore (TRL 4 – 6) sono necessarie ulteriori attività di ricerca e di sviluppo tecnologico, con conseguente realizzazione di prototipi. Considerando che le tecnologie indicate presentano un sufficiente grado di indipendenza le une dalle altre, si giudica che tali attività possano essere condotte in parallelo.

Costo associato per arrivare a TRL +1 (anni ed investimento economico)

Anni: 2 - 3 per tecnologia
Investimento: 2 – 3 M€ per tecnologia
T
A di riferimento TA4



- **Air platforms - Unmanned Aerial Vehicles**

Descrizione dello Stato dell'arte

I sistemi Unmanned (UAS) per la sorveglianza attualmente in servizio od in fase di introduzione sono di impiego prevalentemente militare (ISR ed armed ISR), ma si stanno affacciando sul mercato le prime soluzioni per impiego nel campo civile/border security. Ci sono già stati

esempi di sistemi militari che sono stati impiegati in scenari non militari in occasione di catastrofi naturali o incendi, pattugliamento delle coste, oppure in occasione di importanti summit internazionali etc. Nell'ambito di varietà e classi di sistemi si passa dai sistemi HALE (High Altitude Long Endurance) quali RQ-4/MQ4 NG Global Hawk, ai MALE (Medium Altitude Long Endurance) quali : GA MQ-1 Predator , GA MQ-9 Reaper ed MQ-1C Gray Eagle , IAI Heitan, IAI Heron, Elbit Hermes 900, fino ai sistemi Tattici, quali: Elbit Hermes 450, Sagem Patroller, AAI Shadow 200, Boeing Scan Eagle, Insitu integrator. Nel caso degli HALE e MALE più prestanti si tratta di macchine capaci di operare per almeno 20-30 h ed a grandi distanze, grazie a sistemi D/L BLOS imbarcati, e dimensioni e pesi adeguati (>4 T).Non sono da trascurare, soprattutto per applicazioni navali, gli UAS a decollo verticale ed in particolare quelli basati su macchine ad ala rotante, quali il Saab Skeldar , NG MQ-8 Firescout e Schiebel Camcopter S-100.Discorso a parte meritano i mini e micro UAS. Recentemente stanno incominciando ad essere utilizzati non solo nelle aree remote o di operazione militare ma anche nei NAS (National Air Space) con restrizioni e regole peculiari e sono in corso una serie di iniziative per il loro inserimento nel'ATM.I sistemi UAS hanno raggiunto un livello di maturità notevole, in particolare per l'affidabilità dei velivoli e dei sistemi (centinaia di migliaia di ore di volo in aree operative). Le prestazioni ed i servizi vengono assicurati grazie ai vari pay-load imbarcati, che nel caso dei MALE e dei Large Tactical si traducono generalmente in un doppio sensore (EO/IR e SAR). Attualmente si stanno ampliando la capacità di sensori imbarcati e non sono rare di applicazioni di 3 o più pay-load contemporaneamente (E/O-IR, SAR ed ESM, o impiego di altri sensori quali iper-spettrali). Alcune sfide sono di fronte ad un loro ulteriore sviluppo e diffusione:

- Riduzione Costi ed Footprint logistico (e.g. i sensori di sorveglianza imbarcati ancorché prestanti sono costosi e non sempre disponibili per applicazioni non militari).
- Normativa e standardizzazione per utilizzo dello spettro elettromagnetico (Standardizzazione DataLink)
- Regole Certificative Civili
- Inserimento nello spazio aereo civile ed accettazione da parte della Manned Aviation Community (via tecnologia Sense and Avoid e inserimento ATM).

Descrizione dei Gap tecnologici

Gap nel campo degli Unmanned, su cui si stanno e si devono focalizzare gli sforzi, sono i seguenti:

- Light Airframe
- Autonomia di Missione (decision making and autonomous behavior)
- ATM interfces/Integration
- Auto Taxi, Automatic Take-Off and Landing
- Weather detection and protection
- LOS/BLOS infrastructures
- Ground station – HMI & Training

Trend evolutivi

- Incremento affidabilità dei velivoli, grazie ad architetture ridondate e ricadute tecnologiche nel campo della General Aviation/manned aviotion
- Riduzione costo di esercizio: stanno apparendo i primi esempi di società che offrono il ser-

vizio finale ad utente con gestione delle macchine non da parte dell'utente
- Sperimentazione di nuove tecnologie per aumentare la persistenza della sorveglianza da 1 giorno ad 4 gg –una settimana (Extreme Persistence, vedi Boeing Phantom Eye e -Aero-Vironment Global Observer, con propulsione idrogeno ed Aurora Flight Science Orion con propulsione diesel).
- Aumento delle capacità dei Mini e UAV tattici grazie alla miniaturizzazione sensori e dei sistemi di propulsione (ibrida /elettrica)
- Integrazione di molteplicità di sensori e fusione di queste informazioni sia on-ground che onboard.
- Incremento delle capacità Autonome

In particolare nel campo della Autonomia di Missione sono da tempo noti gli obbiettivi da raggiungere:

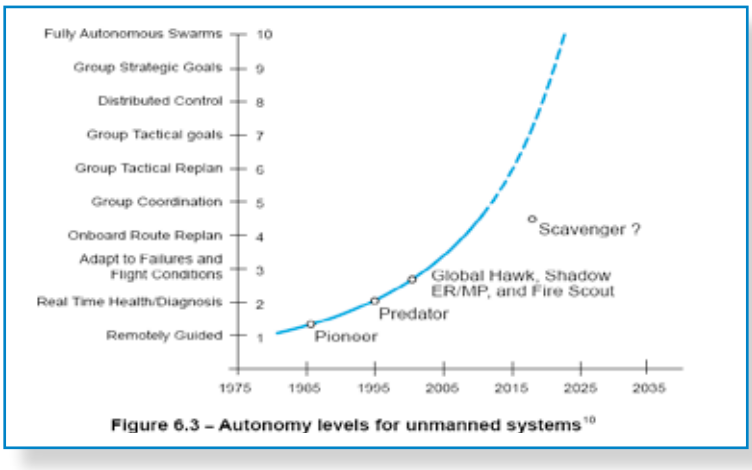
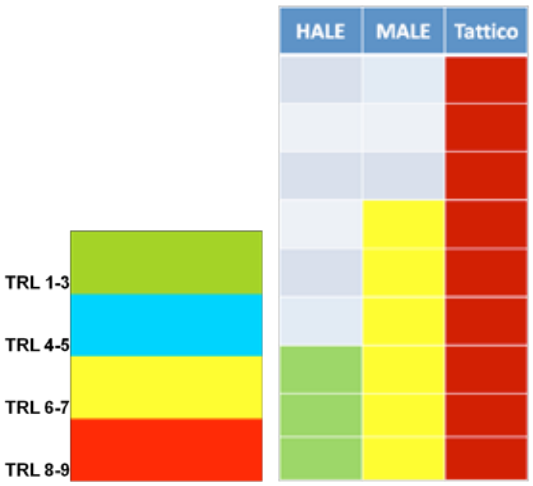


Figure 6.3 – Autonomy levels for unmanned systems[10]

Livello attuale di TRL



Step necessari per arrivare a TRL+1

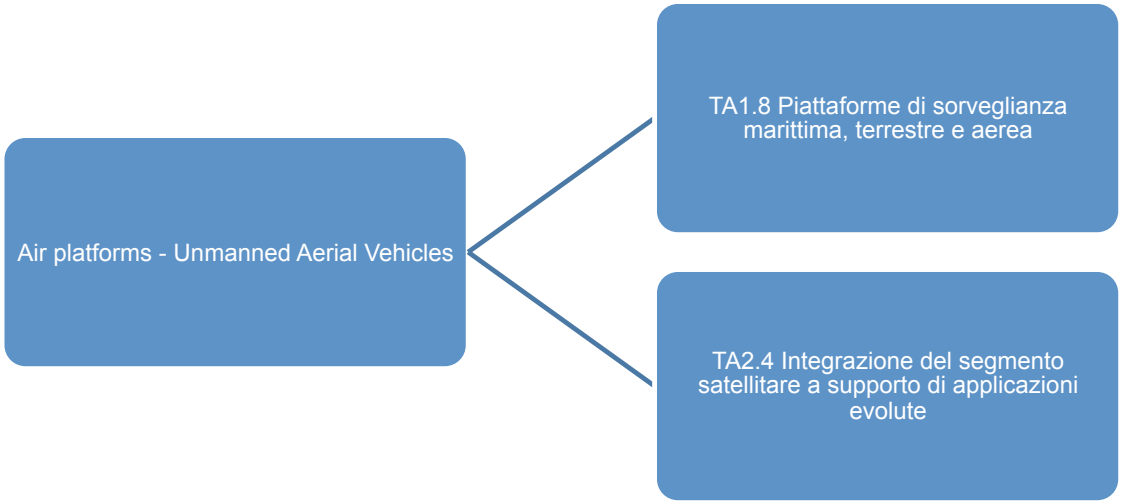
- Riduzione Costi ed Footprint logistico (e.g. i sensori di sorveglianza imbarcati ancorché prestanti sono costosi e non sempre disponibili per applicazioni non militari).

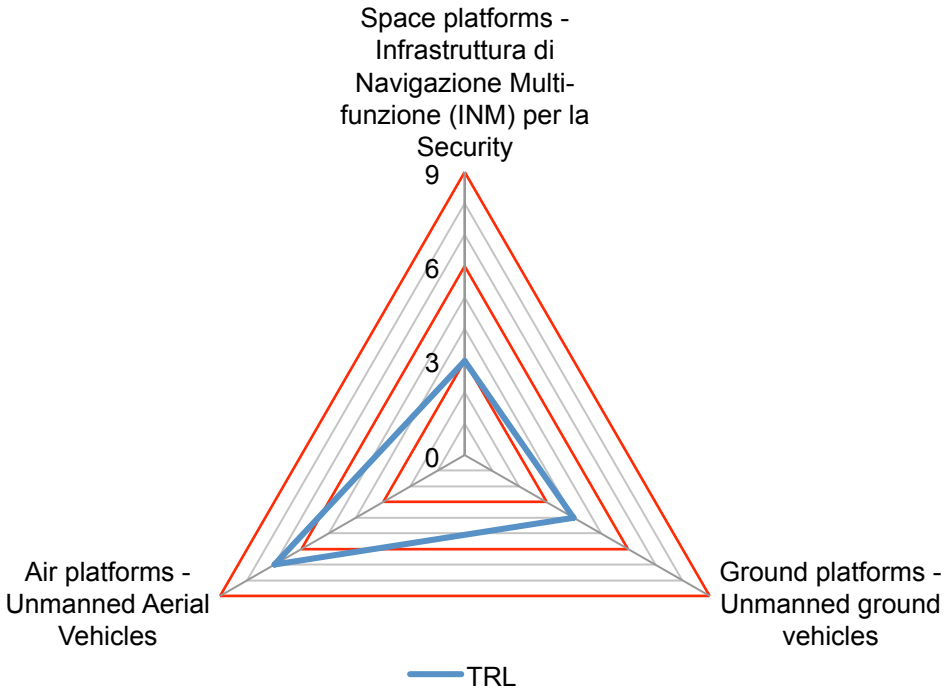
- Normativa e standardizzazione per utilizzo dello spettro elettromagnetico (Standardizzazione DataLink)
- Regole Certificative Civili
- Inserimento nello spazio aereo civile ed accettazione da parte della Manned Aviation Community (via tecnologia Sense and Avoid e inserimento ATM).

Costo associato per arrivare a TRL +1 (anni ed investimento economico)

Tre anni

TA di riferimento TA1





4.4.2 Integrated Systems

Ambiti prioritari di ricerca

- Wide-scale long-range multi-sensor surveillance
- Communication, Command, Control and Information Systems
- Interoperability
- Command & Information Systems Integration

- **Wide-scale long-range multi-sensor surveillance**

Descrizione dello Stato dell'arte

I sistemi di sorveglianza integrati prevedono l'utilizzo di molteplici tecnologie al fine di consentire la sorveglianza efficace di zone di interesse. L'integrazione di tali sistemi prevede la possibilità di scambiare e combinare in modo efficiente le informazioni raccolte dai vari sotto-sistemi componenti. Fra le principali tecnologie utilizzate in sistemi di sorveglianza figurano le seguenti.

- **Sistemi di sorveglianza con sensori video**: si basano sull'utilizzo di telecamere (termocamere, camere ad infrarosso, ecc.). Attualmente vi sono telecamere, dotate di un micro-pc, in grado di fare elaborazione locale prima di inviare dati (a questo punto già raffinati) ad un elaboratore centralizzato. Tipicamente, l'utilizzo di telecamere per riprese video richiede la possibilità di trasmissione dati ad alta velocità. Gli standard di comunicazione utilizzati sono tipicamente Ethernet (IEEE 802.3), nel caso di connessioni cablate, o tutta la classe di standard WiFi (IEEE 802.11a/b/g/n), nel caso di connessioni senza filo.
- **Sistemi di sorveglianza basati su reti di altri sensori**: in questo caso si utilizza una moltitudine di nodi, tipicamente equipaggiati con batteria e collegamento senza filo, dotati di diversi tipi di sensori (chimici, fisici, magnetici, vibrazionali, biologici, audio). In questo caso ogni nodo trasmette piccole quantità di informazione. Lo standard di comunicazione di riferimento è l'IEEE 802.15.4 (low-rate wireless personal area networks, LR-WPANs). Si stanno definendo e sviluppando protocolli di comunicazione in reti di sensori (più in generale, in ambito Internet of Things, IoT) in grado di garantire comunicazioni con protocollo IPv6. Da un lato, ci sono le attività della Internet Engineering Task Force (IETF, http://www.ietf.org/), soprattutto con 6LowPAN ed RPL, e le attività dell'European Telecommunications Standards Institute (ETSI, http://www.etsi.org), soprattutto in ambito machine-to-machine (M2M).

Le principali tecniche utilizzate possono essere classificate come:

- rivelazione di oggetto;
- riconoscimento ed inseguimento di oggetto;
- analisi comportamentale;
- raccolta e gestione delle informazioni (database evoluto).

A livello architetturale, i sistemi integrati di sorveglianza fanno riferimento ad un'architettura gerarchica, con (tipicamente) un unico *operational center* dove le informazioni sullo stato della zona monitorata vengono sintetizzate globalmente. In tale contesto, particolare rilevanza hanno tecnologie di data mining and operations research.

Descrizione dei Gap tecnologici

Un gap tecnologico consiste nella mancanza di un protocollo standard aperto in grado di far comunicare sotto-sistemi di tipo differente. Esistono infatti numerose soluzioni proprietarie, tipicamente basate su protocolli non condivisi. Altri gap tecnologici sono rappresentati dalla necessità di distribuzione dei task di elaborazione (decentralizzazione, rispetto a

sistemi classici con architetture fortemente centralizzate), dall'utilizzo di nuove tecnologie (per esempio l'utilizzo di tecniche di memorizzazione distribuita tramite rateless coding e, più in generale, l'uso di cloud computing) e di nuovi standard per classificazione dei metadati. In tale ambito, il progetto accurato di algoritmi di fusione dei dati è spesso sottovalutato nei sistemi attuali. Il ricorso alle tecniche di Intelligenza Artificiale per l'implementazione di tecniche di autoapprendimento e/o di apprendimento supervisionato dovrebbe essere perseguito in modo capillare, anche tenendo conto di un'eventuale, ma molto probabile, evoluzione nello spazio e nel tempo della minaccia. Evoluzione per la quale i segnali di preallarme potrebbero cambiare nel tempo sia per quanto concerne la loro intensità, sia addirittura per quanto attiene alla loro natura. Ad oggi, la maggior parte dei sistemi di sorveglianza fa scarso uso di algoritmi di controllo schedulati. Più in generale, la parte di controllo (per esempio, la reazione alla rivelazione di un evento particolare tramite emissione di uno specifico allarme) dei sistemi di sorveglianza attuali si rivela spesso inefficace.

Trend evolutivi

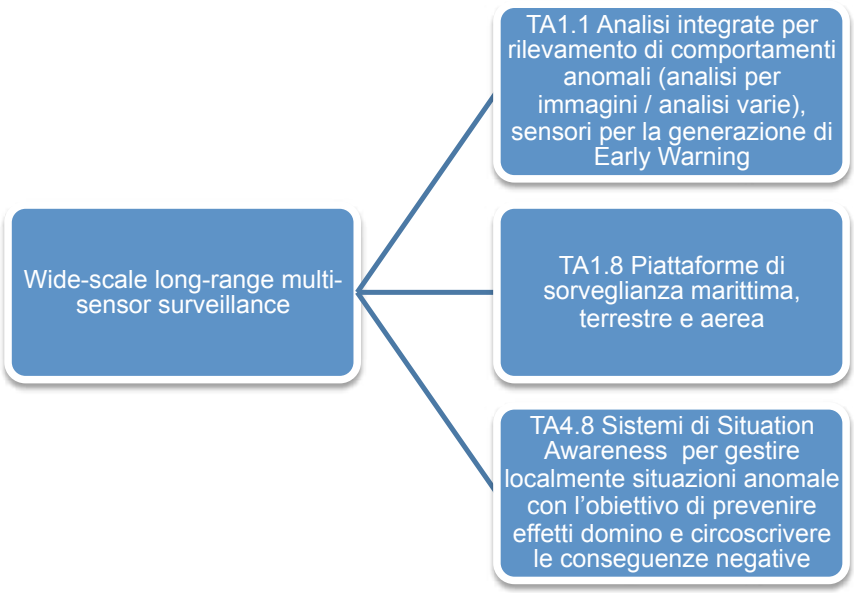
In generale, ambienti multi-sensoriali spazialmente distribuiti presentano opportunità e sfide interessanti per i sistemi di sorveglianza. La data fusion avrà un ruolo fondamentale per condividere l'informazione raccolta da sensori di tipo diverso. Gli aspetti di comunicazione giocano un ruolo chiave, soprattutto a causa dei limiti di banda o della natura asimmetrica delle comunicazioni. È da considerare attentamente la necessità di implementare sistemi di telecamere intelligenti con data-fusion a bordo: appare infatti impensabile, avendo per esempio equipaggiato una zona urbana di centinaia di telecamere, impiegare personale di supervisione in numero proporzionale a quello delle telecamere in funzione. Occorre invece che solo le scene riprese dalle telecamere che individuano una qualche anomalia (disponendo internamente dell'intelligenza necessaria allo scopo) siano presentate sui monitor della sala di controllo. Un altro aspetto fondamentale è legato alla sicurezza della comunicazione fra i moduli del sistema di sorveglianza. Infatti, in alcuni sistemi di sorveglianza i dati devono essere inviati su reti aperte ed il mantenimento della privacy e la gestione dell'autenticazione sono critici. Un altro trend evolutivo, soprattutto in termini di specifiche del sistema, riguarda la possibilità di avere capacità di apprendimento automatico al fine di caratterizzare modelli di scene/situazioni individuando i cosiddetti comportamenti anomali (abnormal behaviours) come segnali premonitori di eventi potenzialmente pericolosi.

Livello attuale di TRL 8-9

Costo associato per arrivare a TRL +1 (anni ed investimento economico)

Si stima in 3-4 anni la durata del periodo di transizione tra TRL 8-9 a TRL 9

I TA di riferimento TA2



- **Communication, Command, Control and Information Systems**

Descrizione dello Stato dell'arte

Un "Communication, Command and Control and Information System" dovrebbe essere in grado di coordinare e supportare nell'esecuzione dei propri compiti tutte le organizzazioni coinvolte nella prevenzione e gestione di incidenti e crisi; il sistema in particolare dovrebbe facilitare:

- le comunicazioni e lo scambio di informazioni necessarie per la costruzione e condivisione della situazione sul campo
- il monitoraggio della situazione e la determinazione delle azioni da compiere (ai vari livelli di comando previsti) per l'ottimizzazione delle risorse disponibili
- l'invio dei relativi comandi alle strutture subordinate e la ricezione di rapporti sull'evoluzione della situazione e sullo stato di avanzamento delle attività.

L'elevato numero di organizzazioni coinvolte e la loro relativa autonomia fa sì che in Italia, come in tutte le altre nazioni europee, non risulta ancora possibile ipotizzare l'impiego di un unico sistema che possa essere utilizzato da tutte le organizzazioni coinvolte. La situazione diviene ancora più complessa se si considera il caso, di crescente interesse, di partecipazione congiunta da parte di organizzazioni di paesi diversi, dovuto sia al loro possibile coinvolgimento diretto (crisi "cross border"), sia al desiderio di aiutare la nazione colpita (attivazione del meccanismo di Protezione Civile Europea); infatti 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 a cui appartengono, con conseguente diversificazione della struttura di Comando, delle responsabilità assegnate ai vari livelli (strategico o di coordinamento, tattico, esecutivo) e della loro dislocazione fisica. Il rimedio ai problemi di interoperabilità è in genere costituito dalla definizione ed adozione di opportuni standard; è noto tuttavia come l'implementazione e il mantenimento di un rigoroso processo di standardizzazione (compresa la necessità di verificare la conformità di apparati e sistemi) risulti in pratica un processo molto difficile, lungo e costoso,

specialmente in ambito internazionale, e possa rallentare l'evoluzione della tecnologia; d'altro canto l'adozione di standard meno rigorosi molto spesso non garantisce un sufficiente livello di interoperabilità.

Descrizione dei Gap tecnologici

Pur rappresentando la standardizzazione una valida soluzione a lungo termine, è prevedibile che ancora per molti anni, nonostante i tentativi di armonizzazione, le diverse organizzazioni mantengano una propria struttura e autonomia, continuando ad avvalersi degli strumenti di supporto attualmente disponibili (sistemi "legacy"). Risulta di conseguenza indispensabile avere la possibilità di rendere interoperabili tali sistemi 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.
La realizzazione di un tale sistema, e soprattutto la reale possibilità di essere adottato a livello nazionale o europeo, dipendono dalla preventiva risoluzione di alcuni problemi tecnici che potrebbero ridurne l'efficacia e la facilità di impiego.

- Il Sistema dovrà consentire agli utilizzatori di accedere a tutte le informazioni di interesse in modo completamente trasparente rispetto alle loro caratteristiche (sorgente, formato, modalità di accesso); l'accesso dovrà avvenire, anche per le informazioni gestite da sistemi "legacy", 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, …); l'operatore dovrà poter individuare e selezionare gli elementi di interesse e visualizzare in modo semplice informazioni di sempre maggiore dettaglio.
- Il Sistema dovrà essere dotato di specifici strumenti software che supportino la pianificazione delle operazioni (compresa quella di contingenza), l'interpretazione, l'analisi e la gestione delle informazioni, e il processo decisionale.
- È 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.

Le tecnologie richieste per l'implementazione del sistema hanno tutte un sufficiente livello di maturità ma richiedendo tuttavia ulteriori sviluppi per consentirne l'impiego nello specifico campo applicativo. In particolare i principali gap tecnologici sembrano essere rappresentati dalla mancanza di:

- Un'ontologia e una terminologia comune e standard che assicurino l'interoperabilità (es. simbologia).
- Architetture (es. SOA) che consentano l'integrazione di sistemi "legacy" senza richiedere la loro modifica e che rispettino vincoli stringenti di sicurezza delle informazioni.
- Strumenti di ausilio alla pianificazione delle operazioni, interpretazione ed analisi della situazione sul campo, ottimizzazione dell'impiego delle risorse disponibili.

- Strumenti di ausilio per specifiche categorie di utilizzatori (ad es. sistemi di assistenza per veicoli di soccorso e di intervento finalizzati a garantire il tempestivo raggiungimento delle aree di crisi)
- Interfacce uomo-macchina di tipo avanzate, che presentino caratteristiche comuni ma che al tempo stesso siano facilmente adattabili alle esigenze di specifiche tipologie di utilizzatori.
- Tool per la costruzione rapida di mappe modelli tri-dimensionali di infrastrutture.
- Tecniche e strumenti per il filtraggio delle informazioni al fine di evitare fenomeni di "information overload".
- Tool che consentano la collaborazione tra utenti distribuiti geograficamente e/o appartenenti a diverse organizzazioni nelle fasi di pianificazione e decisone.

Ovviamente è di fondamentale importanza anche la possibilità di disporre di strumenti affidabili e sicuri per i vari tipi di comunicazioni (voce, dati), argomento che viene comunque trattato a parte.

Trend evolutivi

I trend evolutivi più importanti nel campo dei "Communication, Command and Control and Information Systems" sono rappresentati dai seguenti concetti:

- impiego di strumenti largamente diffusi e di facile uso (ad es. impiego di "Google-earth" per la rappresentazione dello scenario, impiego di strumenti per la cooperazione tipici dei social network) che consentano di utilizzare, a costo praticamente nullo, una serie di informazioni (es. mappe) e di funzionalità avanzate e che garantiscano nel contempo un vasto campo di applicazione (impiego di standard come il KML)
- evoluzione verso il concetto NEC (Network Enabled Capability) per consentire un rapido accesso alle informazioni rilevanti da parte di tutti gli attori coinvolti (crisis manager e first responder) e migliorare l'efficacia delle decisioni; l'approccio net-centrico si sta ormai diffondendo in campo militare ma appare ancora difficile da applicare in altri contesti a causa principalmente dell'indipendenza delle organizzazioni coinvolte.

Livello attuale di TRL

A seconda delle tecnologie il TRL è valutato a livello 3-5.

Step Necessari per arrivare a TRL + 1 (road-map)

Il raggiungimento dell'obiettivo di riduzione dei gap tecnologici richiede l'esecuzione coordinata di una serie di attività di ricerca.

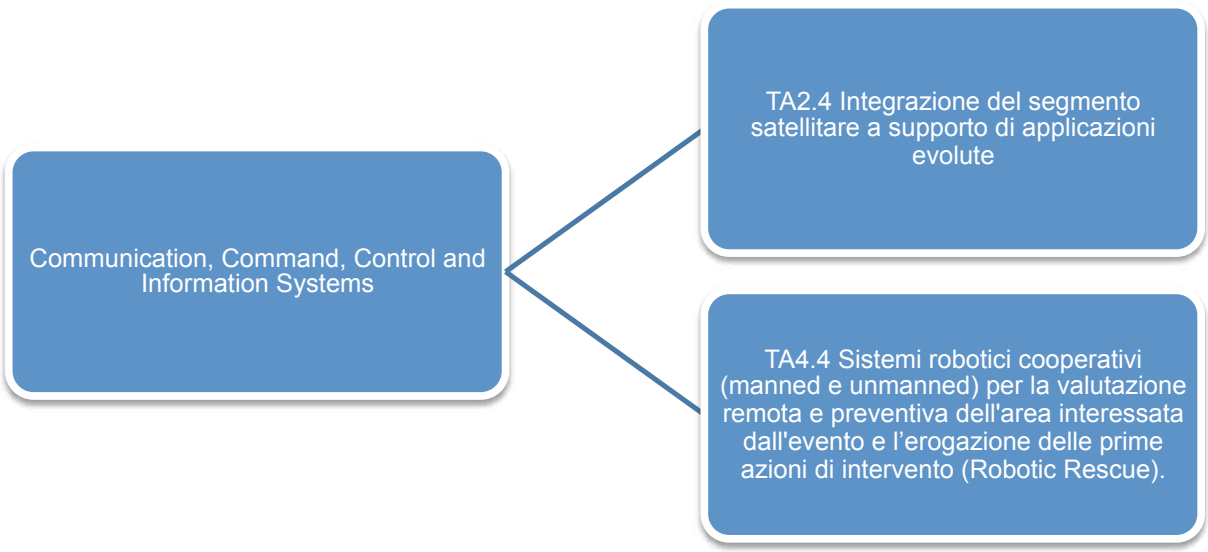
<2013-2015>	Studio e sviluppo di modelli architetturali per l'integrazione e l'interconnessione di sistemi legacy e per garantire l'interoperabilità tra sistemi disomogenei.
<2013-2014>	Sviluppo di un'ontologia comune e standard per l'interoperabilità, sviluppo di strumenti per la conversione di ontologie
<2014-2015>	Sviluppo di strumenti per Situation Awareness, con enfasi sulle problematiche di reperimento, filtraggio e rappresentazione delle informazioni e impiego di strumenti per la collaborazione remota (es. social networks)

<2014-2016> Sviluppo di tool di supporto decisionale, definizione e costruzione di una libreria di strumenti dedicati alla soluzione di problemi di specifiche categorie di utenti, nelle aree di pianificazione e gestione delle emergenze (simulazione di scenari e operazioni, ottimizzazione delle risorse, supporto decisionale).

Costo associato per arrivare a TRL +1 (anni ed investimento economico)

Anni: 4
Investimento: 15 M€

TA di riferimento TA4



- **Interoperability**

Descrizione dello Stato dell'arte

Il tema dell'interoperabilità a livello di operatori di rete e provider di servizi è un tema di ricerca molto attivo dall'ultimo decennio e che attualmente è alla base di molti sforzi di ricerca in ambito Future Internet per abilitare lo sviluppo di servizi a valore aggiunto secondo modelli user-centric e adattati al contesto. Tra le tecnologie e le specifiche allo stato dell'arte citiamo:

- IP Multimedia Subsystem, un modello architetturale proposto per realizzare la convergenza di servizi e di tecnologie di accesso attraverso un'infrastruttura all-IP;
- Service Delivery Platform: framework per la creazione, esecuzione, gestione e tariffazione di servizi a valore aggiunto, tipicamente in ambito Telco;
- Specifiche e tecnologie Service Oriented Architecture, inclusi Web Service;
- Web 2.0, inclusi servizi REST e Web Mashup.

Nel caso particolare di interoperabilità di sistemi satellitari con reti terrestri sono richiesti alcuni adattamenti funzionali e protocollari specifici dovuti alla presenza di ambienti di comunicazione

completamente diversi (es. in termini ritardi di propagazione, richiesta dinamica di banda, ecc). La pila protocollare satellitare coinvolge protocolli, meccanismi e segnalazione spesso non interoperabili con quelli di altri sistemi. A tale proposito sono spesso utilizzati elementi di rete, quali gateway, proxy o acceleratori (es. PEP – Performance Enhancing Proxy), che effettuano operazioni di interfaccia. Questi elementi di interfaccia sono spesso fonti di vulnerabilità, in quanto violano la semantica end-to-end di alcuni protocolli TCP/IP, e rappresentano un ostacolo ad offrire sicurezza in maniera adeguata, nonché al trasporto di eventuali servizi di tipo real-time con garanzia di consegna dei pacchetti (per es. telemedicina, teleoperazione di macchinari e robot). In tema di sicurezza va sottolineata l'incompatibilità tra il protocollo IPsec e i PEP. Alcune soluzioni sono state proposte (Multi-Layer IPsec, Cross-Layer IPsec, Hop-by-Hop IPsec), ma ognuna con delle problematiche relative al livello intrinseco di sicurezza fornibile. Per progettare un sistema di sicurezza adeguato occorre considerare gli standard e le tecnologie satellitari più diffusi in modo da applicare meccanismi di sicurezza efficienti. Il DVB-S/S2 per il collegamento di andata (da hub a terminali satellitari), il DVB-RCS1/2 per il collegamento di ritorno in cui vengono specificati vari algoritmi di assegnazione di banda su domanda (BoD=Bandwidth o Demand), l'architettura BSM (Broadband Satellite Multimedia), che definisce un'interfaccia "satellite indipendent" per facilitare l'interoperabilità, lo standard GMR (Geo-Mobile Radio) per servizi voce via satellite (analogo del GSM terrestre), il GSPS (Global Satellite Phone Service) utilizzato dai sistemi INMARSAT per servizi a basso ritmo di trasmissione, S-MIM (S-band Mobile Interactive Multimedia), che integra il satellite con sistemi terrestri mobili. I protocolli, l'architettura e conseguentemente le soluzioni d'interfaccia dipendono dalla specifica applicazione che si intende supportare.

Descrizione dei Gap tecnologici

Nonostante l'interesse degli operatori verso la creazione di servizi a valore aggiunto basati sulla composizione di funzionalità eterogenee (es. Telco, servizi IT, Web 2.0), le problematiche da affrontare sono molteplici ed includono:

- necessità di modelli di descrizione e composizione dei servizi (in particolare, estensione di modelli e metamodelli di composizione dei servizi in ambito Telco)
- necessità di meccanismi efficienti di gestione e controllo e allocazione di servizi e risorse di rete

A livello di rete, necessita progettare architetture e protocolli adatti alle caratteristiche fisiche e gestionali della rete eterogenea complessiva. I requisiti possono essere completamente diversi da quelli considerati per la progettazione degli attuali protocolli. Allo stesso tempo, occorre garantire prestazioni comparabili a quelle riscontrate nei sistemi "stand-alone". In ambito di sicurezza, i sistemi satellitari prevedono protocolli specifici e quindi di difficile adattamento con quelli installati in sistemi terrestri (protocolli "satellite-dependent"). Infatti, la sicurezza è spesso applicata negli strati più bassi della pila OSI (es. DVB-CA), rendendo difficile l'interoperabilità con altri sistemi in un contesto di comunicazione sicuro. D'altra parte le caratteristiche fisiche di un collegamento satellitare rendono poco efficiente l'utilizzo di tecniche e meccanismi consolidati in altre reti. Ad esempio, gli elevati ritardi e soprattutto il jitter hanno un impatto negativo sui protocolli di scambio chiavi di sicurezza (es. IKE), oppure la variabilità temporale della banda disponibile potrebbe impattare sul sincronismo su cui si basano alcuni sistemi di autorizzazione/login.

Trend evolutivi

Alcuni dei trend evolutivi che mirano a superare i gap tecnologici sopra identificati sono accomunabili nello sforzo di creare architetture funzionali, denominate “Service Overlay Network”, capaci di fornire funzionalità avanzate per la creazione e l’esecuzione di servizi a valore aggiunto con caratteristiche di context-awareness e auto-adattamento. In tale contesto, sono di riferimento le specifiche Next Generation Service Overlay Newtork in corso di definizione da parte del gruppo di lavoro IEEE P1903. Per realizzare tali specifiche, sono in corso attività di ricerca volte a definire nel dettaglio specifiche per:

- Modelli di descrizione e composizione dei servizi (SCXML, BPEL, BPMN)
- Modelli autonomici e di self-adaptation cross-layer per garantire l’autoaggiustamento, la robustezza e la resistenza ai guasti dei sistemi coinvolti.

Per quanto riguarda l’interoperabilità con sistemi satellitari, occorre prima di tutto definire la migliore architettura/configurazione per garantire le prestazioni e il livello di sicurezza dettati dai requisiti di sistema. Tra le varie architetture possibili, il ruolo del satellite può prevedere: backhauling, integrazione a complementare le capacità delle altre reti, soluzione di backup in caso di emergenze. A livello tecnologico, oltre all’ottimizzazione protocollare che riguarda tutti gli strati della pila OSI o elementi di rete evoluti come i PEP, sono stati proposti alcuni nuovi paradigmi di comunicazione basati su: meccanismi cross-layer oppure sulle DTN (Delay Tolerant Networks). Ognuna di queste soluzioni tecnologiche richiede consistenti modifiche dell’architettura di sicurezza e dei protocolli coinvolti.

Livello attuale di TRL 6-7

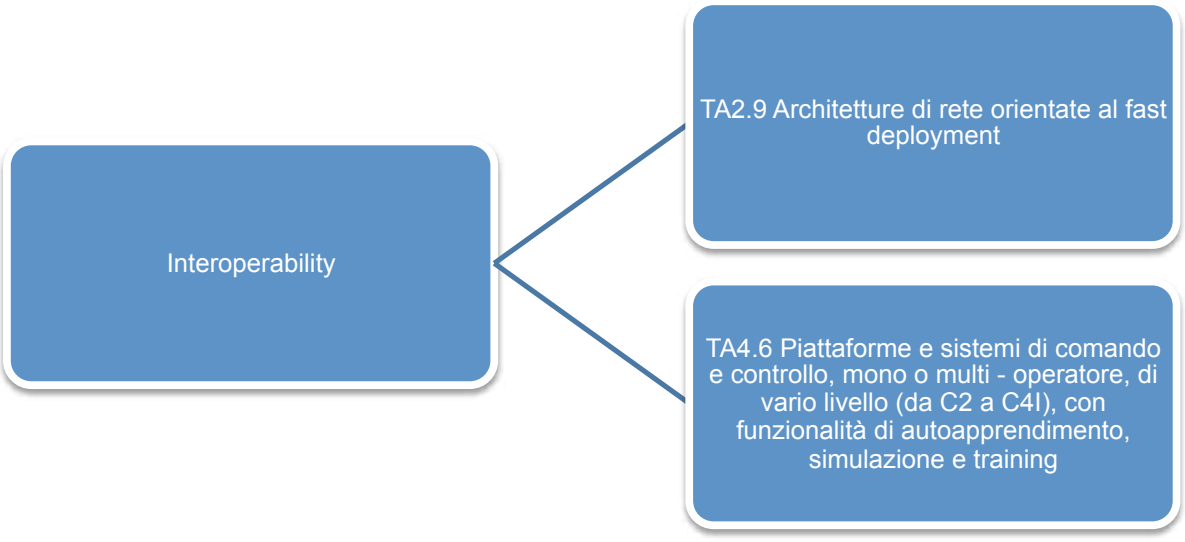
Step Necessari per arrivare a TRL + 1

Si stima necessario procedere in ognuna delle direzioni indicate (cross-layer, DTN, ecc.)

Costo associato per arrivare a TRL +1 (anni ed investimento economico)

Si stima in 3-4 anni la durata del periodo di transizione tra TRL 6-7 a TRL 7-8

I TA di riferimento TA2



- **Command & Information Systems Integration**

Descrizione dello Stato dell'arte

L'uso combinato di componenti indipendenti in un Sistema di Sistemi permette tipicamente di eseguire funzionalità non eseguibili separatamente dai singoli componenti. La complessità di un SoS è la misura dello sforzo e delle risorse richieste affinché un singolo componente sia in grado di comunicare e interoperare con gli altri elementi. Secondo il paradigma SoS, l'interoperabilità tra componenti eterogenei ed autonomi è quindi di estrema rilevanza ed è uno dei fattori che influenza in modo determinante le caratteristiche dei SoS in termini di "sviluppo evolutivo" (evolutionary development) e "comportamento emergente" (emerging behaviour). Le interfacce sono quindi entità di prima classe in un SoS, in quanto permettono lo scambio di informazioni tra i componenti che costituiscono il SoS. In tale contesto, il paradigma Service Oriented Architecture (SOA) è considerato da un'ampia comunità scientifica e industriale come un modello che risponde ai requisiti di interoperabilità e integrazione tra sistemi tipici dei SoS. Tra le tecnologie implementative esistenti del paradigma SOA, rivestono particolare interesse in ambito SoS gli Enterprise Service Bus (ESB). Gli ESB sono infrastrutture di messaggistica che offrono funzionalità di messaggistica, routing dei messaggi, integrazione, discovery di risorse e, in generale, servizi di intermediazione tra più nodi. Facilitano quindi il progetto e sviluppo di applicazioni distribuite basate su modelli orientati ai servizi e/o event-driven. Data l'eterogeneità dei sistemi coinvolti, la sicurezza è difficilmente centralizzabile. Ogni sistema è caratterizzato da specifiche vulnerabilità e prevede tecniche e meccanismi di sicurezza indipendenti dagli altri. Tuttavia, i SoS devono essere progettati ed eserciti in modo che una vulnerabilità su uno specifico componente non si presti all'attacco di altri componenti del sistema per il tramite di detta vulnerabilità. Per questo motivo, occorre implementare schemi di sicurezza multilivello (Multilevel Security). Per quanto riguarda le comunicazioni, l'integrazione può avvenire a livello IP, utilizzando il protocollo IPsec. Un'alternativa è l'introduzione di servizi di sicurezza a livello applicativo (es. HTTPS, TLS, SSL). Per applicazioni di sicurezza (sia civile che militare) e di emergenza (per esempio difesa civile) l'uso di SoS è fondamentale per rispondere ai requisiti operativi e già esistono diverse realizzazioni di reti a supporto delle operazioni di protezione civile ed altri enti istituzionali, basate sull'uso combinato di sistemi terrestri (PMR, DMR, Tetra, WiMax, LTE) e di reti satellitari (DVB RCS o standard proprietari).

Descrizione dei Gap tecnologici

Il progetto e lo sviluppo di SoS deve soddisfare requisiti complessi, determinati in particolare dal fatto che le componenti di un SoS sono autonome dal punto di vista operativo, nel senso che sono gestite per perseguire il loro scopo specifico e, in aggiunta, devono contribuire all'obiettivo globale del SoS. È quindi difficile determinare e addirittura simulare il comportamento di un SoS a partire dal comportamento dei suoi singoli componenti. Per superare questi gap tecnologici, un trend evolutivo consiste nell'arricchire i principi e le tecnologie SOA con modelli autonomici e tecniche di analisi e verifica formale. Un SoS richiede la creazione di nuove tipologie di sistemi che presentano comportamenti e problematiche simili a quelle riscontrabili in sistemi complessi. La soluzione delle problematiche di sicurezza dovrà seguire inevitabilmente le seguenti aree di ricerca:

- Indipendenza operativa degli elementi;
- Indipendenza gestionale degli elementi;

- Sviluppo evolutivo del sistema;
- Distribuzione geografica degli elementi;
- Approcci analitici interdisciplinari;
- Integrazione a livello di rete dei sistemi coinvolti;
- Gestione e garanzia della qualità del servizio end-to-end;
- Compatibilità protocollare (anche relativamente ai protocolli che implementano le funzioni di sicurezza).

Trend evolutivi

I trend evolutivi per il design e sviluppo di SoS affidabili includono:

- Tecniche di self-management e riconfigurazione dinamica che permettano di adattare il comportamento dei componenti ai cambiamenti dell'ambiente circostante o degli obiettivi stessi. Rule-based, machine learning, e tecniche di ottimizzazione per la selezione basata sulla QoS di servizi e risorse di comunicazione sono tecnologie candidate.
- Tecniche di analisi e verifica formale per assicurare l'affidabilità (dependability) del sistema nel suo insieme.

Nei SoS l'interazione tra diverse tecnologie, policy ed aspetti economici hanno un ruolo centrale per l'identificazione di nuove soluzioni. I principali temi di ricerca sono:

- Definizione di un contesto di riferimento e di un'architettura efficiente;
- Definizione di un lessico unificato;
- Selezione di nuove tecniche d'analisi, simulazione e modellazione

Gli attributi chiave da sviluppare nella progettazione di un SoS sono: la flessibilità, l'adattatività, la modularità, interfacce "open", awareness del contesto. Le interfacce sono senza dubbio tra le sorgenti principali di complessità del SoS. Miglioramenti possono riguardare i seguenti ambiti tecnologici:

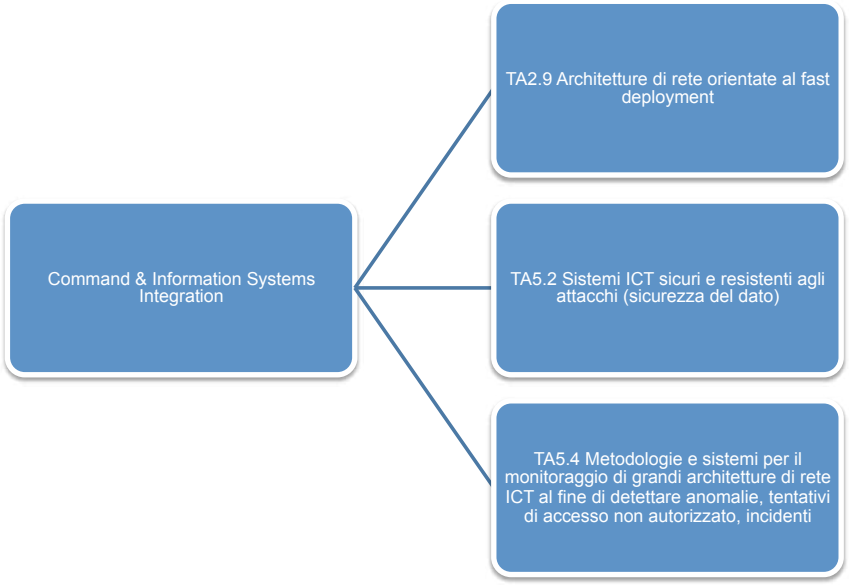
- Progettazione di protocolli di sicurezza end-to-end (IPsec-like) compatibili con le varie interfacce presenti nel SoS (Multilevel);
- Gestione della Qualità del Servizio (QoS) a diversi livelli della pila protocollare in modo da considerare l'effetto di meccanismi e algoritmi implementati nelle varie sotto-reti;
- Introduzione di un Network Management System unificato.

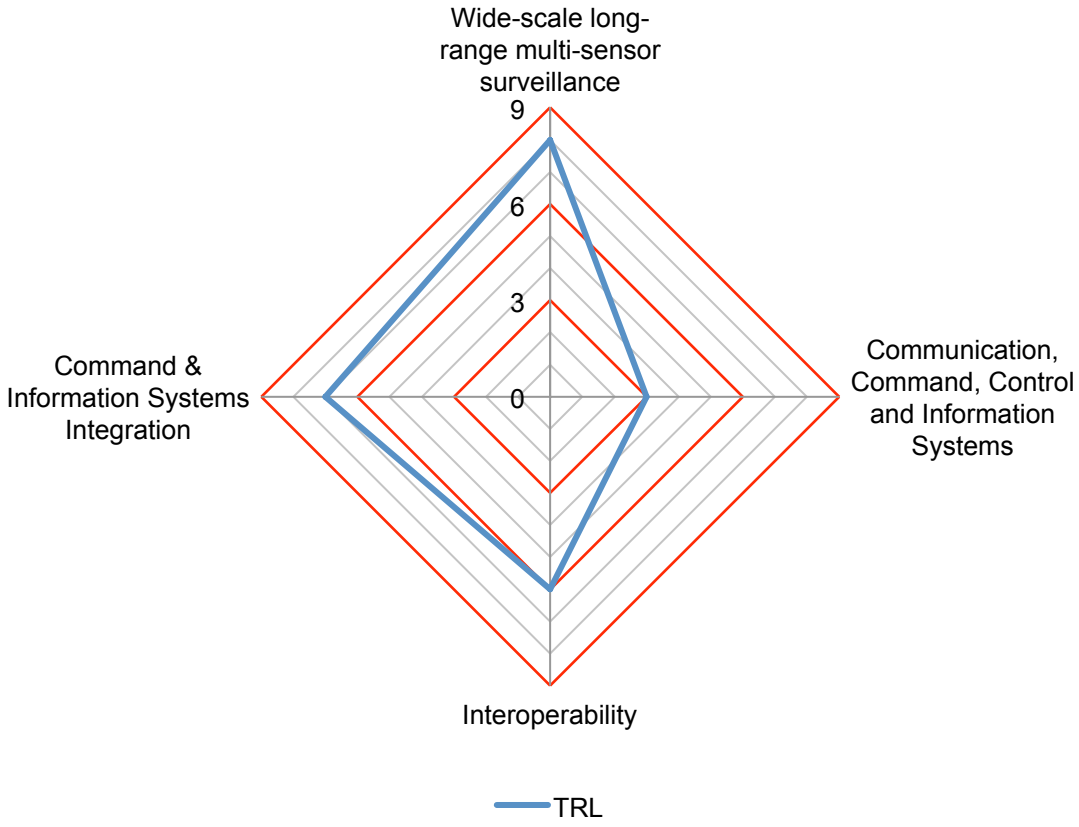
Livello attuale di TRL TRL 7-8

Costo associato per arrivare a TRL +1 (anni ed investimento economico)

Si stima in 3-4 anni la durata del periodo di transizione tra TRL 7-8 a TRL 8-9

I TA di riferimento TA2


Command & Information Systems Integration
TA2.9 Architetture di rete orientate al fast deployment
TA5.2 Sistemi ICT sicuri e resistenti agli attacchi (sicurezza del dato)
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


Wide-scale long-range multi-sensor surveillance
9
6
3
0
Communication, Command, Control and Information Systems
Interoperability
Command & Information Systems Integration
TRL

4.4.3 Networks and information security systems

Ambiti prioritari di ricerca

- Cyber protection systems and architectures (cyber security)
- Cyber threat detection
- Protezione della diffusione e memorizzazione dell'informazione

- **Cyber protection systems and architectures (cyber security)**

Descrizione dello Stato dell'arte

Per cyber-security si intende l'insieme di tecnologie, processi e metodologie progettati per proteggere reti, sistemi, programmi e dati da attacchi, danni o accessi non autorizzati. Il ruolo fondamentale assunto dalle Tecnologie per l'Informazione e la Comunicazione (ICT) nella nostra vita quotidiana ha prodotto, oltre ad innegabili benefici, un nuovo scenario nel quale risultiamo essere sempre più esposti a minacce di natura informatica, che non hanno più come obiettivo solo e soltanto il nostro personal computer, ma possono colpire qualsiasi sistema che usi le tecnologie ICT. Numerose sono le prove che dimostrano come queste minacce stiano rapidamente evolvendo ed abbiano ormai raggiunto livelli di elevata pericolosità e complessità. Azioni sofisticate, mirate e coordinate sono state condotte negli ultimi anni contro obiettivi sensibili, a riprova della diversa natura assunta dagli attacchi informatici e della dimensione globale che li caratterizza. Le botnet rappresentano un esempio della nuova generazione di attacchi, dal momento che esse si basano sull'uso di ampi e coordinati gruppi di host per eseguire sia azioni di attacco a forza bruta sia attacchi subdoli e pressoché invisibili, come i cosiddetti stealthy attack. Il concetto di cyber-security va, quindi, oltre quello tradizionale di sicurezza informatica ed il passo avanti è determinato proprio dalla nuova dimensione e complessità degli attacchi da fronteggiare e dall'impatto, anche di tipo economico e sociale, che essi possono avere. Non a caso il nuovo programma di ricerca HORIZON 2020 della Commissione Europea ha incluso cyber-security come uno dei temi chiave per affrontare la sfida della promozione di società inclusive, innovative e sicure. Nuove strategie e nuove tecnologie sono necessarie per far fronte a questa nuova forma di minacce e garantire la protezione del cittadino, delle infrastrutture e dei servizi. Gli attuali strumenti di sicurezza, sia quelli per la prevenzione che quelli per la rilevazione, sono stai progettati per proteggere una parte o un elemento dell'intero ecosistema dalla tipologia di attacchi in grado di sfruttare le vulnerabilità di quella parte o di quell'elemento. Risulta, invece, cruciale per la protezione di sistemi distribuiti e complessi adottare strategie globali di cyber-security che si basino su azioni coordinate che prevedano la collaborazione tra tutti gli attori coinvolti. È necessaria un'analisi estesa ed accurata di informazioni e dati riguardanti tutti i componenti e/o i livelli del sistema da difendere al fine di averne una visione completa e poter individuare con efficacia e tempestività i potenziali rischi e, qualora l'attacco sia già in corso, i suoi sintomi.

Descrizione dei Gap tecnologici

Le minacce contro il cosiddetto cyber-space, ossia il complesso agglomerato di persone, sistemi e servizi interagenti per mezzo di tecnologie ICT, possono essere classificate nelle seguenti 4 categorie: minacce contro beni e/o risorse personali, minacce contro beni e/o risorse di proprietà di organizzazioni, minacce contro beni e/o risorse virtuali e minacce contro infrastrutture. La varietà dei possibili attacchi, da quelli contro la privacy e la gestione dell'identità a quelli contro le infrastrutture critiche, rende l'idea della complessità che caratterizza il problema della individuazione delle soluzioni tecnologiche per garantire la cyber-security. Web 2.0, applicazioni P2P, Instant Messaging, voce e video su IP e, in generale, servizi su IP che stanno sostituendo quelli tradizionali, social networking sono solo alcune delle aree tecnologiche interessate da vulnerabilità ed esposte a cyber-attacks. Gli strumenti attualmente a disposizione per la cyber-security hanno limitate capacità dal momento che sono stati progettati e realizzati per far fronte ad un sottoinsieme delle problematiche che debbono essere tenute in

conto nel momento in cui si vuole elaborare una strategia di difesa di successo. Se facciamo riferimento, ad esempio, alla tecnologia SIEM (Security Information and Event Management), largamente usata per la protezione da cyber-attacks, i prodotti attualmente disponibili presentano limiti evidenti nella capacità di raccogliere ed elaborare informazioni dai diversi livelli (rete, sistema operativo, applicazione) di un sistema o da differenti domini (fisico, logico, virtuale). In generale, la lacuna principale delle attuali tecnologie per la cyber-security è quella di non fornire una visione globale dell'asset da proteggere e, quindi, di non consentire l'osservazione e l'elaborazione delle differenti manifestazioni e sintomi che accompagnano l'esecuzione di un cyber-attack.

Trend evolutivi

La natura globale dei cyber-attacks sta determinando un cambio di rotta nello sviluppo dei sistemi di sicurezza, che sono ora chiamati a gestire e correlare in tempo reale grosse moli di eventi ed informazioni di varia natura, di differente provenienza e caratterizzati da differenti formati, per incrementare il grado di protezione e migliorare la cyber-security. Tecnologie promettenti, quali Complex Event Processing, sono, infatti, oggetto di studio per essere utilizzate come supporto alla correlazione real-time di flussi di dati ed eventi raccolti da sorgenti eterogenee, finalizzata alla rilevazione di effetti distribuiti e di varia natura di uno stesso incidente di sicurezza. Un altro aspetto che sta caratterizzando l'evoluzione dei sistemi per la cyber-security è legato al concetto di trust. Gli strumenti per la protezione da cyber-attacks dovrebbero prevedere meccanismi per la gestione della trust, che consentano di stabilire il livello di affidabilità di una sorgente dati e, quindi, determinare se le informazioni da essa fornite possano essere usate come input al processo di valutazione dello stato di sicurezza di un'infrastruttura o di un sistema. Un ulteriore elemento che dovrà essere tenuto in conto nella definizione di strategie efficaci per fronteggiare le cyber-threats è rappresentato dalla necessità di consentire lo scambio di informazioni tra i diversi sistemi e attori coinvolti nella gestione della cyber-security al fine di rendere possibile l'attuazione di un approccio cooperativo che, sfruttando la complementarietà delle competenze in gioco, possa favorire l'azione di prevenzione e contrasto delle nuove tipologie di attacchi.

Livello attuale di TRL

A seconda delle tecnologie, il TRL è valutato a livello 3-4

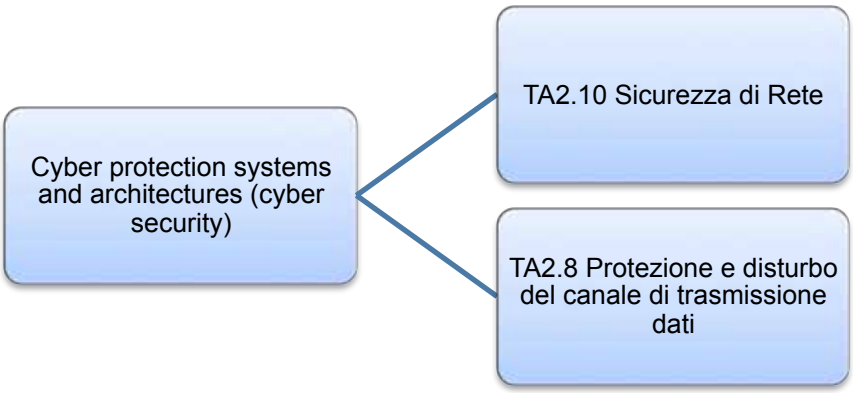
Step Necessari per arrivare a TRL + 1 (road-map)

2013-2015	Sviluppo di sistemi innovativi, trusted, multi-dominio e cross-layer per migliorare la cyber-security delle infrastrutture e dei servizi
2013-2015	Creazione di una piattaforma per *information sharing and exchange* che consenta l'interoperabilità tra i sistemi di differenti stakeholders al fine di incrementare al base di conoscenza nell'ottica di un approccio cooperativo alla cyber-security

Costo associato per arrivare a TRL +1

Anni: 2.5 Investimento: 20 MEuro

TA di riferimento TA5



- **Cyber threat detection**

Descrizione dello Stato dell'arte

La corretta, efficiente, e rapida identificazione di attacchi e minacce è una attività fondamentale, propedeutica a qualunque soluzione di protezione (di sistemi, dati, infrastrutture) o mitigazione di attacchi sviluppata o proponibile nel contesto cyber security. Le moderne tecniche di monitoraggio del traffico in reti e sistemi ICT e di rilevamento di minacce ed attacchi devono rispondere a numerosi requisiti, spesso tra loro contrastanti:

- **Accuratezza** – al fine di poter automatizzare le procedure di mitigation, eventualmente evitando ove applicabile un esplicito intervento umano, è strettamente necessario disporre di tecniche aventi al tempo stesso un elevato tasso di detection ed un basso tasso di falsi allarmi (requisiti tipicamente in conflitto);
- **Operatività in tempo reale** – Tempi di reazione estremamente rapidi sono possibili solamente operando con tecniche di threat detection "online", ovvero che prevedano l'analisi in tempo reale del traffico e la conseguente determinazione immediata di anomalie e minacce;
- **Scalabilità** – I moderni e futuri sistemi di monitoraggio devono essere pensati per gestire volumi di traffico estremamente significativi (In Internet si inizia a parlare di zetta-bytes, 10^{21} bytes), ed una sempre maggiore capillarizzazione delle infrastrutture di rete, con conseguente necessaria moltiplicazione dei punti di osservazione (vantage points).
- **Flessibilità** – a fronte di minacce polimorfe (si pensi per esempio al caso eclatante di sistemi di command&control per Botnet), ed in continua evoluzione, è necessario rispondere con strumenti di monitoraggio ed analisi estremamente flessibili, programmabili, e facilmente (e rapidamente!) adattabili al mutamento ed all'evoluzione delle minacce e delle forme di attacco.
- **Eterogeneità** – la correlazione tra allarmi o notifiche di anomalie provenienti da sonde o sensori eterogenei, atti a rilevare differenti aspetti (feature) del traffico a differenti livelli protocollari (livello di rete, livello applicativo, livello umano o sociale o comportamentale), o atti a quantificare anche aspetti non direttamente legati al traffico (ad esempio in infrastrutture quali smart grid), è tipicamente la chiave di volta per poter correttamente discriminare tra anomalie apparenti (causate da un comportamento legittimo) ed attacchi o minacce "reali".

Tali aspetti tipicamente emergono come trade-off caratterizzanti le attuali piattaforme di monitoraggio. Ad esempio, analisi offline sono tipicamente molto accurate, ma forniscono risultati in

ritardo. O ancora, soluzioni centralizzate possono avere problemi di scalabilità. Infine, mentre alcuni aspetti, come la capacità di correlare allarmi provenienti da sonde eterogenee, sebbene ancora centrali nelle attività di ricerca, cominciano comunque ad essere relativamente maturi, altri aspetti, come la flessibilità e programmabilità dei sistemi di monitoraggio, e le tecniche di analisi e correlazione online operanti a "wire speed", richiedono significativi sviluppi.

Descrizione dei Gap tecnologici

Le tecnologie che affrontano e risolvono gli aspetti discussi al paragrafo precedente hanno diverso grado di maturità, ma anche nei casi di tecnologie e soluzioni relativamente più consolidate sono richiesti ulteriori sviluppi per consentirne l'impiego in scenari applicativi reali. In particolare, i gap tecnologici più significativi includono:

1. Capacità di operare direttamente sui flussi di dati (eventualmente aggregati) e di prendere decisioni in tempo reale.
2. Capacità di correlare eventi eterogenei e semanticamente complessi, appartenenti sia al dominio della sicurezza logica che di quella fisica, garantendo tempestività (comportamento near real-time) e accuratezza (alto rate di detection abbinato a basso rate di falsi positivi).
3. Supporto efficiente all'elaborazione distribuita, con possibilità di effettuare elaborazioni complesse sia "at the edge" (cioè in nodi computazionali prossimi ai data feeds) che "in the core" (cioè negli stadi successivi dell'elaborazione, sui dati già pre-processati).
4. Scalabilità (intesa come capacità di allocare maggiore potenza di calcolo all'occorrenza), elasticità (intesa come capacità di rilasciare risorse di calcolo al diminuire del carico), e resilienza (intesa come capacità del sistema di monitoraggio di fornire un servizio fidato anche in presenza di attacchi e malfunzionamenti).
5. Versatilità, cioè la capacità di proteggere in maniera efficace infrastrutture eterogenee (quali ad esempio infrastrutture ICT per smart grids, trasporto multimodale, etc)

Trend evolutivi

Per colmare i gap tecnologici sopra menzionati è indispensabile lo sviluppo di:

- Tecniche efficienti ed accurate per stream analysis, ovvero in grado di operare direttamente sul flusso di dati (eventualmente aggregato) e prendere decisioni in tempo reale. Gli aspetti maggiormente critici a questo riguardo risultano essere: i) ottenere livelli di accuratezza e falsi positivi paragonabili a tecniche offline, ii) sviluppare tecnologie specifiche, eventualmente anche HW-intensive, per operare a wire speed su collegamenti multi-gigabit, e iii) ideare e validare nuovi algoritmi efficienti in termini di complessità computazionale e requisiti di memoria.
- Sistemi di correlazione real-time efficienti, basati sulla combinazione di paradigmi computazionali di stream processing e di Complex Event Processing (CEP), in grado di operare su dati ed allarmi altamente eterogenei.
- Tecniche e tecnologie per la convergenza tra sicurezza logica e fisica.
- Piattaforme flessibili e facilmente adattabili (mediante riprogrammazione o riconfigurazione anche in modalità online) alle mutate condizioni di contesto, minacce ed attacchi. Tale flessibilità supplementare non deve andare a scapito dell'efficienza e della sicurezza delle piattaforme stesse.
- Infrastrutture di monitoraggio ed analisi distribuite capaci di effettuare elaborazioni ed analisi

direttamente integrata nelle sonde (per ridurre la necessità di trasportare dati verso sistemi centralizzati di analisi), di normalizzare le osservazioni, di riconfigurarsi e riorganizzarsi a fronte di attacchi, di sfruttare - soprattutto "in the core" - le grandi potenze di calcolo rese disponibili dal paradigma emergente del cloud computing.

Livello attuale di TRL

A seconda delle tecnologie, il TRL è valutato a livello 3-4

Step Necessari per arrivare a TRL + 1 (road-map)

2013-2015	Sviluppo delle tecniche e delle tecnologie di stream processing e di Complex Event Processing (CEP), convergenza di sicurezza logica e fisica
2013-2015	Sviluppo di piattaforme integrate distribuite, applicabili anche a scenari non esclusivamente TLC
2014-2016	Exploitation delle nuove potenzialità offerte dal cloud computing (in particolare per quanto riguarda la protezione delle Critical Infrastructures)

Costo associato per arrivare a TRL +1

Anni: 2.5 Investimento: 20MEuro

TA di riferimento TA5

- **Protezione della diffusione e memorizzazione dell'informazione (network and storage protection)**

Descrizione dello Stato dell'arte

La protezione dell'accesso al dato e della diffusione dell'informazione assume sempre maggiore rilevanza in un contesto moderno caratterizzato da processi di gestione dell'informazione sempre più elaborati, che coinvolgono una molteplicità di entità e infrastrutture di comunicazione non sempre necessariamente fidate (ad es. outsourced). Garantire la confidenzialità e l'accesso selettivo all'informazione gestita è vitale non soltanto in ambito militare e del Segreto di Stato, ma anche nel mondo civile, ad esempio in organismi di salvaguardia dell'Ordine Pubblico o della popolazione e del territorio (dato il carattere vitale che tali informazioni possono avere rispetto al benessere della popolazione e alla preservazione dei servizi), in organismi privati quali banche o altre aziende di servizi (data la necessità di garantire contestualmente privatezza ed efficienza del sistema globale dei servizi), in infrastrutture critiche comunicanti quali i sistemi di distribuzione dell'energia, etc. L'approccio tradizionale a tale problema consiste nella specifica di infrastrutture ed architetture software atte a garantire uno scambio controllato di informazioni tramite, tipicamente, server di perimetro e reti private virtuali. Tale approccio mostra però una notevole complessità tecnico/gestionale, soprattutto in sistemi atti a gestire informazioni e/o flussi di dati appartenenti a reti di organizzazioni diverse su una stessa piattaforma (ad esempio piattaforme dual-user o multi-user). Inoltre, mostra limiti funzionali in contesti in cui la distribuzione e la memorizzazione dell'informazione è richiesta (per motivi di affidabilità e prestazioni, in condizioni di emergenza, etc) anche su server, cache, database o rendez-vous points (es. in contesti publish/subscribe) delocalizzati presso organizzazioni

intermediarie o per gestione esterna (outsourcing) non necessariamente fidate. Per far fronte a queste limitazioni, l'attuale trend evolutivo è incentrato nella radicale trasformazione dei paradigmi tradizionali di sicurezza dell'informazione: dalla protezione delle reti e dei sistemi, alla protezione del dato stesso (data centric security). Diversamente dall'approccio tradizionale incentrato sulla protezione del perimetro e che prevede il confinamento dei dati critici, tale muovo modello di sicurezza riconosce il livello di esposizione al rischio delle varie informazioni e mira a ripristinare la fiducia focalizzando l'attenzione sui dati stessi. Ciò si potrà ottenere soltanto combinando adeguatamente processi, semantica dei flussi informativi, e nuove tecnologie per la protezione del dato, sia a livello di distribuzione e memorizzazione (es. in database cifrati), che, idealmente, soluzioni crittografiche direttamente integrate nel dato stesso.

Descrizione dei Gap tecnologici

Le tecnologie discusse al paragrafo precedente hanno diverso grado di maturità. Ma anche nei casi di tecnologie relativamente più consolidate, sono richiesti ulteriori sviluppi per consentirne l'impiego in scenari applicati. In particolare:

- Per quanto riguarda architetture capaci di garantire un livello di confidenzialità differenziato su applicazioni e flussi informativi operanti a diverso livello, l'obiettivo è realizzare nuovi sistemi operativi partizionati e/o multilivello, che permettono la separazione delle informazioni a livello spaziale e temporale in modo completo ed affidabile, e garantiscono (anche su una stessa macchina di dimensioni ridotte e di tipo consumer) la completa indipendenza dei flussi di dati appartenenti a reti di organizzazioni diverse.
- Un ulteriore aspetto importante consiste nella creazione di middleware e sistemi avanzati, in grado di presiedere alla comunicazione controllata tra flussi di informazione appartenenti a differenti livelli, all'eventuale scambio selettivo di informazione in funzione di particolari condizioni di contesto, alla verifica del rispetto delle politiche di sicurezza ed alla gestione delle situazioni anomale e/o di rischio.
- Infine, per quanto riguarda la data-centric security, il livello di maturità è inferiore agli approcci sopra citati ma il possibile ritorno in termini di migliorato livello di sicurezza e maggior semplicità di gestione e controllo giustifica una forte attenzione. Gap tecnologici che si ritiene importante affrontare includono: i) sviluppo di tecnologie abilitanti (tecniche sistemistiche e/o crittografiche incentrate sul dato, e loro integrazione in database cifrati ed in protocolli per la distribuzione dei dati in rete), ii) soluzioni e metodologie per la gestione dei flussi informativi (modellistica di processi per la data-centric security, ontologie per la descrizione dei flussi informativi, modelli di policies per data-centric security, etc), e iii) applicazione, anche di tipo proof-of-concept, ad un sempre maggiore numero di contesti applicativi.

Trend evolutivi

La trasformazione, verso modelli di sicurezza incentrati sui dati, delle tecnologie e soluzioni per la protezione della diffusione e memorizzazione dell'informazione, rappresenta la naturale risposta ai trend evolutivi in corso nell'ambito delle architetture software orientate ai servizi, nelle architetture emergenti multi-utente e cloud, e nella sempre maggior penetrazione di sistemi multi-utente che prevedono applicazioni e flussi informativi operanti a diverso livello e con differenti requisiti di confidenzialità e di controllo delle politiche di accesso. In questo scenario, è possibile ipotizzare:

- un ulteriore sviluppo di tecnologie per la protezione del dato sia nella sia fase di distribuzione attraverso sistemi e domini amministrativi eterogenei, che nella sua memorizzazione di database cifrati in grado di supportare un range estremamente ampio di politiche di autorizzazione e controllo di accesso (role-based, attribute-based, purpose-based) anche dipendenti dal contesto (situazioni di emergenza, attacco, rischio, etc);
- Un ulteriore sviluppo, maturazione, ed applicazione "in campo" di nuove ed emergenti tecniche di protezione e controllo di accesso infrastructure-less, ovvero direttamente integrate nei dati stessi (sticky policies, Attribute-based encryption).
- La sempre più ampia maturazione e diffusione di middleware e strumenti software atti a semplificare la gestione ed il controllo della diffusione e lo scambio dell'informazione in
- scenari complessi e distribuiti, multi-utente e multi-autorità.

Livello attuale di TRL

A seconda delle tecnologie, il TRL è valutato a livello 3-4

Step Necessari per arrivare a TRL + 1 (road-map)

<2013-2015> Piattaforme multi-livello – specifica, sviluppo e sperimentazione di piattaforme per applicazioni multi-livello, inclusive di sistemi operativi partizionati e multilivello, sistemi di virtualizzazione del trasporto e distribuzione dell'informazione, sistemi preposti al controllo dell'interazione e scambio informativo tra livelli.

<2013-2015> Middleware per la gestione dell'informazione in sistemi eterogenei –studio, specifica e sperimentazione di sistemi software distribuiti per la gestione ed il controllo della diffusione e lo scambio dell'informazione in scenari complessi, multi dominio e multi autorità.

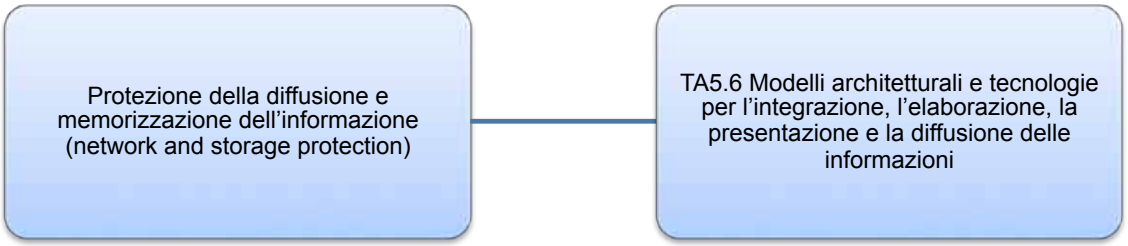
<2013-2015> Tecnologie ed algoritmi abilitanti la data centric security – studio ed applicazione di soluzioni innovative (crittografiche e sistemistiche) per la protezione dei dati e flussi informativi integrati nei dati stessi

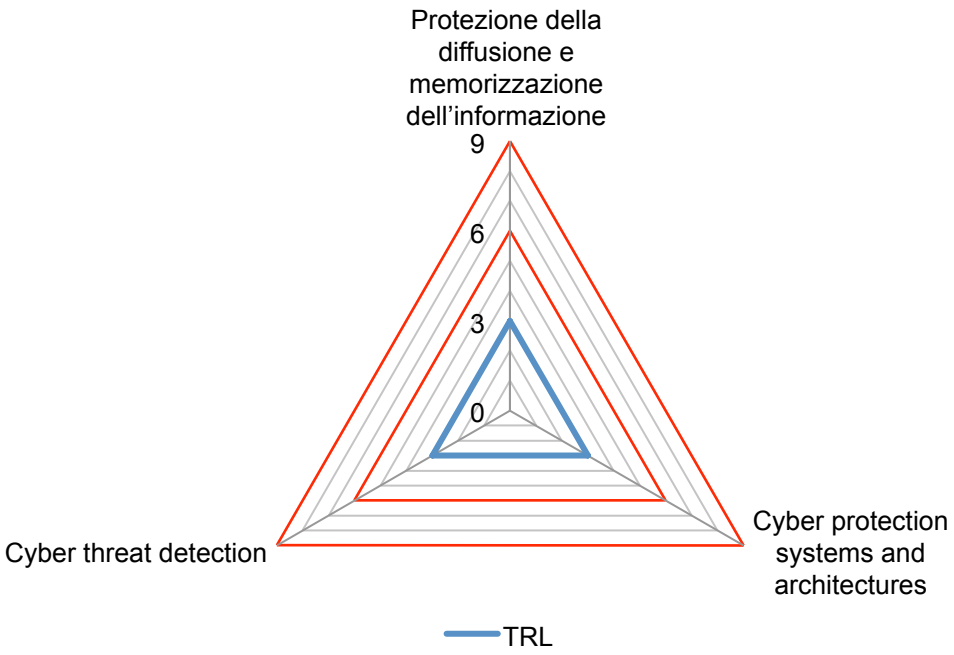
<2014-2016> Data-centric security – Studio, sviluppo, e sperimentazione in contesti applicativi di soluzioni integrate per la data-centric security e per i relativi processi di gestione della sicurezza anche in funzione del contesto.

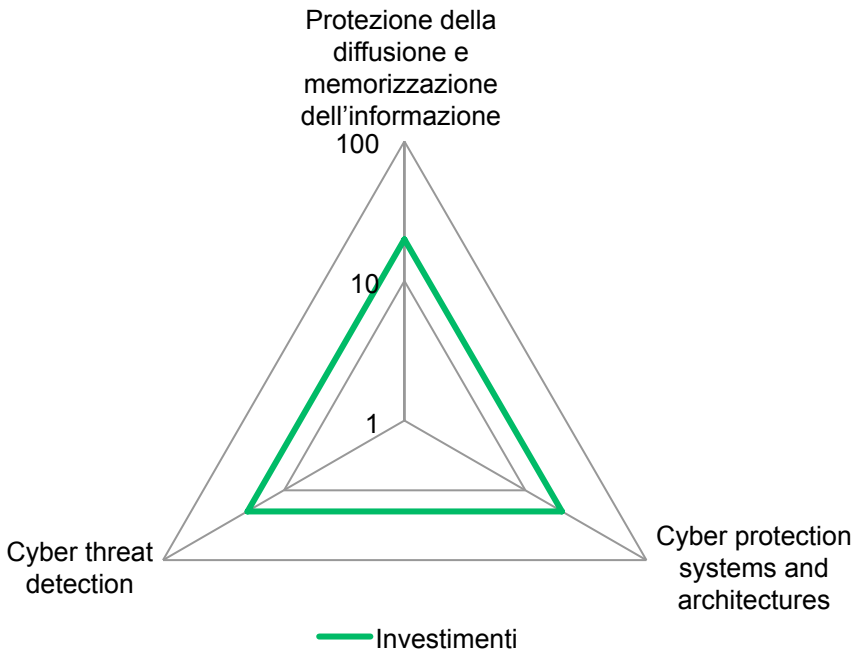
Costo associato per arrivare a TRL +1

Anni: 2.5 Investimento: circa 20 Meuro

TA di riferimento TA2, TA5




Protezione della diffusione e memorizzazione dell'informazione
9
6
3
0
Cyber protection systems and architectures
Cyber threat detection
TRL


Protezione della diffusione e memorizzazione dell'informazione
100
10
1
Cyber protection systems and architectures
Cyber threat detection
Investimenti

5. Curricula di coloro che hanno contribuito

Chairs

Cristina Leone. Laureata in Ingegneria Elettronica. In Finmeccanica dal 2003 coordina le attività europee in campo della sicurezza, gestendo la partecipazione delle aziende del Gruppo ai diversi programmi di ricerca. Precedentemente in Alenia Spazio, è stata Project Manager di apparati di bordo, con la responsabilità sia del presidio progettuale e tecnologico delle attività e che dell'interfaccia tecnica con i primi contractors di satellite. È Co-chair della piattaforma tecnologica SERIT e Chair del Security R&T Commitee di ASD (Associazione Europea delle Industrie dell'Aerospazio e della Difesa).

Fabio Martinelli. Laureato in Scienze dell'Informazione nel 1994, dottore di ricerca in Informatica Teorica nel 1998, dal 2005 è primo ricercatore presso l'Istituto di Informatica e Telematica del CNR. I suoi principali interessi di ricerca riguardano la sicurezza informatica e l'applicazione di strumenti informatici per la sicurezza. È coordinatore del progetto interdipartimentale sicurezza del CNR e della rete di eccellenza Europea NESSoS su cybersecurity per l'Internet del Futuro. È co-chair della piattaforma tecnologica SERIT.

Membri del Board

Michela Alunno Corbucci. Laurea Magistrale in Ingegneria Elettronica nel 2004. In Finmeccanica, si occupa di attività di ricerca per la Sicurezza in Italia e in Europa. Dal 2011 membro del comitato internazionale ASD-DRT (Aerospace Security & Defence - Defence Research & Technology) e del Gruppo di Lavoro RITEC (Ricerca e Tecnologia) di AIAD (Federazione delle Aziende Italiane per l'Aerospazio, la Difesa e la Sicurezza).

Luca Giannicchi. Laureato in ingegneria Ambiente e Territorio nel 2002 presso l'università La Sapienza di Roma e Master di II livello in ingegneria d'impresa nel 2008 presso l'università Tor Vergata di Roma. Dal 2005 lavora in Finmeccanica, presso la Direzione Tecnica, occupandosi delle attività europee di ricerca in ambito Security e coordinando la partecipazione della aziende del Gruppo ai relativi bandi di finanziamento. Dal 2010 segue la pianificazione scientifica e tecnologica delle aziende del gruppo che operano in campo civile ed in particolar modo gli scenari applicativi Smart City e Smart Grid.

Luca Papi. Laureato in Ingegneria dei Materiali presso l'Università degli Studi di Perugia e in Scienze Applicate ai Beni Culturali presso l'Università degli Studi Sapienza di Roma. E' tecnologo presso il Dipartimento ICT del CNR. E' membro del gruppo di coordinamento della Piattaforma SERIT e del gruppo di coordinamento delle attività del CNR nel settore spaziale nell'ambito della Piattaforma SPIN-IT (Space Innovation in Italy).

Daniele Sgandurra. PostDoc Researcher presso il Gruppo Sicurezza dell'Istituto di Informatica e Telematica del CNR di Pisa. I suoi campi di ricerca sono la cyber security, i sistemi di rilevamento delle intrusioni e la sicurezza dei dispositivi mobili. È membro del gruppo di coordinamento della Piattaforma SERIT.

Lista partecipanti

Enrico Appiani. Lavora presso la Direzione Strategie e Innovazione di Selex Elsag, come architetto di soluzioni cross-business e responsabile delle tecnologie di Cyber Security. Ha lavorato per oltre 30 anni nella Elsag di Genova, divenuta recentemente Elsag Datamat, come responsabile di progetti e ricerche su supercalcolo, pattern recognition, intelligence, sicurezza e homeland security.

Alessandro Barelli. Ricercatore all'Istituto di Anestesiologia e Rianimazione presso l'Università Cattolica del Sacro Cuore. Dirigente Medico U.O.C. Anestesia, Terapia Intensiva Postoperatoria e Terapia del Dolore e Responsabile del Centro Antiveleni al Policlinico Universitario "A. Gemelli". Direttore di Corso ALS (Advanced Life Support) e ERC (European Resuscitation Council). Direttore Regionale Europeo AHLS International Programme, (Advanced Hazmat Life Support). Direttore Programma europeo Hazmat (American Academy of clinical toxicology).

Paolo Bellofiore. Laureato in Ingegneria Elettronica indirizzo Telecomunicazioni, ha lavorato dal 1986 al 1991 in VitroSelenia. Dal 1991 lavora in Telespazio dove ha ricoperto diversi incarichi. Dal 1999 al 2007 è stato responsabile di prodotto dei Servizi a Valore Aggiunto (Formazione a Distanza e Telemedicina), dal 2007 al dicembre 2010 ha prestato la propria attività quale Senior Program Manager presso la Funzione Innovazione Tecnologica, seguendo specificatamente programmi di Telecomunicazione e Security. Dal 2011 lavora nella Funzione CTO, Ricerca Agevolata e Brevetti ed è Responsabile dell'Unità Organizzativa Programmazione, Gestione dei Programmi e IPR. Coautore di due richieste di Brevetto e di 6 pubblicazioni.

Alberto Bianchi. Referente in Selex Elsag dei programmi finanziati Europei e Italiani dei settori sicurezza fisica, biometria, cyber security, automazione, logistica, energia, infomobilità e trasporti

Giuseppe Bianchi. Professore ordinario presso l'Università degli studi di Roma Tor Vergata. La sua attività di ricerca è documentata da più di 170 pubblicazioni e i suoi lavori contano più di 8000 citazioni. E' stato coordinatore generale e tecnico/scientifico di diversi progetti europei, tre dei quali sulla sicurezza delle reti.

Sandro Bologna. Laureato in Fisica all'Università di Roma La Sapienza ha maturato una lunga esperienza nel campo della Safety&Security ricoprendo diverse posizioni. E' stato responsabile di Progetti di Ricerca nazionali ed internazionali, nonchè responsabile di Unità di Ricerca presso ENEA, maturando esperienze professionali in Italia, Europa e USA. Attualmente ricopre la carica di Presidente dell'Associazione Italiana esperti in Infrastrutture Critiche (AIIC) e Membro dell Experts Group in seno alla European Reference Network for Critical Infrastructure Protection (ERNCIP).

Daniele Cecchi. Laureato in Ingegneria Elettronica presso l'Università degli Studi di Roma La Sapienza nel 1976. Dal 1990 è stato responsabile dell'Unità di Ricerca e Sviluppo della Datamat S.p.A. per passare poi, con analogo incarico, in Elsag Datamat e quindi in Selex Sistemi Integrati, Unità di Business Grandi Sistemi dove lavora dal 2010 coordinando le attività di ricerca per il settore difesa e sicurezza.

Amedeo Cesta. Ricercatore CNR presso l'Istituto di Scienze e Tecnologie della Cognizione dove si occupa di intelligenza artificiale. Ha fondato e attualmente coordina il gruppo di Pianificazione e Scheduling dell'istituto. Ha condotto ricerche su diversi ambiti dell'Intelligenza Artificiale,come i Multi-Agent Systems, l'Interazione Uomo- Macchina, la Pianificazione & Scheduling.

Ester Ciancamerla. Ricercatrice all'ENEA dal 1979. Il suo principale interesse è su metodologie basate sul rischio, modelli e strumenti di modellazione per l'analisi di vulnerabilita' ed interdipendenze di Infrastrutture Critiche.

Donatello Conte. Laureato in Ingegneria Informatica nel 2002 presso l'Università "Federico II" di Napoli, e il Dottorato di ricerca in Ingegneria dell'Informazione nel 2006 presso l'Università di Salerno. Dal 2006 è Ricercatore nel settore scientifico disciplinare di Sistemi di Elaborazione dell'Informazione presso l'Università di Salerno. È membro dello IAPR e del Technical Committee 15 dello IAPR (Graph-based Representations in Pattern Recognition) dal 2002.

Luigi Coppolino. Ricercatore universitario nel settore dei sistemi per l'elaborazione dell'informazione. Attualmente è in servizio presso l'Università degli Studi di Napoli "Parthenope" . La sua attività di ricerca si focalizza principalmente nell'ambito della affidabilità e sicurezza dei sistemi di calcolo ed in particolare dei sistemi per la protezione delle Infrastrutture Critiche. L'Ing. Coppolino è stato coinvolti in numerosi progetti europei anche come consulente aziendale.

Ileana D'Angelo. Strategie e Innovazione di Selex Elsag, ha una consolidata esperienza di progetti industriali innovativi in ambito ICT e Sicurezza. Promuove il trasferimento tecnologico dalla ricerca all'industria, indirizzando lo sviluppo del piano strategico di innovazione aziendale.

Salvatore D'Antonio. Ricercatore presso l'Università degli Studi di Napoli "Parthenope". I suoi interessi di ricerca riguardano la sicurezza delle reti e la protezione delle infrastrutture critiche. Ha coordinato progetti di ricerca del Settimo Programma Quadro ed è coinvolto in attività di standardizzazione in ambito IETF ed ETSI.

Andrea De Gaetano. Dirigente di Ricerca CNR-IASI. Responsabile del Laboratorio di Biomatematica al CNR-IASI. Specialista in Chirurgia d'Urgenza all' Università degli Studi di Milano. Dottore di Ricerca in Matematica Applicata presso l'Universite' de Pau et des Pays de l'Adour. Laurea Magistrale in Giurisprudenza alla Università di Urbino. Autore di numerose pubblicazioni su Journals con Impact Factor.

Claudio De Lazzari. Laureato in Ingegneria Elettronica presso l'Università di Roma La Sapienza, specializzazione in Ingegneria Biomedica. Dal 1987 è ricercatore presso il Cnr, prima all'Istituto di Tecnologie Biomediche, attualmente all'Istituto di Fisiologia Clinica. I suoi principali interessi scientifici comprendono la modellazione del sistema cardiovascolare e di diversi dispositivi per l'assistenza meccanica circolatoria, la simulazione e l'ottimizzazione dell'assistenza ventilatoria.
Lo sviluppo di modelli numerici per lo studio della crescita delle cellule staminali cardiache in prossimità di tessuto necrotico. La telecardiologia.

Ethel De Paoli. Amministratore Delegato di Tecnoalimenti SCpA, biologa. Esperta in sistemi di trasferimento tecnologico nel settore agroalimentare.

Marco De Vito. Innovation manager presso Tecnoalimenti. Laureato in Scienze e Tecnologie alimentari presso l'Università Statale di Milano. Esperto in processi di sviluppo dell'innovazione nel settore agroalimentare.

Federica Di Camillo. Laureata in Giurisprudenza presso l'Università degli Studi di Roma "La Sapienza". Responsabile di ricerca nell'Area Sicurezza e Difesa dell'Istituto Affari Internazionali (IAI), si occupa di aspetti istituzionali della politica europea di sicurezza e di difesa e di mercato della difesa e sicurezza. Dal 2005 è impegnata in attività di analisi e di networking con responsabilità di progetti comunitari relativi a problematiche di sicurezza a livello nazionale ed europeo con particolare riguardo a strategie e sviluppi istituzionali, capacità ed evoluzioni tecnologiche, terrorismo internazionale ed armi non convenzionali, cyber security. Selezionata dal Dipartimento di Stato statunitense per la partecipazione all'International Visitor Leadership Program sul tema "U.S. - European Security Issues" (2010). Dal 2011 rappresentante IAI presso IMG-s (TA6) e SERIT (TA6).

Daniela Drimaco. Ha conseguito nel 2005 la Laurea in Ingegneria delle Telecomunicazioni presso l'Università di Napoli Federico II. Da 6 anni lavora presso Planetek Italia s.r.l. come Business Development Manager nel settore della ricerca e sviluppo con particolare attenzione all'ambito dei sistemi e delle infrastrutture spaziali per sistemi di Osservazione della Terra.

Gianluigi Ferrari. E' Professore Associato di Telecomunicazioni presso l'Università di Parma, dove coordina il Wireless Ad-hoc and Sensor Networks (WASN) Lab del Dipartimento di Ingegneria dell'Informazione.

Paolo Antonio Fichera. E' ricercatore senior presso il laboratorio di Robotica (UTTEI-ROB) del Centro Ricerche Casaccia dell'ENEA. Dopo un'esperienza in Montedison nel settore della manutenzione di grossi impianti industriali è entrato in ENEA nel 1987. Ha operato principalmente nei campi della teleoperazione, della robotica industriale avanzata e della robotica mobile autonoma. E' membro del gruppo europeo di Security IMGS-TA e co-chair dell'Area TA4 di Serit.

Pasquale Foggia. Ha conseguito la Laurea in Ingegneria Informatica nel 1995 e il Dottorato di Ricerca in Ingegneria Informatica ed Elettronica nel 1999 presso l'Università "Federico II" di Napoli. Dal 2004 al 2008 è stato Professore Associato nel Dipartimento di Informatica e Sistemi della stessa università, mentre dal 2008 svolge lo stesso ruolo all'Università di Salerno. È membro dello IAPR ed è stato coinvolto in numerose iniziative dello IAPR Technical Committee 15 dal 1997.

Gianfranco Fornaro. Primo ricercatore presso l'Istituto per il Rilevamento Elettromagnetico dell'Ambiente del CNR. Da circa 20 anni svolge attività di ricerca nel settore Radar ad Apertura Sintetica (SAR) dove ha pubblicato diversi lavori sulle riviste internazionali di maggiore interesse, ottenendo anche prestigiosi premi. E' da diversi anni Professore Aggiunto nel settore dell'Ingegneria

delle Telecomunicazioni e docente presso la scuola estiva internazionale sui Radar/SAR del Fraunhofer Institute.

Alessandro Garibbo. Laureato nel 1988 in Ingegneria Elettronica presso l'Università di Genova. Ha frequentato la prestigiosa Scuola Superiore Guglielmo Reiss Romoli dell'Aquila dove si è specializzato in telecomunicazioni. Ha conseguito il Master of Science in Electrical Engineering presso il Politecnico della New York University nel 1991. Dal 1990 al 2000 ha lavorato in Telecom Italia. Ha fatto parte dei working group ESRAB per la definizione delle tecnologie di interesse per la ricerca europea per la sicurezza. Attualmente lavora nella Direzione Strategie e Innovazione di Selex Elsag.

Dino Giuli. Professore Ordinario del settore di Telecomunicazioni dell'Università di Firenze. E' stato Presidente del Centro di Servizi Informatici e Telematici dell'Università di Firenze e membro del Comitato Scientifico del CINECA. Dal 1996 è promotore e coordinatore scientifico del Dottorato di ricerca in Telematica e Società dell'Informazione. La sua attività di ricerca ha riguardato in larga misura il settore delle applicazioni della telematica e dei sistemi di monitoraggio ambientale. Dino Giuli è autore di oltre 150 pubblicazioni scientifiche. E' membro dell' AEI e senior member della IEEE.

Marco Gonnelli. Laureato in Ingegneria Informatica presso il Politecnico di Milano. Dal 2005 ha prestato servizio con il grado di Sottotenente di Vascello del Corpo delle Armi Navali della Marina Militare fino a che, nel 2008 ha iniziato la sua carriera nello stesso grado del Corpo delle Capitanerie di Porto. In questa veste ha svolto la propria attività prima presso il laboratorio di Telerilevamento dell'Accademia Navale Italiana di Livorno e poi presso il Reparto ITC e Sistemi di Monitoraggio del Traffico Marittimo del Comando Generale del Corpo.

Antonio Graziano. Laureato in Ingegneria Elettronica presso l'Università di Palermo nel 1988. Dopo aver lavorato nella divisione R&D di Ericsson Fatme, nel 1990, è entrato a far parte di SELEX Sistemi Integrati (originariamente SELENIA), come analista di sistema. E' stato team leader di progetti di studio, nazionali e internazionali, sul tracciamento, fusione dati e network centric warfare (NCW).

Patrizia Grifoni. Laureata in Ingegneria Elettronica nel 1990 presso l'Università "La Sapienza" di Roma. Dal 1990 è ricercatrice CNR all'Istituto di ricerca sulle Politiche Sociali e della Popolazione. Dal 1993 al 200, è stata professore a contratto di "Elaborazione delle Immagini" all'Università di Macerata. E' autrice di oltre 130 pubblicazioni scientifiche.

Daniele Gui. Professore associato all'Istituto di Clinica Chirurgica dell' Università Cattolica del Sacro Cuore. Direttore U.O.C. Chirurgia d'Urgenza, Policlinico Universitario "A. Gemelli" di Roma. Associato di ricerca CNR-IASI. Fellow del American College of Surgeons (FACS). Direttore di Corso ATLS (Advanced Trauma Life Support). Autore di numerose pubblicazioni su Journals con Impact Factor. Principal Investigator di numerosi studi clinici.

Antonino Iacoviello. Dottore di Ricerca in Amministrazione pubblica europea e comparata – Università di Roma La Sapienza - Ricercatore in Diritto Pubblico presso l'Istituto di Studi sui Sistemi Regionali Federali e sulle Autonomie "Massimo Severo Giannini" del Consiglio Nazionale delle Ricerche (ISSIRFA-CNR). Docente a contratto presso la Scuola Sottuficiali della Guardia di Finanza – L'AQUILA, già

Avvocato in Roma - Materie di interesse: Diritto pubblico; Diritto amministrativo; Diritto dell'Unione europea.

Ivo Iavicoli. Ricercatore Confermato (Professore Aggregato) all' Istituto di Medicina del Lavoro della Università Cattolica del Sacro Cuore. Dottore di ricerca in Medicina del Lavoro e Igiene Industriale presso l' Università degli Studi di Milano. Adjunct Professor, School of Public Health Sciences, University of Massachusets at Amhearst.

Michele Luglio. Laureato in Ingegneria Elettronica e Dottore di Ricerca. Dal 1995 al 2004 è stato ricercatore universitario e dal 2004 è professore associato di Telecomunicazioni presso l'Università di Roma "Tor Vergata". Nel 2001 e 2002 è stato Visiting Professor presso l'Università della California Los Angeles.

Donato Macone. Ingegnere, dottorando presso il dipartimento di Ingegneria Elettronica, delle Telecomunicazioni e Informatica dell'Università La Sapienza di Roma. Ha conseguito nel 2007 la laurea in Ingegneria Informatica e nel 2009 la laurea magistrale, sempre in Ingegneria Informatica. Ha partecipato a diversi progetti europei.

Elena Maestri. Professore associato di Biologia Applicata presso l'Università di Parma. Le attività di ricerca riguardano le biotecnologie ambientali e la sicurezza alimentare, in particolare la presenza di contaminanti di origine intenzionale o accidentale. E' autrice di oltre 100 pubblicazioni.

Sabina Magalini. Ricercatore Confermato (Professore Aggregato) all' Istituto di Clinica Chirurgica della Università Cattolica del Sacro Cuore. Dirigente Medico U.O.C. Chirurgia d'Urgenza del Policlinico Universitario "A. Gemelli". Associato di Ricerca CNR-IASI. Fellow del American College of Surgeons (FACS). Autrice di numerose pubblicazioni su Journals con Impact Factor. Principal Investigator di numerosi studi clinici.

Lucio Marcenaro. Più di 10 anni di esperienza nell'elaborazione di immagini e sequenze video. Autore di più di 30 articoli scientifici in questo ambito di ricerca. Dopo la laurea in Ingegneria Elettronica nel 1999, ha ricevuto il dottorato di ricerca in Informatica ed Elettronica nel 2003. Dal 2003 al 2012 è stato Amministratore Delegato e responsabile dello sviluppo di TechnoAware srl. Dal marzo del 2011 è ricercatore universitario in Telecomunicazioni presso la Facoltà di Ingegneria dell'Università di Genova.

Lorenzo Marchesi. Referente Programmi Cofinanziati e GCP, Sezione Fisiopatologia dello Shock (struttura di ricerca congiunta IASI-CNR/UCSC).

Nelson Marmiroli. Professore Ordinario di Tecnologie Ricombinanti presso l'Università di Parma. Le sue attività di ricerca riguardano le applicazioni della genomica e proteomica alle biotecnologie ambientali e alla sicurezza alimentare. In questo contesto ha coordinato progetti nazionali ed internazionali, esplorando strumenti per la prevenzione e la difesa contro frodi alimentari e contro attacchi intenzionali alle risorse agroalimentari e ambientali. E' autore di oltre 150 pubblicazioni e dirige un gruppo di ricerca di 20 unità.

Michele Minichino. In ENEA dal 1981, e' coordinatore del programma per la Protezione delle Infrastrutture Critiche. Il suo principale interesse di ricerca e' su metodi, algoritmi, strumenti e modelli per l'affidabilità, la sicurezza e la qualità di servizio di sistemi critici interagenti.

Laura Moltedo. Laureata in Fisica nel 1969, dal 1995 Dirigente di Ricerca CNR presso l' Istituto per le Applicazioni del Calcolo. nell'area Informatica Matematica e Applicazioni, distaccata presso il Dipartimento Patrimonio Culturale del CNR. Dopo essere stata membro del Consiglio Scientifico del Dipartimento Tecnologie dell'Informazione e delle Comunicazioni, è stata fino ad aprile 2012 membro del Consiglio Scientifico del Dipartimento Patrimonio Culturale.

Claudio Moriconi. Laurea in fisica. Direttore dei laboratory di robotica dell'ENEA dal 1995. Ha condotto numerosi progetti nazionali, europei ed in Antartide. Membro di comitati internazionali quali lo IARP (robotica), membro dell'SC SIRI fino al 2006, delegato security ENEA e membro in IMGS e SERIT

Silvana Moscatelli. Laureata in scienze politiche, dottore di ricerca in Ordine Internazionale e Diritti Umani presso l'Università Sapienza di Roma. Professore a contratto di Human Rights presso la Facoltà di Scienze Politiche, Sociologia, Comunicazione dell'Università Sapienza di Roma.

Annamaria Nassisi. Laureata in Fisica presso l'Università degli Studi di Roma "La Sapienza". Nel corso della sua carriera ha maturato una esperienza sia nel mondo universitario, come ricercatrice, che nel mondo della PMI, come analista e sviluppatore SW, e da circa 25 anni nel settore spazio iniziando come ingegnere di sistema fino all'attuale carica di responsabile delle iniziative sulla Security, a livello transnazionale, per la Thales Alenia Space.

Giuseppina Padeletti. Dirigente del Consiglio Nazionale delle ricerche, attualmente Direttore dell'Istituto per lo Studio dei Materiali Nanostrutturati del CNR. Expertise in Chimica e Scienza dei Materiali, per applicazioni in settori quali Sicurezza, Forense, Medicina, Beni Culturali.

Antonio Palucci. Responsabile del Laboratorio Diagnostiche e Metrologia dell'Unità Tecnica Sviluppo di Applicazioni della Radiazione dell'ENEA di Frascati che comprende 30 unità . Il Laboratorio DIM si occupa principalmente dello sviluppo di tecnologiche all'avanguardia elettro-ottiche per il monitoraggio locale o a distanza, e della loro successiva ingegnerizzazione ed impiego in campagne di misura dedicate. E' coordinatore di diversi progetti Europei e NATO nell'ambito della Security.

Stefano Pasquariello. Ha conseguito la laurea in ingegneria Elettronica presso l'Università "Sapienza" di Roma nell'anno 2000. Dopo varie esperienze di analista software, al suo ingresso in Datamat S.p.A, nell'unità di R&D Militare, assume la responsabilità di team leader in diversi progetti di ricerca internazionali. Attualmente in SELEX Sistemi Integrati S.p.A., si occupa del coordinamento delle attività di Research and Technology dell'azienda con particolare riferimento ai programmi di ricerca Europei Civili e Militari.

Piero Pellizzari. Comandante della Guardia Costiera Italiana. Si è laureato in Scienze Marittime e Navali presso l'Accademia Navale Italiana di Livorno, dove ha completato il corso di formazione per Ufficiali.

Dal 1996, è stato direttamente coinvolto in tutti i progetti relativi all'acquisizione e all'aggiornamento di beni e servizi che hanno interessato la Guardia Costiera nei settori delle comunicazioni, del controllo del traffico navale (VTS), della navigazione radio, del comando/controllo e dei sistemi di comunicazione destinati a bordo di tutte le nuove imbarcazioni della Guardia Costiera.

Gennaro Percannella. Ha conseguito la Laurea con lode in Ingegneria Elettronica nel 1998 e il Dottorato di Ricerca in Ingegneria Informatica ed Elettronica nel 2002 presso l'Università di Salerno. Attualmente è Ricercatore di Informatica e Visione Artificiale presso l'Università di Salerno, dove è membro del gruppo di ricerca MIVIA. È membro dello IAPR e autore di più di 60 articoli in riviste a conference internazionali nel campo della Computer Vision e della Pattern Recognition.

Palmiro Poltronieri. Laureato in Scienze Biologiche all'Università del Salento ed ha conseguito il dottorato di ricerca in Biologia e Patologia cellulare e molecolare presso l'Università degli studi di Verona. Dal 2001 è ricercatore CNR a tempo indeterminato all'Istituto di Scienze delle Produzioni Animali.

Elaheh Pourabbas Dolataba. Laureata in ingegneria elettronica presso l'Università degli Studi di Roma "La Sapienza" ed ha conseguito il dottorato di ricerca in Bioingegneria presso l'Università degli Studi di Bologna. Nel periodo 1997-2000 è stata ricercatrice a tempo determinato presso l'Istituto di Analisi dei Sistemi ed Informatica (IASI) "Antonio Ruberti" - Consiglio Nazionale delle Ricerche (CNR). Nel 2001 è risultata vincitrice del concorso di ricercatore presso l'Istituto di Analisi dei Sistemi ed Informatica (IASI) "Antonio Ruberti" - CNR.

Raffaello Prugger. Direttore di Tecnoalimenti dal 2007. Oltre 20 anni di attività nella realizzazione e condizione della ricerca industriale a livello nazionale ed europeo. Auditor internazionale di progetti e valutatore progetti FP6.

Carlo Regazzoni. Laureato in Ingegneria Elettronica, ha conseguito il titolo di Dottore di Ricerca in Telecomunicazioni dall'Università di Genova. Dal 1990, è responsabile dell'area Industrial Signal and Image Processing (ISIP) del gruppo di ricerca in Elaborazione dei Segnali e Telecomunicazioni (SP&T) nel dipartimento di ingegneria biofisica ed elettronica (DIBE). Dal 1999 è responsabile del Gruppo SP&T. Dal 1995 è stato dapprima ricercatore, poi professore associato (2000) ed infine professore straordinario nel raggruppamento Ingegneria Informatica delle Telecomunicazioni (2005).

Luigi Romano. Dal 2010 Professore Ordinario per il settore scientifico-disciplinare Sistemi di elaborazione delle informazioni. In attesa della presa di servizio, riveste ancora il ruolo di Professore Associato presso la Facoltà di Ingegneria dell'Università degli Studi di Napoli "Parthenope". È un esperto di sistemi di rete critici. Collabora con la European Network and Information Security Agency. È membro del gruppo IMG-S TA, un'organizzazione promossa dalla AeroSpace and Defence Industries Association of Europe con il compito di formulare proposte per la Commissione Europea riguardo alle linee di finanziamento per la sicurezza informatica.

Francesco Saverio Romolo. Professore a contratto ed EP, SAPIENZA Università di Roma "Sapienza" – Dipartimento di Medicina Legale. Chargé de cours, Maître assistant titolare del corso "Chimica analitica in materia di sicurezza", Università di Losanna (Svizzera). Pubblica e partecipa a gruppi di lavoro e progetti di ricerca finanziati a livello nazionale ed internazionale in materia di sicurezza.

Vittorio Rosato. Laurea e Dottorato di Ricerca in Fisica. In ENEA dal 1990, è attualmente Responsabile del Laboratorio Infrastrutture Informatiche e Tecnologiche presso il Centro Ricerche Casaccia (Roma). Si occupa di analisi di sistemi complessi e di modelli di simulazione delle Infrastrutture Critiche. E' Coordinatore della Divisione Futuro del Polo ICT della Regione Abruzzo, co-fondatore e attuale Presidente di Ylichron S.r.l.

Cesare Roseti. Laureato in Ingegneria delle Telecomunicazioni presso l'Università degli Studi di Roma "Tor Vergata". Nel 2003 e nel 2004 ha collaborato ad attività di ricerca presso il "Computer Science Department" dell'Università della California (LA). Nel 2009 ha ricevito il "Premio Innovazione Finmeccanica 2009" da Telespazio. Nel 2009 ha conseguito il master in "Homeland Security" presso l'università di Bologna. Attualmente è assegnista di ricerca e docente del corso "Laboratorio di segnali e trasmissione" all'università di Roma "Tor Vergata".

Giancarlo Salviati. Direttore di Ricerca del CNR, Professore a Contratto presso il Dipartimento di Fisica dell' Università di Parma e professore presso Anna University (Chennai). Ha pubblicato 200 lavori JCR ed è responsabile di 35 progetti internazionali e nazionali.

Mario Savastano. Laureato in Ingegneria Elettronica nel 1979 presso l'Università "Federico II" di Napoli. Dal 1982 lavora con il Consiglio Nazionale delle Ricerche ed attualmente è Primo Ricercatore dell'Istituto di Biostrutture e Bioimmagini di Napoli. Collabora con varie istruzioni pubbliche nazionali ed internazionali nel settore delle tecnologie biometriche. Dal 2002 è coordinatore del gruppo di lavoro 6 (WG 6 on "Cross-Jursidicational and Societal Aspects") del Sottocomitato ISO SC 37 "Biometrics".

Gian Mario Scanu. Giornalista pubblicista. Laureato nel 2006 in Scienze della Comunicazione, presso l'Università degli studi di Siena. Nel 2008 ha conseguito il Master di II livello presso l'Università di Pisa in Comunicazione pubblica e politica. Dal 2012 lavora all'Istituto di Informatica e Telematica del Cnr, dove si occupa, tra le altre cose, della comunicazione e divulgazione delle attività della Piattaforma Serit.

Roberto Setola. Direttore del Laboratorio Sistemi Complessi e Sicurezza dell'Università CAMPUS BioMedico di Roma. Direttore del Master universitario di secondo livello in "Homeland Security - sistemi, metodi e strumenti per la security ed il crisis management. Ha una esperienza decennale nel campo della Protezione delle Infrastrutture Critiche ed è il Segretario della AIIC - Associazione Italiana esperti Infrastrutture Critiche.

Paolo Maurizio Soave. Dirigente Medico U.O.C. Anestesia, Terapia Intensiva Postoperatoria e Terapia del Dolore e Consulente del Servizio di Tossicologia Clinica presso il Policlinico Universitario "A. Gemelli" di Roma. Membro del Gruppo Tecnico Difesa Civile istituito presso la Prefettura di Roma. Istruttore AHLS (Advanced Hazmat Life Support) e ALS (Advanced Life Support).

Francesco Soldovieri. Primo ricercatore presso l'Istituto per il Rilevamento Elettromagnetico dell'Ambiente del CNR ed è stato professore a contratto presso la Seconda Università di Napoli e l'Università Mediterranea di Reggio Calabria. Attualmente fa parte dell'Editorial Board delle IEEE Geoscience and Remote Sensing Letters e del Journal of Geophysics and Engineering, coordinatore

scientifico del progetto FP7 Integrated System for Transport Infrastructures surveillance and Monitoring by Electromagnetic Sensing (ISTIMES).

Marco Trussardi. Laureato nel 1996 in Ingegneria Elettronica presso l'Università di Roma- Tor Vergata. Responsabile Piano Tecnologico ed Osservatorio Tecnologico. Chair della Piattaforma Tecnologica Serit.

Mario Vento. Fellow della International Association for Pattern Recognition (IAPR). Attualmente è Professore Ordinario in Informatica e Intelligenza Artificiale presso l'Università di Salerno, dove è responsabile del gruppo di ricerca MIVIA. Dal 2002 al 2006 è stato Chair dello IAPR Technical Committee TC15 "Graph Based Representation in Pattern Recognition", e dal 2003 è Associate Editor della rivista "Electronic Letters on Computer Vision and Image Analysis". È autore di oltre 170 articoli scientifici su riviste e conferenze internazionali.

Giordano Vicoli. Laureato in Ingegneria Elettronica con specializzazione in informatica. Lavora presso l'ENEA come ricercatore nel campo della protezione delle Infrastrutture Critiche. E' ora responsabile ENEA del Progetto Europeo AFTER.

Giuseppe Viesti . Professore Ordinario di Fisica all' Università di Padova dove è presidente del Consiglio di Corso di Studi in Fisica. Attivo da 35 anni nel campo della Fisica Nucleare fondamentale ed applicata e della strumentazione. Membro della collaborazione ALICE al CERN. Coordinatore del progetto FP7 MODES_SNM nel campo della sicurezza nucleare.

Andrea Zappettini. Laureato in Fisica all'Università di Parma nel 1992. Nel 1997 ha conseguito il dottorato in Scienze dei Materiali e Tecnologie, sempre all'Università di Parma. Dal 1996 al 1998 ha lavorato presso Venezia Tecnologie (gruppo ENI). Dal 1996 al 2001 ha lavorato per Corecom (gruppo Pirelli) come capo del laboratorio di Materiali Fotonici. Dal 2001 è ricercatore all'IMEM-CNR. E' autore di oltre 110 pubblicazioni.

Maria Katiuscia Zedda. Dopo una laurea in Ingegneria Elettrica ed un Dottorato di Ricerca in Ingegneria Industriale è stata per svariati anni visiting reaseracher (in una posizione JOC) presso il Joint European Torus (Culham, Oxford, UK) per supporto all'attività sperimentale per i sistemi di controllo e protezione del reattore a fusione. Dal 2008 lavora presso Akhela dove è responsabile della pianificazione e del coordinamento dei progetti di ricerca. Nel 2011 è stata chiamata a fare il valutatore dell'FP7.

Per un errore di stampa è stato omesso il cv di un collaboratore:

Matteo Colantoni. Laureato in Ingegneria Informatica presso l'Università La Sapienza di Roma, lavora da circa 15 anni in multinazionali operanti nel settore dell'ICT e della Sicurezza, dove ha maturato significative esperienze in qualità prima di System Engineer e poi di Project Manager in progetti complessi; ha acquisito, negli ultimi anni, competenze di Business Development sui mercati internazionali e ricopre, attualmente, il ruolo di Project Manager per il cliente Telecom Italia (area Enterprise Portals). Possiede la certificazione PMI-PMP.

6. Progetti di Ricerca in ambito Sicurezza a cui partecipano i membri di SERIT

TA 1 – Sorveglianza e situazioni awareness

SUNNY	Smart UNmanned aerial vehicle sensor Network for detection of border crossing and illegal entrY

TA 2 – Comunicazione

AFTER	A Framework for electrical power systems vulnerabilità identification, defense and restoration
CockpitCI	Cybersecurity on SCADA: risk prediction, analysis and reaction tools for Critical Infrastructures
ISITEP	Inter System Interoperabiity for Tetra TetraPol Networks
WISEC	Sicurezza Radio: canale intrinsecamente nuovo

TA 3 - Detection & Identification System

SAMURAI	Suspicious and Abnormal behaviour Monitoring Using a netwoRk of cAmeras& sensors for sItuation awareness enhancement

TA 4 – Tecnologie per crisis management

DESTRIERO	A DEcision Support Tool for Reconstruction and recovery and for the IntEroperability of international Relief units in case Of complex crises situations, including CBRN contamination risks
PANDORA	Advanced Training Environment for Crisis Scenarios

TA 5 – Information, processing and management

ALARP	A railway automatic track warning system based on distributed personal mobile terminals
AMBER	Assessing, Measuring and BEnchmarking Resilience
ANIKETOS	Secure and Trustworthy Composite Services
CHESS	Composition with Guarantees for High integrity Embedded Software Components aSsembly
CONNECT	Emergent Connector for Eternal Software Intensive Networked Systems
CONTRAIL	Open Computing Infrastructure for Elastic services
CRUTIAL	Critical UTility InfrastructurAL Resilience
DEMONS	DEcentralized, cooperative, and privacy preserving MONitoring for trustworthiness Safe Port Operations using EGNOS SoL Service
DOTS - LCCI	Dependable Off The Shelf based middleware systems for Large scale Complex Critical Infrastructures
INSPIRE	INcreasing Security and Protection through infrastructure REsilience
MASSIF	MAnagement of Security information and events in Service InFrastructures
NESSoS	Network of Excellence on Engineering Secure Future Internet Software Services and Systems
SESAMO	Security and Safety Modeling

TA 6: CBRNE

CALYPSO	Calypso HF Radar Monitoring System and Response Against Marine Oil Spills in The Malta Channel
CBRNEmap	Road mapping study of CBRNE demonstrator
CISIA	Conoscenze integrate per sostenibilità e innovazione del “Made in Italy” agroalimentare
CONffiDENCE	Contaminants in food and feed: Inexpensive detection for control of exposure
DREAM	Design and development of REAlistic food Models with well characterised micro and macro structure and composition
EDEN	End user driven DEmo for cbrNe
ICT- E3	ICT per l’Eccellenza dei Territori
MODES_SNM	Modular Detection System for special nuclear material
MONIQA	Monitoring and quality assurance of food Network of excellence
RF- IZP- 2008 -1160478	Messa a punto di dispositivi nanotecnologici (biosensori) per il rilevamento di allergeni in alimenti di origine animale e vegetale
S.I.Mi.S.A.	Strumenti Innovativi per il Miglioramento della Sicurezza Alimentare: Prevenzione, Controllo, Correzione
SIASIC	Sorgenti inquinanti sommerse nei mari siciliani (Submerged pollutant sources in the Sicilian Seas)
SICMA	Simulation of Crisis Management Activities
SITCEN	Development of a prototype for the International Situational Centre on Interaction in Case of Ecoterrorism
TAWARA_RTM	TAp WAter RAdioactivity Real Time Monitor
Prodotti innovativi per il monitoraggio e la decontaminazione/detossificazione di agenti nervini ed esplosivi nell’ambiente e/o per la gestione delle emergenze	Prodotti innovativi per il monitoraggio e la decontaminazione/detossificazione di agenti nervini ed esplosivi nell’ambiente e/o per la gestione delle emergenze

TA 7: Aspetti legali ed etici della sicurezza

CIPRNet	Critical Infrastructure Protection Research Network

SG 4 – Sicurezza del trasporto su strada

Contratto di Ricerca tra Zeropiù Srl e l'IAC CNR	Contratto di Ricerca tra Zeropiù Srl e l'IAC CNR
HYCON2	Highly complex and networked control systems
Multipopulation Models for Vehicular Traffic and Pedestrians	Multipopulation Models for Vehicular Traffic and Pedestrians
PRIN 2009	Problemi iperbolici non lineari per le applicazioni

SG 5 – ICT per la sicurezza

SAWSOC	Situation Aware Security Operations Center

SG 7 – Sicurezza aeroportuale

Contratto di ricerca tra IAC Selex Sistemi Integrati Spa (2008 - 2010)	Contratto di ricerca tra IAC Selex Sistemi Integrati Spa (2008 - 2010)
GAMMA	Global AtM security Management

SG 9 – Sicurezza nel costruito

HARMONISE	A Holistic Approach to Resilience and Systematic Actions to Make Large Scale Urban Built Infrastructure Secure

SG 12 – Sicurezza agroalimentare

FOODNET	Studio di un nuovo sistema integrato, su piattaforma informatica, polifunzionale, di tecnologie per il trasporto di prodotti agro alimentari freschi
TRACEBACK	Integrated System for a reliable traceability of entire food supply chains

Altri progetti non catalogati nei TA/SG:

AMISS	Active and Passive Microwaves for Security and Subsurface imaging
ANVIL	Analysis of Civil Security Systems in Europe
APQTA	Attività di contrasto dei traffici illeciti di rifiuti
ASINFO	Architetture di sistema e Servizi integrati per l'Infomobilità
BONAS	BOmb factory detection by Networks of Advanced Sensors
CASHMA	Context Aware Security by Hierarchical Multilevel Architectures
CHIRON	Cyclic And Person Centric Health Management
CONTAIN	CONtainer securiTy Advanced Information Networking
CRESCENDO	Coordination action on Risks, Evolution of threatS and Context assessment by an Enlarged Network for an r&D rOadmap
CUSTOM	Drugs And PreCUrsor Sensing By ComplemenTing Low COst Multiple Techniques
DEFSEC	Study on industrial implications in Europe of the blurring of dividing lines between Security and Defence
eDIANA	Embedded Systems for Energy Efficient Buildings
EFFISEC	Efficient Integrated Security Checkpoints
eHealthMonitor	Intelligent Knowledge Platform for Personal Health Monitoring Services
E JRM	electronic Justice Relationship Management

ERNCIP	EU Reference Network for Critical Infrastructure Protection
ESETF	Explosives Security Experts Task Force
EUROCON	Study on State Control of Strategic Defence Assets
EU - US Security Strategies	EU – US Security Strategies
FACIES	Online identification of Failure and Attack on interdependent Critical Infrastruc-turES
FIDELITY	Fast and trustworthy Identity Delivery and check with ePassports leveraging Traveller privacy
FORLAB	Forensic laboratory
GEMOM	Genetic Message Oriented Secure Middleware
IMPULSO	Integrated Multimodal Platform for Urban and Extra Urban Logistic System Optimisation
ISOTREX	Integrated system for on line trace explosives detection in solid and vapour state
ISTIMES	Integrated System for Transport Infrastructures surveillance and Monitoring by Electromagnetic Sensing
LANDSCAPING	Landscaping Identifying the mismatch between requirements and planned capabilities: Air Operations
MEDUSE	Marine park Enhanced applications baseD on Use of integrated GNSS Ser-vices
MOS24	Motorways of the Sea 24
NDE	Network on Detection of Explosive

NECTC	Network Enabled Capabilitis Technical Challenges
n.S.HI.E.L.D.	New embedded Systems arcHItecturE for multi Layer Dependable solutions PERSEUS Protection of European Seas and borders through the intelligent use of surveillance
p.S.HI.E.L.D.	Pilot embedded Systems arcHItecturE for multi Layer Dependable solutions
PROTECTRAIL	The Railway Industry Partnership for Integrated Security of Rail Transport
RADEX	Raman Stand Off
REFIRE	REference implementation of interoperable indoor location & communication systems for FIrst Responders
SAFER	Sicurezza Attiva nei sistemi FERroviari
SAFEPORT	Safe Port Operations using EGNOS SoL Services
SANDERA	The future impact of defence and security on the European Research Area
SeaBILLA	Sea Border Surveillance
SecuFood	Security of the European Food Supply Chain
SecureMetro	Secure Metro
SIMOB	Sistema Integrato per l'infomobilità
SINTESIS	Sistema INTEgrato per la Sicurezza ad Intelligenza diStribuita
SIRIS	Progettazione e sviluppo sperimentale di una piattaforma di servizi di infomobilità e tracciamento per la raccolta e trasporto dei rifiuti speciali

SITMar	Sistema integrato per il trasporto marino
SITRAM	Sistema Trasporto Tranviario Innovativo
SLIMPORT	Sicurezza, Logistica, Intermodalità Portuale
SMART	Services for SMEs in collAborative tRansporT research projects
TECOM	Trusted Embedded Computing
THEVI2	Threat Vulnerability Path Identification for Critical Infrastructures Compilation of a comprehensive all hazards catalogue for critical infrastructure

Il vol. 2 di SEcurity Research in ITaly è stato finanziato dal progetto:

Si ringraziano Stefania Fabbri e Paolo Gentili per la collaborazione nella rilettura e correzione dei testi,
e Francesco Gianetti per la parte grafica

Tutte le immagini presenti nel libro sono state acquistate dalla banca dati www.thinkstockphotos.it

Finito di stampare a giugno 2012 a Cascina presso Stylgrafica Cascinese