2020

Ministero dello Sviluppo Economico

Volume LXIII

LA COMUNICAZIONE

Note Recensioni e Notizie

Pubblicazione della Direzione Generale per le Tecnologie delle Comunicazioni e la Sicurezza Informatica - Istituto Superiore delle Comunicazioni e delle Tecnologie dell'Informazione

SICUREZZA INFORMATICA - QUALITÀ DEI SERVIZI - COORDINAMENTO FREQUENZE
PIANIFICAZIONE E GESTIONE SPETTRO RADIO - SORVEGLIANZA MERCATO
APPARECCHIATURE RADIO - INTEROPERABILITÀ NUMERAZIONE - INTERNET GOVERNANCE
STANDARDIZZAZIONE - RICERCA IN TLC E ICT - SCUOLA SUPERIORE DI SPECIALIZZAZIONE TLC
AUTORITA' NIS, TELCO E PERIMETRO SICUREZZA CIBERNETICA NAZIONALE

DGTCSI ISCTI

In copertina

Il panfilo Elettra: il laboratorio galleggiante di Guglielmo Marconi.

All'interno del **Museo Storico della Comunicazione di Roma** *è stata ricostruita la cabina radiotelegrafica, all'interno della quale sono stati collocati gli apparati originali scampati miracolosamente agli eventi bellici. Nel 1943 infatti la nave fu requisita dalle forze armate tedesche e adattata a neve scorta. Nel 1944 fu affondata sulla costa jugoslava. Il relitto fu in seguito recuperato, a cura dell'Amministrazione delle Poste e Telegrafi. Sono esposti un radiotrasmettitore a onde medie delle officine Marconi di Genova, usato dallo scienziato sul panfilo Elettra, e il trasmettitore a onde corte da 2 kW, costruito a Londra dalla "Marconi" Wireless Telegraph Co. Ltd" in servizio presso la stazione radio italiana a grande potenza di Coltrano.*

Ministero dello Sviluppo Economico
Direzione Generale per le Tecnologie delle Comunicazioni e la Sicurezza Informatica - Istituto Superiore delle Comunicazioni e delle Tecnologie dell'Informazione

LA COMUNICAZIONE
Note Recensioni & Notizie

Pubblicazione della Direzione Generale per le Tecnologie delle Comunicazioni e la Sicurezza Informatica - Istituto Superiore delle Comunicazioni e delle Tecnologie dell'Informazione

Numero Unico Anno 2020
Vol. LXIII

Direttore: Dott.ssa Eva Spina

Hanno collaborato per la redazione di questo numero:

Eva Maria Alfieri, Andrea Ferraris, Marcella Graziosi

Luciana Favia *per l'usabilità del documento*

Corrado Pisano *per il sito web*

Coordinamento, supporto tecnico e grafica:

Ing. Fabrizio Zanuccoli

Si ringraziano gli Autori degli articoli e i componenti del Comitato di Revisione della rivista che hanno contribuito alla realizzazione di questo numero.
L'immagine di copertina è stata gentilmente messa a disposizione dal Museo Storico della Comunicazione di Roma del Ministero dello Sviluppo Economico:
http://cultura.mise.gov.it/museoPPTT_fe/index.do

La Comunicazione - Note, Recensioni & Notizie è la rivista "storica" dal 1952 di informazione scientifica edita dalla DGTCSI - ISCTI (Areta Tecnica Comunicazioni), e ha lo scopo di documentare lo sviluppo del settore della Comunicazione Elettronica, attraverso le sue rubriche di "Note" (contenenti esperienze, studi, ricerche e tutte quelle informazioni di taglio prettamente tecnico-scientifico), di "Recensioni" (di libri, testi, trattati, ecc.) ed infine di "Notizie" (brevi resoconti d'attualità relativi ad incontri, conferenze, seminari, attività di ricerca, ecc.).

Sommario

Introduzione del Direttore

Il 2020 è stato un anno segnato indiscutibilmente dalla pandemia del Covid19. Le abitudini della vita quotidiana e le modalità lavorative e di studio hanno subito modifiche sostanziali, con un vasto ricorso agli strumenti e ai servizi digitali. Ciò ha attribuito, come immediata conseguenza, un ruolo ed una rilevanza primaria alla sicurezza cibernetica.

La Rivista La Comunicazione – Note, recensioni, notizie concentra pertanto l'attenzione nel numero del 2020 su vari aspetti della sicurezza informatica, dalle metodologie del *risk assessment* alle analisi per le vulnerabilità degli hardware e alla gestione delle informazioni, dalla sicurezza quantistica fino alla correlazione tra Intelligenza Artificiale e diagnosi del Covid 19.

La linea editoriale ha inteso quindi approfondire aree di analisi e temi innovativi collegando la ricerca scientifica ad argomenti di stretta attualità, supportando la diffusione del lavoro di giovani studiosi ed esperti.

L'edizione del 2020 consente altresì di esaminare gli esiti di una sperimentazione, compiuta all'interno dei laboratori della DGTCSI – ISCTI, sugli effetti dei segnali del radiomobile in una delle bande pioniere per il 5G sugli impianti TV riceventi i segnali del digitale terrestre di seconda generazione nella banda adiacente, in considerazione del prossimo *refarming* delle frequenze attualmente ad uso *broadcasting* ai servizi mobili in banda larga.

Nel ringraziare la redazione per il lavoro e la professionalità dimostrata, La Comunicazione, nell'edizione 2020, si propone come strumento di divulgazione scientifica, attuale e aggiornata, per approfondire gli studi in essere su temi sfidanti e delineare le prospettive future che ci offre la tecnologia.

Dott.ssa Eva Spina

Direttore della
Direzione Generale per le Tecnologie delle Comunicazioni
e la Sicurezza Informatica - Istituto Superiore delle
Comunicazioni e delle Tecnologie dell'Informazione

Sicurezza Quantistica: L'uso delle Quantum Key Distribution su scala nazionale

Quantum Security: The use of Quantum Key Distributions on a national scale.

Francesco Matera ♦

♦ *Fondazione Ugo Bordoni*

Sommario

Questo articolo descrive uno studio sull'introduzione di sistemi di trasmissione che possiedono una gestione della sicurezza basata sulla meccanica quantistica, mediante le *Quantum Key Distribution (QKD),* nelle infrastrutture di telecomunicazione in fibra ottica già esistenti. In particolare, sono analizzate le soluzioni e le prestazioni in ciascun segmento di rete per definire percorsi fisici end-to-end QKD, da sorgente a destinazione, e compatibili con il concetto di partizione della rete, detto *slicing,* definito nelle architetture delle nuove reti 5G. E' riportata una analisi dei costi per l'introduzione delle QKD in ogni segmento di rete con particolari dettagli per i costi necessari per una rete di telecomunicazione italiana, sicura dal punto di vista quantistico.

Abstract

This article describes a study on the introduction of transmission links that have a security management based on quantum mechanics, through Quantum Key Distribution (QKD), in existing fibre optic telecommunication infrastructures. In particular, the solutions and performances in each network segment are analysed to define end-to-end QKD physical paths from source to destination, and compatible with the concept of network partition, called slicing, defined in the architectures of the new 5G networks. An analysis of the costs for the introduction of QKDs in each network segment is reported with particular details for an Italian telecommunications network, secure from a quantum point of view.

Keywords: QKD, WDM, Access, FSO, 5G, slicing

1. Introduzione

Le tecniche quantistiche stanno uscendo dai laboratori per essere utilizzate in diversi contesti, e in termini di sicurezza il quantum computing potrebbe rendere obsoleti gli attuali algoritmi crittografici, mettendo a rischio la protezione dei dati e delle comunicazioni. Questo aspetto sta portando ad un'accelerazione per l'adozione di contromisure, soprattutto per proteggere dati e infrastrutture critiche. Oggi, è ampiamente riconosciuto che è fondamentale iniziare a pensare ad infrastrutture di sicurezza a prova di futuro e sviluppare un piano di gestione del rischio basato su un approccio quantistico il prima possibile.

Va sottolineato che nel campo degli studi sull'uso degli effetti quantistici nei dispositivi per la commutazione l'Istituto Superiore delle Tecnologie delle Comunicazioni e dell'Informazione, ora Direzione Generale per le tecnologie delle comunicazioni e la sicurezza informatica - Istituto superiore delle comunicazioni e delle tecnologie dell'informazione (DGTCSI - ISCTI), è stato uno dei primi centri di ricerca che già più di trenta anni fa, in collaborazione con la Fondazione Ugo Bordoni, aveva sperimentato specifiche tecniche come mostrato nel lavoro [1] che riguardava il trasferimento del momento angolare.

Attualmente, le Quantum Key Distribution (QKD) sono riconosciute come una delle più importanti metodologie di comunicazione quantistica sicura [2-5] e adottano un canale fotonico per crittografare le informazioni attraverso i principi della meccanica quantistica. I sistemi QKD sono già operativi in diversi contesti, permettendo anche collegamenti su lunghe distanze in configurazioni Point to Point (P2P) [6-10].

Inoltre, è stata ampiamente dimostrata la possibilità di far coesistere nella stessa fibra ottica canali quantistici e canali classici, mostrando così la possibilità di realizzare reti ibride senza la necessità di installare nuove fibre [11-14]. Tuttavia, rispetto ai sistemi classici devono essere prese alcune precauzioni, a cominciare dalla necessità di sostituire gli amplificatori ottici per la compensazione delle perdite nelle fibre ottiche, in quanto nel caso dei canali quantistici il rumore ASE, emesso da tali amplificatori, avrebbe un effetto devastante, e, al momento, deve ancora essere dimostrata la possibilità di adottare ripetitori quantistici in reti QKD [4]. Fortunatamente, la trasmissione di informazioni quantistiche sicure su lunga distanza può essere ottenuta suddividendo la tratta complessiva in segmenti, ognuno gestito con un apparato QKD, realizzando così dei nodi intermedi denominati Trusted Repeater Nodes (TRN) [3-4]. I TRN possono essere situati negli stessi luoghi degli amplificatori ottici, ed è infatti questa la soluzione adottata ad esempio nel collegamento tra Pechino e Shanghai [3].

Oggi i sistemi QKD operano anche nel segmento delle reti di acceso, in collegamenti Point-to-Point (P2P), ma anche in architetture Gigabit Passive Optical Networks (GPON) [15], in collegamenti ottici nello spazio libero (Free Space Optical communication, FSO) [16] e recentemente anche in fibre multimode e multicore [17].

Tuttavia, per la loro completa introduzione, in tutta la rete di telecomunicazioni, dall'area di accesso a quella core, sono ancora necessari diversi passaggi tecnologici. Nonostante queste

difficoltà, ci sono già molte proposte per includere le tecniche QKD in vaste aree geografiche arrivando a gestire le risorse di tipo quantistiche [18], adottando approcci di Software Defining Network (SDN) [19-20] e operando con partizioni di tipo slice definite nel contesto delle reti 5G [21-22].

In questo articolo, per ogni segmento di rete, sono descritte le problematiche tecniche associate con l'adozione di una sicurezza quantistica basata su QKD al fine di poter definire percorsi QKD end-to-end che, compatibilmente con le nuove architetture sviluppate per le infrastrutture 5G, possano essere etichettati come una sorta di Quantum Slice. Il principale obiettivo di questo lavoro è l'analisi dei costi che sarebbe necessario sostenere per introdurre, in una rete che copra le principali città di un Paese come l'Italia sfruttando le infrastrutture già esistenti, un set minimo di dispositivi QKD per attuare un approccio di sicurezza quantistica.

2. Breve panoramica sulle QKD operanti nelle reti esistenti.

Sperimentazioni in tutto il mondo confermano l'efficacia della crittografia quantistica; tra questi possono essere citati gli esempi di Vienna [6], Tokyo [7], Firenze [8], Cambridge [9], nonché di particolare rilevanza il caso cinese tra Pechino e Shanghai [3]. Inoltre, la regolamentazione su QKD è studiata negli organismi ITU ed ETSI (ETSI ISG-QKD) ed un grande interesse per questa tecnologia è anche mostrato dalle Telco con le iniziative nel 3GPP per le reti 5G [22]. Le QKD sfruttano un canale quantistico solo per produrre e distribuire chiavi per crittografare (e de-crittografare) un messaggio scambiato su un canale classico di comunicazione [2].

Le basi ed i protocolli di questa procedura di sicurezza si possono trovare in letteratura [4] e come riferimento il protocollo più noto è quello BB84. Nonostante il notevole interesse su questo tema, è ancora presente un certo scetticismo principalmente perché questi sistemi funzionano con potenze molto basse, e quindi qualsiasi fonte di perdite e/o di rumore (classico e quantistico) degrada fortemente le loro prestazioni: come conseguenza il bit rate consentito dalle QKD per la trasmissione della chiave (key rate) è estremamente inferiore ai tradizionali sistemi di trasmissione ottica. In pratica, partendo dalla generazione di una sequenza di impulsi, solo un numero estremamente limitato di essi può essere effettivamente utilizzato per la trasmissione QKD, con una key rate che risulta essere molto inferiore alla frequenza degli impulsi generati e che si abbassa sempre di più all'aumentare delle perdite subite durante il percorso del segnale [3-5]. Inoltre, sono necessari diversi minuti prima che la sincronizzazione possa consentire al sistema QKD di funzionare nelle migliori condizioni [16]. Molti sforzi sono ancora necessari per aumentare la key rate, ma anche la massima distanza di propagazione, e quindi rendere i sistemi QKD economici, compatti e robusti.

I sistemi QKD possono coesistere con un intenso traffico dati nella stessa fibra [9-13], tramite la tecnologia Wavelength Division Multiplexing (WDM), eliminando così la necessità di usare fibre dedicate, non solo costose ma spesso anche non disponibili. Pertanto, il backbone QKD-over-WDM è diventato una soluzione promettente e fattibile per le future reti quantistiche. Attualmente si suppone che una trasmissione WDM quantistica adotti tre diversi

tipi di canali [17]: il *Measuring Base Channel* (MBCh), il *Traditional Data Channel* (TDCh) e il *Quantum Key Channel* (QKCh). In particolare, l'MBCh è il canale pubblico che trasmette segnali classici ed ha il compito di trasportare la sequenza della base di misurazione selezionata e le informazioni per la correzione degli errori, il QKCh è il canale che trasmette i segnali quantistici ed i TDCh sono i classici canali che trasportano l'informazione ad alto bit rate.

Occorre comunque sottolineare che devono essere prese delle importanti precauzioni per la coesistenza tra canali quantistici e canali classici, anche per limitare le degradazioni dovute agli effetti non lineari della fibra; in particolare, lo scattering Raman [22] e gli effetti di missaggio a quattro onde (FWM) [4] indotti da MBCh e TDCh, che possono degradare le prestazioni nella trasmissione del QKCh.

I canali quantistici devono essere conformi ad un sistema DWDM commerciale, ad es. 40 lunghezze d'onda (con spaziatura dei canali a 100 GHz) o 80 lunghezze d'onda (con spaziatura dei canali a 50 GHz). Pertanto, il problema dell'allocazione della lunghezza d'onda per i tre tipi di canali deve essere considerato nelle reti ottiche abilitate al QKD. In alcuni lavori, per ottenere un isolamento appropriato dalla comunicazione dei dati, si alloca il QKCh nella banda O (1260–1360 nm) [17], mentre, nei sistemi DWDM commerciali, il TDCh si trova solitamente nella banda C (1530–1565 nm). Tuttavia, occorre osservare che nella banda O ci sono livelli di perdite più alti rispetto alla banda C, il che limita la velocità di trasmissione e la massima distanza raggiungibile. Di conseguenza, i tre canali possono essere allocati in banda C per garantire le migliori prestazioni di trasmissione. Inoltre, il posizionamento del QKCh in banda C può limitare gli effetti dovuti allo scattering Raman [22]. Pertanto, le lunghezze d'onda assegnabili per i QKCh possono iniziare da 1530 nm, e inoltre una spaziatura di 200 GHz può essere adottata come banda di guardia tra QKCh e gli altri canali classici per ridurre al minimo gli effetti di miscelazione a quattro onde (FWM). Il MBCh, che trasporta i segnali classici per la conferma della chiave segreta utilizzata, può condividere lunghezze d'onda nella banda C [16].

Per i collegamenti su lunga distanza con tecnologia QKD sarebbe necessario una sorta di ripetitore quantistico. Sfortunatamente i ripetitori quantistici non sono ancora fattibili con l'attuale tecnologia ed, al momento, una soluzione interessante per trasmettere segnali QKD su lunghe e lunghissime distanze si basa sull'introduzione di ripetitori che gestiscono i QKD come sistemi indipendenti [3], mentre MBch e TDCh sono otticamente amplificati da EDFA.

Diverse architetture di reti di accesso, basate sulla propagazione ottica, possono sfruttare le proprietà delle QKD ed in questo contesto le reti GPON appaiono molto attraenti, anche se le perdite dovute allo splitter riducono il numero di utenti QKD [14]. *QKD over FSO* [15] è un altro modo per sfruttare la propagazione ottica per la sicurezza quantistica evitando l'installazione della fibra; questo approccio risulta quindi essere molto interessante per l'introduzione del QKD sia nel segmento di accesso sia per il backhauling, e.g.: per connettere le terminazioni di apparati radio con le BaseBand Unit (BBU). Tornando al segmento core, sarà fondamentale la gestione delle varie lunghezze d'onda con l'ottimizzazione dello spettro

WDM come mostrato ad esempio in [17-18]. Nonostante gli aspetti complessi sopra citati, l'importanza di queste tecnologie è testimoniata anche dall'interesse ad essere incluse nelle nuove architetture e gestioni di rete basate sulle Software Defined Networking (SDN) come descritto ad esempio in [19-21]. Ad esempio, è dimostrato [16] che il monitoraggio in tempo reale dei parametri quantistici fornisce informazioni al controller SDN per proteggere i percorsi della luce nella rete ottica, con configurazioni dei percorsi ottici flessibili per garantire la distribuzione delle chiavi quantistiche anche in caso di attacchi. Inoltre, l'uso di QKD nel contesto delle Network Function Virtualization (NFV) è stato anche studiato con diverse dimostrazioni per verificare l'applicazione di approcci di crittografia utilizzando chiavi quantistiche per rendere sicure alcune funzioni NFV [18]. Sulla base dei progressi ottenuti sulle tecnologie QKD e sulla loro applicazione principalmente nei contesti relativi alle soluzioni SDN e NFV, l'uso di QKD sembrerebbe avere ora un ruolo molto importante anche per realizzare interconnessioni sicure all'interno del framework 5G [22].

3. Infrastrutture di reti basate su QKD

Seguendo le considerazioni descritte nella Sez. 2, e facendo riferimento al lavoro [23], la Fig. 1 illustra un esempio di rete completa che utilizza sistemi QKD sia nelle componenti di core sia in quelle di accesso (comprensive anche dei raccordi verso le antenne di accesso radio). Nell'area core (area gialla), ciascun nodo finale è costituito da un Quantum Backbone Node (QBN), equipaggiato con un ricevitore e trasmettitore QKD [4], che può funzionare sia come sorgente sia come destinazione; lungo il collegamento, che può essere anche di centinaia di km, un nodo di transito può operare come Trusted Repeater (TR) e ogni TR ha un trasmettitore e un ricevitore QKD. Per consentire ai canali QKCh, MBCh e TDCh di coesistere nella stessa fibra, nella fig. 1 è considerato uno schema di bypass EDFA che consente al QKCh di non passare attraverso gli EDFA, utilizzando speciali componenti come multiplexer e demultiplexer per separare il canale QKCh dai canali MBCh e TDCh, il che risulta necessario per evitare il rumore ASE degli EDFA.

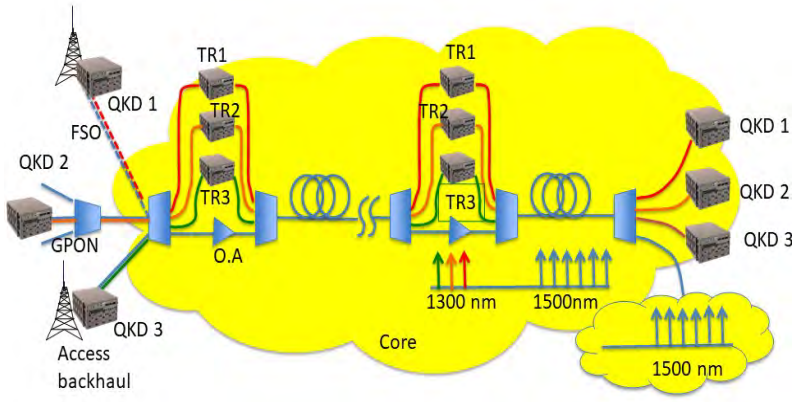

Figura 1 - *Esempio di una rete completa che utilizza le QKD. [23].*

Nell'area core si ipotizzano collegamenti costituiti da N tratte in fibra ottica lunghe 80 km che collegano i nodi di transito. Il core è collegato sia ai terminali QKD sia alle infrastrutture di accesso/backhaul/ fronthaul, dove possono essere localizzati terminali QKD, sfruttando specifici canali ottici da adottare per la trasmissione quantistica, ed utilizzando sia fibre ottiche dedicate, sia canali WDM in infrastrutture in fibra condivisa come nel caso delle reti GPON o dei collegamenti FSO. I canali quantistici possono essere usati anche in fibre Multimodo e Multicore [17].

Come esempio tipico consideriamo il caso di fibre ottiche operanti a 1550 nm, in cui le perdite sono di circa 0,2 dB/ km; ricordando che i sistemi QKD possono funzionare con perdite massime fino a 30 dB [4] significa che il limite pratico per la massima distanza è di circa 150 km . Tuttavia, andare a questa distanza comporta anche un output con un key rate fortemente ridotto. Dai risultati riportati in [4-5] si può affermare che due sono i regimi di propagazione che si possono adottare per i QKCh, assumendo una lunghezza della fibra di 80 km; infatti oltre alla lunghezza d'onda a 1550 nm (banda C), in cui si può operare con un key rate di 0,5 Mb/s, si può utilizzare anche la banda a 1300 nm (banda O), che presenta però una attenuazione più alta, e come conseguenza un più basso key rate pari a 0,25 Mb/s. Per il segmento di accesso, nel caso di infrastrutture GPON la limitazione principale è data dalla "splitting loss" e quindi, nel caso di 32 ONU, la key rate può essere dell'ordine di 0,5 Mb/s [14]. Dettagli specifici per i canali quantistici nelle infrastrutture GPON, anche per limitare le perdite dovute allo splitter, possono essere trovati in [14]. Un key rate più elevato potrebbe essere ottenuto nei collegamenti P2P e nelle soluzioni FSO a causa delle minori distanze in gioco. Ipotizzando di operare con percorsi slice a partire dal segmento di accesso/backhaul, e attraversando l'intera rete core, la velocità massima deve essere fissata a 0,25 Mb/s e 0,5 Mb/s rispettivamente per le bande O e C.

4. Analisi dei costi per sistemi QKD nelle reti attuali

Scopo di questo paragrafo è fornire alcune informazioni sui costi per l'introduzione di un approccio sulla sicurezza basato sulle QKD nelle reti attuali, anche se i dati disponibili sui costi dei dispositivi sono molto pochi e l'unico riferimento completo è riportato nella tabella 1 di [4] e solo per reti dorsali. L'introduzione dei canali QKD nei collegamenti WDM richiede costi aggiuntivi piuttosto elevati a causa, oltre che di apparati QKD, anche per l'introduzione di ulteriori dispositivi come i filtri ottici [4]. Con riferimento alla fig. 1, per ogni collegamento QKD punto-punto il costo aggiuntivo è composto dai seguenti quattro principali contributi: C_Q è il costo relativo ai ricetrasmettitori QKD supposti uguali in tutti i nodi della rete (che operano come sorgente e destinazione), C_B è il costo legato alle apparecchiature ausiliarie per gli apparati sorgente e destinazione e C_T è il costo per le apparecchiature ausiliarie relative ad ogni TRN; inoltre è incluso anche un costo C_W per l'occupazione spettrale del canale QKD nel collegamento WDM.

Seguendo la tabella dei costi di [4] e assumendo valori medi, sono state considerate le seguenti assunzioni per i costi: C_Q = 25k €, C_B = 20k €, C_T = 12,5k € e C_W = 6,5 €/km. Il costo totale per un collegamento QKD nell'area core è quindi [4]:

$$C_T = C_Q N_a + C_B N_B + C_T N'_a + C_W L_a \quad (1)$$

dove N_a è il numero totale di ricetrasmettitori QKD, N_B è il numero totale di nodi endpoint, N'_a è il numero totale dei TR e L_a è la lunghezza totale del collegamento. Analizzando i costi relativi alle reti di accesso (anche per raggiungere apparati BBU), il contributo principale è dovuto al trasmettitore e al ricevitore nel caso di soluzioni P2P e FSO, mentre nel caso di soluzioni PON, dobbiamo distinguere se l'infrastruttura di riferimento è GPON o WDM-PON, poiché la soluzione WDM-PON ha già i filtri richiesti che devono essere invece aggiunti nella GPON. In moderni sistemi WDM-PON, la funzione di demultiplexing può essere realizzata da un reticolo a guida d'onda (WGR) [24] che, come riportato in [24], ha un costo di circa 20k € per un WGR 32x. Per quanto riguarda l'FSO, si può considerare un costo inferiore per l'infrastruttura senza fibra ottica, grazie a un apparato end-to-end più semplice.

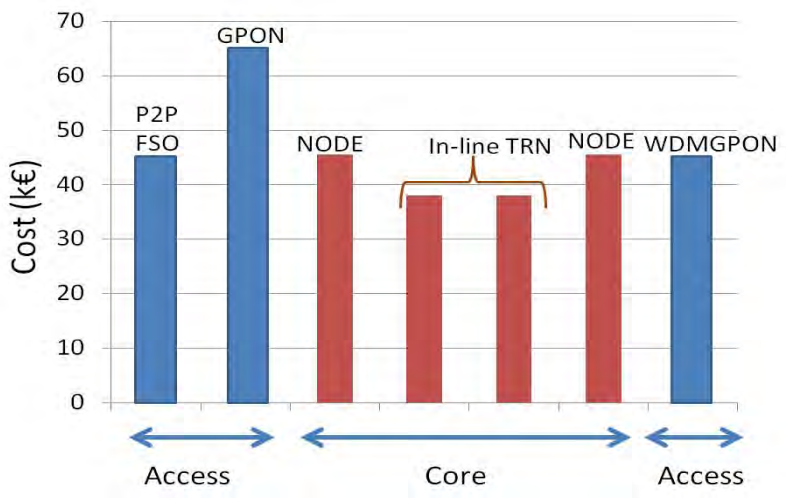

Figura 2 - *I costi in ciascun segment della rete*

Nella fig. 2, per ogni segmento di rete, è illustrato il dettaglio dei costi tipici per l'introduzione delle QKD in un ambiente End-to-End (E2E). Da ciò deriva che un collegamento QKD E2E lungo 800 km, compresi gli accessi P2P, richiede un costo aggiuntivo di circa 561k €, che è piuttosto elevato, ma va confrontato con il costo di un apparato ottico classico (e.g.: lo switch ottico 128x128 con porte da 10 Gb/s ha un costo di circa 500k € con 41k € per l'interfaccia da 10 Gb/s) [25].

5. Un esempio per l'introduzione delle QKD in Italia.

Come esempio, per l'introduzione di un approccio di sicurezza QKD in una rete nazionale completa, si ipotizza il caso Italia supponendo di considerare un numero di nodi pari a 17, rappresentativi delle principali città, con i 16 link riportati nel riquadro di fig. 3 (parte sinistra). Nella figura 3 (parte destra), le barre blu riportano i costi totali di ogni collegamento. Il risultato principale di tale analisi è che per realizzare una connessione sicura quantistica completa relativa all'Italia basata sulla topologia illustrata in fig. 3 è necessario un investimento di circa 3M€.

Figura 3 - *Collegamenti tra le principali città italiane in cui si suppone l'introduzione di sistemi QKD. A sinistra i collegamenti sono numerati da 1 a 16. A destra i relativi costi complessivi degli apparati QKD per ciascun link.*

Tuttavia, per avere una comunicazione QKD efficace tra tutti i nodi della rete italiana è necessaria un'architettura che tenga conto di tutte le possibili richieste QKD da qualsiasi sorgente a qualsiasi destinazione, e ciò significa avere molti più collegamenti QKD tra nodi che possono essere anche molto distanti l'uno dall'altro.

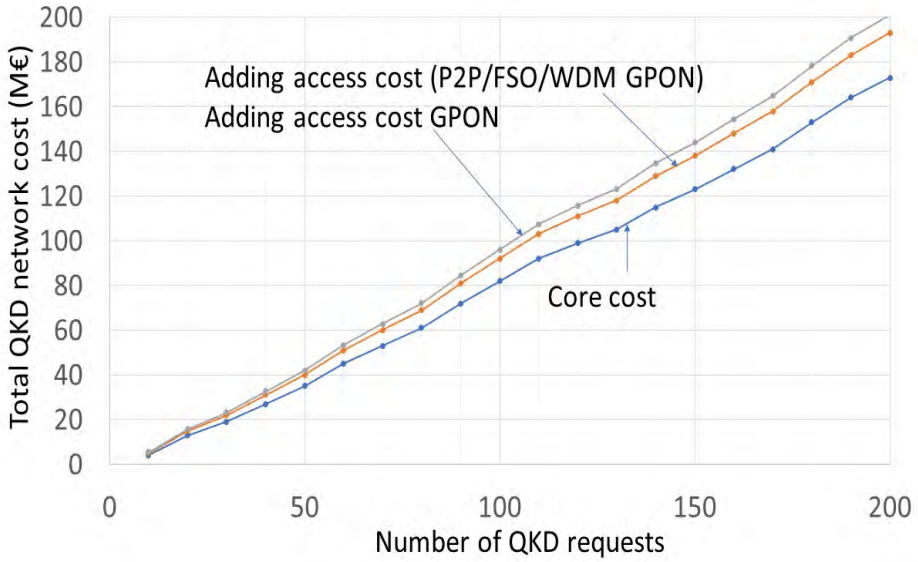

Figura 4 - *Costi totali per una rete QKD italiana in funzione delle richieste per connessioni QKD tra i diversi nodi*

Per avere un'idea degli investimenti necessari per supportare tutte le diverse richieste QKD, che possono venire dai 17 nodi, è stata effettuata un'analisi dei costi calcolando il valore di ogni collegamento tra due nodi scelti casualmente tra quelli riportati in fig. 3, e ipotizzando richieste QKD che vanno da 10 a 200 come riportato in fig. 4. Tale intervallo è stato scelto poiché in questa rete con V = 17 nodi, tutte le connessioni possibili sono V * (V-1) / 2 = 136, inclusi alcuni collegamenti molto lunghi. Inoltre, alcune coppie di nodi, per origine e destinazione, potrebbero richiedere più connessioni QKD o key rate più elevati, che è anche equivalente a più lunghezze d'onda QKCh. I percorsi tra i nodi sono calcolati dall'algoritmo del percorso più breve di Dijkstra [4] e applicando la relazione 1 si valutano i costi complessivi come riportato in fig. 4 distinguendo i casi della sola rete core e quelli comprendenti i costi aggiuntivi per la parte di accesso supponendo sia l'accesso basato su P2P/FSO/WDM-GPON sia l'accesso su GPON. L'aumento dei costi è pressoché lineare con alcune piccole variazioni di pendenza dovute principalmente alla diversa lunghezza del collegamento preso in considerazione. Tali costi potrebbero anche essere ridotti introducendo alcune strategie nella scelta dei percorsi come descritto in [4] per condividere alcune risorse di rete.

6. Conclusioni

Questo lavoro ha riportato uno studio sulla fattibilità di una rete operante con un approccio di sicurezza basato sulla tecnologia QKD, collegando le principali città d'Italia, e includendo anche il segmento di accesso fino all'antenna radio e consentendo di definire dei percorsi *slice* di tipo quantistico per essere gestiti in un framework 5G. I risultati mostrano la necessità di

ampi investimenti che, però, rientrano in quelli necessari per la realizzazione di nuove reti. E' anche vero che questo passo appare necessario visto ciò che stanno facendo altri Paesi nei prossimi anni sui temi della sicurezza quantistica.

Ringraziamenti.

Si ringrazia la Direzione Generale per le tecnologie delle comunicazioni e la sicurezza informatica - Istituto superiore delle comunicazioni e delle tecnologie dell'informazione (DGTCSI - ISCTI) per il supporto a questa attività e la Dott.ssa Marina Settembre per il supporto teorico sulle tematiche quantistiche e sulla sicurezza nelle reti.

Riferimenti bibliografici

[1] A. Santamato, M. Settembre, M. Romagnoli, B. Daino, Y. Shen, "Self-Induced Stimulated Light Scattering" Physical Review Letters vol. 61, 113 (1988).
[2] E. Diamanti et al, Nature Partner Journal **2**, 16025 (2016)
[3] Q. Zhang, F.Xu, Y. Chen, C. Peng, J. Pan, Optics Express **26**, (2018).
[4] Y. Cao et al, J. Opt. Comm. Netw. 285-298 **11** (2019).
[5] P. Eraerds, et al, New J. Phys., **12** 063027 (2010)
[6] M. Peev et al.," New J. Physics, **11**, (2009)
[7] M. Sasaki et al., Opt. Express **19**, 10 387 (2011)
[8] D. Bacco et al., EPG Quantum Technology (2019)
[9] A. Wonfor et al, Int. Conf. Quantum Cryptography, 1–3 (2017).
[10] T. A. Eriksson et al., Commun. Physics **2**, (2019)
[11] R. Lin et al, in Proc. ECOC 2018
[12] L. J. Wang, et al, Appl. Phys. Lett., **106**, 081108 (2015)
[13] N. A. Peters, et al, New J. Phys., **11**, (2009)
[14] S. Aleksic , et al, 18th NOC-OC&I (2013).
[15] P. V. Trinh , et al IEEE Access **6,** 4159-4175 (2018)
[16] E. Hugues-Salas, et al, J. Opt. Commun. Netw. **11**, A209–A218 (2019)
[17] Y. Cao, et al, J. of Opt. Comm. and Networking **9**, 995-1004 (2017).
[18] Y. Zhao et al., IEEE Commun. Mag. **56**, 130–137 (2018)
[19] A. Aguado et al, J. Lightw. Technol., **35**, 1357–1362 (2017)
[20] R. Wang et al , J. Lightw. Technol. **38**, 139-140 (2020)
[21] Jin Cao , et al , IEEE Communication & Tutorials, **22**, 170-195 (2020),
[22] H. Kawahara, A. Medhipour, and K. Inoue, Opt. Commun., **284**, 691–696 (2011).
[23] F. Matera, "Quantum Key Distribution in Optical Networks" IEEE ICOP 2020.
[24] G. Maier et al J. of Lightwave Techn., **18**, 125-143 (2000)
[25] S. Sengupta et al IEEE Commun. Mag. **41**, 60-70 (2003).

Intelligenza Artificiale e diagnosi precoce del COVID-19

Artificial Intelligence and early diagnosis of COVID-19

Agostino Giorgio♦

♦ *Dipartimento di Ingegneria Elettrica e dell'Informazione – Politecnico di Bari*

Sommario

Con il dilagare della pandemia da COVID-19 la comunità scientifica si è attivata tempestivamente innanzitutto per sequenziare il virus e, quindi, per cercare cure adeguate e vaccini, ora finalmente disponibili, per la prevenzione della malattia. Infatti, la sequenza del nuovo virus fu pubblicata già dai cinesi ad inizio pandemia e per questo la diagnosi è apparsa subito di facile pronuncia con la tecnica dei tamponi naso-faringei, dei test sierologici e antigenici, delle radiografie toraciche, metodologie tutte già ben note alla comunità scientifica. In assenza di sequenziamento la diagnosi sarebbe stata più difficile. Infatti, nella gran parte delle pandemie del passato l'agente patogeno era sconosciuto mentre nel caso del COVID-19 il sequenziamento del virus ha consentito di partire da una identità genetica ben precisa. Ciò ha permesso poi il rapido sviluppo dei vaccini con nuove tecnologie come quella del mRNA, o RNA messaggero. Per questo motivo diagnosi e prevenzione vaccinale sono strettamente legate. Tuttavia, ciò che sembra meno sviluppato attualmente sono metodi per la diagnosi precoce della malattia che sarebbero utili soprattutto per prevenire o curare ai primi sintomi la polmonite interstiziale che è la causa principale dei ricoveri in terapia intensiva e dei decessi. Obiettivo di questo lavoro è mostrare come ci siano tecnologie tipicamente utilizzate in elettronica per l'acquisizione ed elaborazione di dati, specialmente di immagini, con particolare riferimento ad algoritmi di intelligenza artificiale (IA), nota anche come Deep Learning (DL) e Machine Learning (ML), che potrebbero permettere una diagnosi assai precoce dell'insorgere della polmonite interstiziale da COVID-19 e non solo. A tale scopo, almeno per un primo screening, potrebbe essere anche sufficiente l'utilizzo di smartphone di media capacità, senza necessità di ricorrere a costosa strumentazione medica ed esami diagnostici generalmente proibitivi per tempi di attesa e molto onerosi. Pur nella consapevolezza che sono sempre più gli scienziati ed i gruppi di ricerca che utilizzano strumenti di IA per la diagnosi medica del COVID-19 e non solo, l'obiettivo del presente lavoro non è quello di presentare un'analisi critica e/o descrittiva delle attività in corso di svolgimento da parte della comunità scientifica bensì quello di presentare gli strumenti ingegneristici alla base delle attività dei vari gruppi di ricerca con strumenti di IA. Pertanto, vedremo innanzitutto come sia possibile diagnosticare precocemente l'insorgere della polmonite interstiziale; successivamente faremo una panoramica comparativa, qualitativa e quantitativa, dei metodi algoritmici utili allo scopo; infine, vedremo come uno smartphone possa essere utile come strumento per la diagnosi precoce.

Abstract

With the spread of the COVID-19 pandemic, the scientific community took prompt action, first of all to sequence the virus and, therefore, to seek adequate treatments and vaccines, now finally available, for the prevention of the disease. In fact, the sequence of the new virus was already published by the Chinese at the beginning of the pandemic and for this reason the diagnosis immediately appeared to be easy to pronounce with the technique of nasopharyngeal swabs, serological and antigenic tests, chest radiographs, all methods already well known. to the scientific community. Without sequencing, diagnosis would have been more difficult. In fact, in most of the pandemics of the past the pathogen was unknown while in the case of COVID-19, the sequencing of the virus made it possible to start from a very specific genetic identity. This then allowed the rapid development of vaccines with new technologies such as mRNA, or messenger RNA. For this reason, vaccination diagnosis and prevention are closely linked. However, what seems less developed at present are methods for early diagnosis of the disease which would be useful especially when it is becoming more complicated towards interstitial pneumonia which is the main cause of ICU admissions and deaths. The aim of this work is to show how there are technologies typically used in electronics for the acquisition and processing of data, especially images, with particular reference to artificial intelligence (AI) algorithms, also known as Deep Learning (DL) and Machine Learning. (ML), which could allow a very early diagnosis of the onset of COVID-19 interstitial pneumonia and more. For this purpose, at least for a first screening, the use of medium-capacity smartphones may also be sufficient, without the need to resort to expensive medical equipment and diagnostic tests that are generally prohibitive for waiting times and very onerous. Despite the awareness that more and more scientists and research groups are using AI tools for the medical diagnosis of COVID-19 and beyond, the aim of this work is not to present a critical and / or descriptive analysis of the activities in progress by the scientific community but to present the engineering tools underlying the activities of the various research groups with AI tools. Therefore, we will first see how it is possible from a medical point of view to diagnose the onset of interstitial pneumonia early; subsequently we will make an overview of the algorithmic methods useful for this purpose; finally, we will see how a smartphone can be useful as a tool for early diagnosis.

1. Introduzione

I polmoni (fig. 1) sono i due organi preposti alla fornitura di ossigeno all'organismo e all'eliminazione dell'anidride carbonica dal sangue, ovvero agli scambi gassosi fra aria e sangue (processo noto con il nome di ematosi). Situati nella cavità toracica, sono avvolti da una membrana sierosa, la pleura, fondamentale per lo svolgimento delle loro funzioni. I polmoni sono separati da uno spazio compreso tra la colonna vertebrale e lo sterno, il mediastino, che comprende al suo interno il cuore, l'esofago, la trachea, i bronchi, il timo e i grossi vasi.

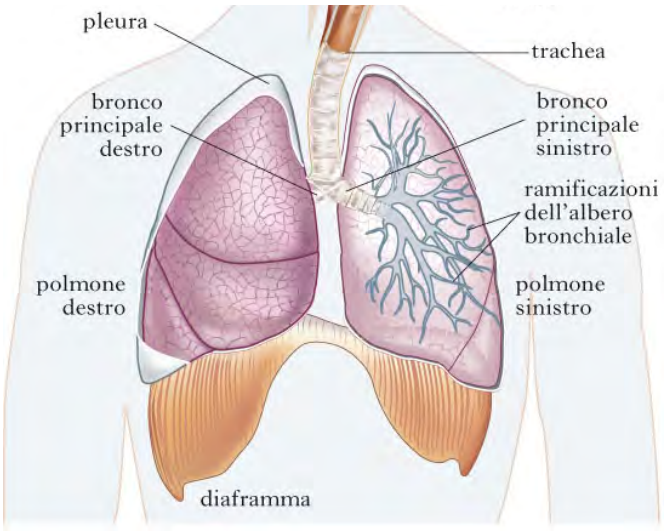

Figura 1 - *Struttura dell'apparato respiratorio: i polmoni*

Il loro compito principale è quello di ricevere il sangue carico di anidride carbonica e prodotti di scarto dalla circolazione periferica e di "ripulirlo" arricchendolo di ossigeno per poi inviarlo al cuore, da dove viene fatto circolare verso organi e tessuti.
La respirazione fisiologica è un processo automatico, controllato inconsciamente dal centro respiratorio posto alla base del cervello. La respirazione può essere controllata anche volontariamente, per esempio, quando si parla, canta o quando si trattiene volontariamente il respiro.
Gli organi sensoriali situati nel cervello, nell'aorta e nelle carotidi monitorano e rilevano i livelli ematici di ossigeno e di anidride carbonica interni all'organismo.
Nei soggetti sani, l'aumento della concentrazione di anidride carbonica rappresenta lo stimolo di maggiore importanza per una respirazione più profonda e rapida. Al contrario, quando la concentrazione di anidride carbonica nel sangue è bassa, il cervello riduce la frequenza e la profondità del respiro.
Durante la respirazione è possibile acquisire ad un segnale (fig. 2) la cui morfologia è assimilabile approssimativamente ad una sinusoide di periodo compreso tra 3.3 e 5 s avendo dunque una frequenza compresa tra 0.2 e 0.3 Hz, in un soggetto sano, la cui respirazione può variare tra 12 e 18 atti/min.

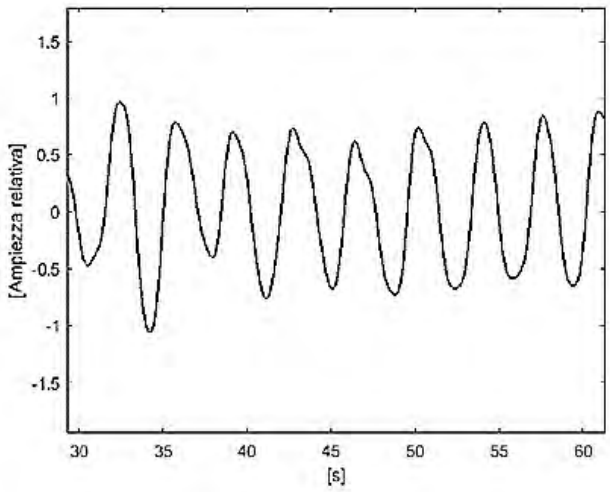

Figura 2 - *Segnale respiratorio con ampiezza normalizzata al suo valore massimo*

In questo segnale i tratti ascendenti rappresentano le inspirazioni e quelli discendenti le espirazioni, mentre la profondità del respiro dipende dal soggetto e dall'attività che sta svolgendo. Infatti, in base al tipo di respirazione ed allo stato dell'individuo, questo segnale può avere diversa ampiezza e i picchi possono essere più o meno ravvicinati nel tempo. Pertanto, dalla frequenza respiratoria e dalla morfologia del suo segnale è possibile risalire ad eventuali patologie che possono essere diagnosticate.

Le patologie dell'apparato respiratorio sono tra le più diffuse essendo legate a molteplici cause, dal banale virus del raffreddore a condizioni più gravi come tubercolosi, cancro ai polmoni e… COVID-19.

La tecnica dell'ascoltazione (o auscultazione) bronco-polmonare è il metodo più semplice e rapido per i medici per rilevare anomalie in fase di inspirazione ed espirazione rispetto al normale murmure vescicolare e diagnosticare o almeno ipotizzare la presenza di patologie.

Infatti, l'ascolto dei suoni respiratori permette ad un orecchio esperto di comprendere se il flusso d'aria all'interno dell'apparato respiratorio fluisce normalmente o è ostacolato da qualcosa. A seconda della sede di passaggio dell'aria si hanno diversi tipi di rumori fisiologici quali rumori vescicolari, bronco-vescicolari, bronchiali e tracheali [1, 2].

Il murmure vescicolare è il normale suono udibile a livello della maggior parte dei campi polmonari e che viene prodotto dalle piccole vibrazioni delle pareti degli alveoli in un soggetto sano. Tra le caratteristiche da analizzare dei suoni auscultati vi è il rapporto temporale tra inspirazione ed espirazione (I:E) normalmente di 1:2 ma se maggiore di 1:3 significa che vi sono limitazioni del flusso aereo, come nel caso di asma o broncopneumopatia cronica.

Tipici suoni anomali come i sibili (wheezes) durante l'espirazione e i crepitii (crackles) durante l'inspirazione sono ben noti sintomi di malattia [1, 2].

La presenza di qualunque patologia respiratoria si manifesta come un'alterazione dei suoni ascoltati in ampiezza, durata e frequenza. Di seguito viene riportata una tabella con le più

comuni patologie respiratorie e le relative caratteristiche della forma d'onda rilevabile tramite uno stetoscopio elettronico.

Tabella 1. Comuni patologie respiratorie e relative caratteristiche dei suoni rilevabili tramite stetoscopio

Tipologia di suono	Frequenza	Durata	Ampiezza/Profondità
Murmure vescicolare (normale)	< 200 Hz	4-5 sec	500 ml
Soffi	> 400 Hz	≥ 100 ms	
Stridore	400-800 Hz		
Ronchi	< 400 Hz	> 100 ms	
Rantoli	> 400 Hz	≥ 10 ms	
Crepitii	> 1000 Hz	< 7 ms	
Eupnea (normale)	14-20 atti/min	4-5 sec	500 ml
Apnea	nulla	15 sec	nulla
Tachipnea	> 20 fino a 40-60 atti/min		500 ml
Bradipnea	< 16, spiccata < 9 atti/min		500 ml
Respiro di Cheyne-Stokes	varia	45-180 sec	variabile
Respiro di Biot	variabile con alternanza di 4/5 atti/min e apnea	apnea di 10-30 sec	variabile
Respiro di Kussmaul	varia		variabile
Iperpnea	> 20 atti/min		> 500 ml

Oltre al murmure, c'è un particolare segnale, proveniente dall'apparato respiratorio, che può fornire importanti informazioni diagnostiche che è il suono proveniente dalla tosse.
Non tutti i suoni della tosse sono uguali, e questo è ben noto; tuttavia, forse meno noto è che ci sono delle caratteristiche che possono permettere una diagnosi precoce di patologie anche molto gravi, quali la polmonite.
Questo aspetto è stato studiato ed applicato dai ricercatori della Università di Lovanio al bestiame, ovvero per monitorare lo stato di salute delle mucche da latte e diagnosticare precocemente eventuale polmonite [3] ed è stato applicato sia dall'autore del presente articolo [4], che da altri ricercatori [5, 6] per la diagnosi precoce del COVID-19.
Per capire come ciò sia possibile, dobbiamo fare una breve panoramica sull'intelligenza artificiale (IA), applicata in maniera ormai sempre più diffusa ed affidabile per il riconoscimento dei segnali, degli oggetti e dei volti ed in particolare definire il concetto di caratteristiche (tecnicamente note come features) di un segnale, alla base dell'utilizzo di qualunque algoritmo di IA.

Il nocciolo dell'algoritmo per la diagnosi precoce della polmonite da COVID-19 consiste nella trasformazione dei suoni respiratori (inclusa la tosse) in immagini e poi applicare l'IA per classificare tali immagini come normali ovvero patologiche. Questa classificazione è proprio la diagnosi cercata ed è possibile ottenerla con un semplice smartphone, come vedremo.

2. Intelligenza Artificiale: Machine Learning e Deep Learning

Per IA si intende un metodo per analizzare dati che si ispira al modo di funzionare del cervello umano e che si concretizza in diversi modelli o algoritmi di calcolo, noti come reti neurali [7], di enorme utilità in molteplici ambiti.
Le operazioni che svolge l'IA sono: analisi di dati, individuazione e quantificazione di elementi caratterizzanti tali dati (processo noto come estrazione di features) e classificazione dei dati ovvero assegnazione di una ben precisa categoria di appartenenza. Tutto ciò a seguito di un processo noto come addestramento del modello, ovvero di attribuzione da parte del modello di IA di un determinato tipo e valore di features ad una determinata categoria di appartenenza.
Questo metodo è ormai di uso comune nel riconoscimento del parlato (implementato nei ben noti assistenti vocali presenti negli smartphone e nei PC e in dispositivi "intelligenti" come Alexa, Siri, Google) [8, 9] e si applica molto bene alla classificazione delle immagini ovvero al riconoscimento automatico di oggetti perché ogni classe di oggetti ha delle caratteristiche ben precise: la classe delle penne, per quanto siano le penne una diversa dall'altra, presenta caratteristiche ben diverse dalla classe delle automobili, per esempio.
Nell'ambito, poi, di uno stesso tipo di oggetti (le automobili, per esempio) è chiaro che ognuno ha caratteristiche proprie che lo distinguono dagli altri per cui anche in questo caso è possibile estrarre features che permettono di stabilire con un certo grado di probabilità di quale oggetto specifico si tratti all'interno di una certa categoria.
È molto importante sottolineare che l'IA fornisce risposte non certe in assoluto ma certe con un determinato livello di "confidenza", cioè con una determinata probabilità.
Nelle neuroscienze, il termine "rete neurale" viene utilizzato con riferimento a una rete o a un circuito formato da neuroni. L'esistenza di reti neurali biologiche, naturali, ha ispirato nell'informatica le cosiddette reti neurali artificiali (ANN, Artificial Neural Network).
Una ANN è un modello di calcolo la cui struttura stratificata assomiglia alla struttura della rete di neuroni nel cervello, con strati di nodi connessi. Una ANN può apprendere dai dati, quindi può essere addestrata a riconoscere pattern, classificare i dati e prevedere ("calcolare") eventi futuri sulla base di quanto ha appreso.
Una ANN combina diversi livelli (layer) di elaborazione. È formata, infatti, da un layer di input, uno o più layer nascosti e un layer di output. I layer sono interconnessi tramite nodi o neuroni, ed ogni layer utilizza l'output del layer precedente come input, per una elaborazione in cascata dei dati in ingresso.
Le ANN che operano su due o tre layer di neuroni connessi sono conosciute come reti neurali superficiali. Al contrario, le reti profonde, note come reti di Deep Learning (DL), possono avere molti layer, anche centinaia. Entrambe sono tecniche di Machine Learning (ML) che imparano direttamente dai dati di input [10-12].

Il DL è particolarmente adatto per applicazioni di identificazione complesse come il riconoscimento facciale, la traduzione di testi e il riconoscimento vocale. È anche una tecnologia chiave utilizzata nei sistemi avanzati di assistenza alla guida tra cui la classificazione delle corsie, il riconoscimento della segnaletica stradale e dei pedoni [13, 14].
Il DL in realtà non è un concetto troppo recente. Infatti, è stato teorizzato per la prima volta negli anni '80, ma si è sviluppato soltanto di recente, con il potenziamento esponenziale dei sistemi di calcolo, per due ragioni principali:

- perché un addestramento efficace, che permetta di ottenere poi risultati corretti con una elevata probabilità, richiede una grande quantità di dati già classificati, etichettati. Per esempio, per lo sviluppo delle automobili a guida autonoma sono necessarie milioni di immagini e migliaia di ore di video;
- perché richiede una notevole potenza elaborativa. Le attuali Graphic Processing Unit (GPU) ad alte prestazioni sono dotate di un'architettura parallela molto efficiente per il DL [15]. In combinazione con i cluster o il cloud computing, i team di sviluppo sono in grado di ridurre i tempi di addestramento per una rete di DL da diverse settimane a poche ore.

Qual è la differenza tra ML e DL?
Il DL è una forma specifica di ML. Come schematizzato in figura 3, un flusso di lavoro di ML per classificare, per esempio, automobili, inizia con un processo di estrazione delle *features* dalle immagini (fotogrammi da un video in tempo reale, per esempio), processo da eseguire separatamente rispetto alla fase di ML vera e propria e che richiede che vengano esplicitamente indicate le *features* da estrarre. Queste vengono quindi organizzate in un *dataset* ed utilizzate per creare un modello che categorizza gli oggetti nell'immagine.
Con un flusso di lavoro di DL, invece, le *features* significative vengono individuate automaticamente ed estratte dalle immagini, con notevole vantaggio perché non è richiesta una fase preliminare di individuazione e validazione delle stesse da parte dell'operatore. Inoltre, il DL esegue un apprendimento *end-to-end*, in cui una rete apprende automaticamente come elaborare dati grezzi e svolgere un'attività di classificazione.
Un vantaggio fondamentale del DL è la possibilità di migliorare le prestazioni con l'aumentare della quantità di dati forniti per l'addestramento [16].

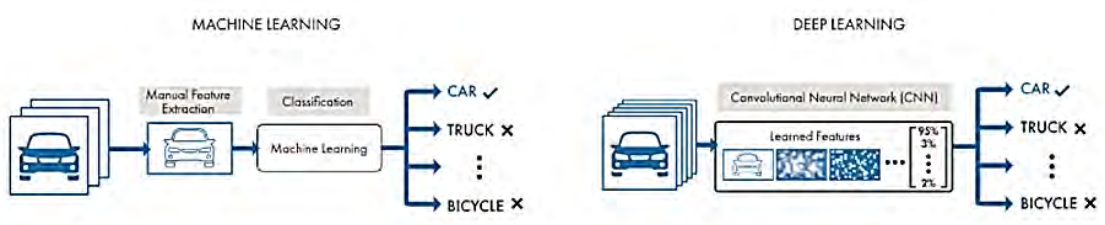

Figura 3 - *Confronto tra un approccio di ML (a sinistra) e DL (a destra) nella categorizzazione di veicoli. Il ML prevede la selezione manuale delle features e di un classificatore per l'ordinamento delle immagini. Con il DL l'estrazione delle features e la procedura di modellazione sono automatiche*

Al fine di produrre una diagnosi precoce di COVID-19 da tosse è più indicato il DL per via dell'automatismo con cui vengono individuate ed estratte le *features* ma si potrebbe anche usare il ML qualora non vi fossero dati a sufficienza a disposizione per addestrare la ANN.
Vediamo, quindi, come creare e addestrare un modello di DL.
I tre modi più comuni sono [16]:

- Addestramento della rete da zero e creazione del relativo modello di classificazione: per addestrare una rete di DL da zero, è necessario raccogliere un set di dati etichettati di grandi dimensioni e progettare un'architettura di rete dedicata. Ciò è utile per le nuove applicazioni o per le applicazioni che dispongono di un grande numero di categorie di output. Si tratta di un approccio poco comune poiché, considerata la grande quantità di dati e la critica velocità di apprendimento, il progetto e l'addestramento di queste reti richiede giorni o settimane.
- Transfer Learning: la maggior parte delle applicazioni di DL utilizza l'approccio denominato Transfer Learning (TL), un processo che consiste nella modifica e nel riaddestramento di un modello già esistente e precedentemente addestrato (rete preaddestrata) per riconoscere categorie di oggetti (classi) diversi da quelli di interesse [17, 18]. Si parte, dunque, da una rete neurale esistente (ve ne sono numerose: AlexNet, GooglNet, SquezeeNet, ResNet, CoffeeNet, ecc.) e la si modifica e riaddestra a riconoscere nuove classi di oggetti [19].
- Se la rete preaddestrata è in grado di riconoscere, ad esempio, 1000 classi di oggetti, con il TL, una volta modificata la rete, è possibile svolgere una nuova attività, per esempio il riconoscimento di sole 5 classi di oggetti anziché 1000. Questo approccio presenta il vantaggio di non dover progettare una ANN da zero e di richiedere molti meno dati per l'addestramento rispetto al caso in cui questo avvenga da zero, per cui i tempi di calcolo si riducono notevolmente.

In figura 4 vengono rappresentati gli step per modificare ed addestrare la rete tramite TL.
Successivamente verranno forniti alcuni dettagli in merito al tipo di ANN utilizzate per il DL sia alla specifica procedura di TL

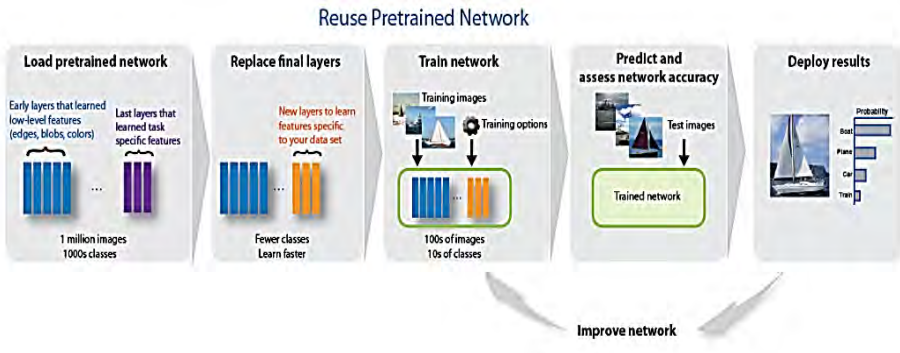

Figura 4 - *Algoritmo relativo all'addestramento di una rete neurale tramite il transfer learning. Tali steps devono essere eseguiti rigorosamente in cascata.*

2.1 Algoritmi per il Deep Learning: reti neurali convoluzionali

Nell'apprendimento automatico, una Rete Neurale Convoluzionale (CNN) è un tipo di ANN in cui il pattern di connettività tra i neuroni è ispirato dall'organizzazione della corteccia visiva animale [20]. Oltre alle CNN esistono anche altre reti come le reti LSTM, le quali a differenza delle prime acquisiscono i dati in ingresso come sequenza di vettori, contenenti tutte le informazioni caratterizzanti il dato da classificare.La CNN, come qualsiasi ANN, impara a eseguire attività di classificazione direttamente da immagini, video, testo o suono e non necessita di estrazione manuale delle *features*.
Le applicazioni che richiedono il riconoscimento degli oggetti e la visione artificiale, come i veicoli a guida autonoma e le applicazioni di riconoscimento facciale, si affidano in gran parte alle CNN in combinazione con l'utilizzo di GPU e del calcolo parallelo.
Come qualunque ANN, una CNN è composta da un *layer* di input, uno di output e molti *layer* nascosti nel mezzo.
Questi *layer* eseguono elaborazioni sui dati con l'intento di enfatizzare ed apprendere caratteristiche specifiche dei dati stessi. Tre dei layer più comuni che si replicano ripetutamente per costituire una CNN (fig. 5) sono: *convolution*, attivazione o ReLU e *pooling*.

- *Convolution*: questo layer inserisce le immagini in ingresso attraverso una serie di filtri convoluzionali, ognuno dei quali attiva determinate caratteristiche dalle immagini.
- L'unità lineare rettificata (ReLU), detto anche layer di attivazione, consente un addestramento più rapido ed efficace della rete mappando i valori negativi a zero e mantenendo i valori positivi. Questa operazione viene talvolta definita attivazione poiché solo le funzionalità attivate vengono trasferite al livello successivo.
- Il *pooling* semplifica l'output eseguendo il downsampling non lineare, riducendo il numero di parametri che la rete deve apprendere.

Queste operazioni vengono ripetute su decine o centinaia di livelli, con ogni strato che impara a identificare caratteristiche diverse dell'immagine in ingresso.

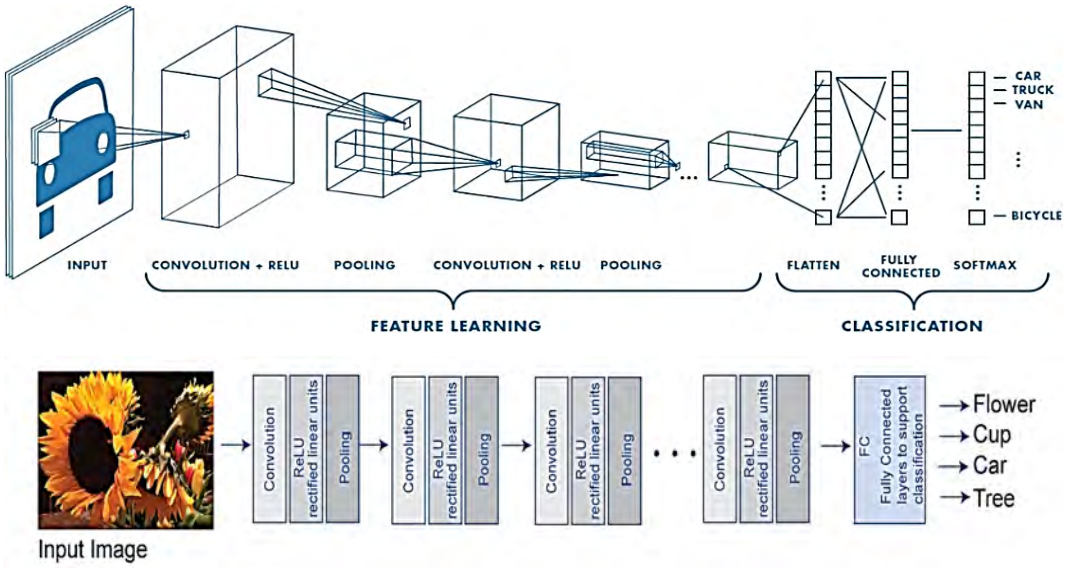

Figura 5 - *Esempio di una rete con molti strati convoluzionali. I filtri vengono applicati a ciascuna immagine di addestramento con risoluzioni diverse e l'output di ciascuna immagine convoluta viene utilizzato come input per il livello successivo. La CNN ha il compito di acquisire l'immagine e classificarla tra differenti categorie*

Il penultimo *layer*, denominato *fully connected layer*, fornisce un vettore di dimensioni K, dove K è il numero di classi che la rete sarà in grado di riconoscere. Il livello finale dell'architettura CNN utilizza un *layer* di classificazione per fornire *l'output* della classificazione cioè l'indicazione della classe cui appartiene l'oggetto rappresentato nella immagine di *input*.
Per la classificazione di oggetti da immagini la CNN riconosce la variazione di tonalità di colore in ogni pixel dell'immagine, così da capire sulla base della variazione della stessa di quale oggetto si tratti. L'algoritmo di riconoscimento quindi, si basa sul "percorrere" l'immagine in tutta la sua dimensione per intercettare variazioni di tonalità di colore, assegnando a ogni regione un valore numerico interpretato ed elaborato dai vari *layer* interconnessi.

2.2 Addestramento di una CNN

Per l'addestramento di una CNN il TL si rivela ancora una volta come un metodo molto efficiente perché richiede una minore quantità di dati rispetto all'addestramento da zero e tempi di calcolo ridotti.
Occorre, a tal fine, come schematizzato in figura 4, innanzitutto scegliere la rete preaddestrata che si ipotizza essere la più adeguata al tipo di attività che si vuole eseguire e, prima di avviare la procedura di riaddestramento, occorre modificarne opportunamente alcuni *layer* in modo che sia adatta al nuovo tipo di attività (ad esempio se dobbiamo analizzare immagini e classificare automaticamente la presenza di gatti, automobili, persone, penne le classi di output della rete saranno 4 mentre partiamo da una rete preaddestrata che sa classificare 1000 tipologie di oggetti diversi da quelli di nostro interesse).

Modificata la rete, occorre disporre di un *dataset* per l'addestramento, da suddividere in *mini-batch*: ogni iterazione del processo di addestramento utilizza differenti *mini-batch* di dati.
Ogni ciclo di addestramento è chiamato *epoch*. Il numero massimo di *epoch* e la dimensione delle *mini-batch* possono essere impostati come *training options*. In ogni *epoch* viene calcolata la perdita e la precisione del gradiente dell'addestramento eseguito.
Il gradiente permette di percorrere lungo una direzione specifica l'immagine in fase di analisi al fine di riconoscere le variazioni di tonalità dei colori, come visibile in figura 6.

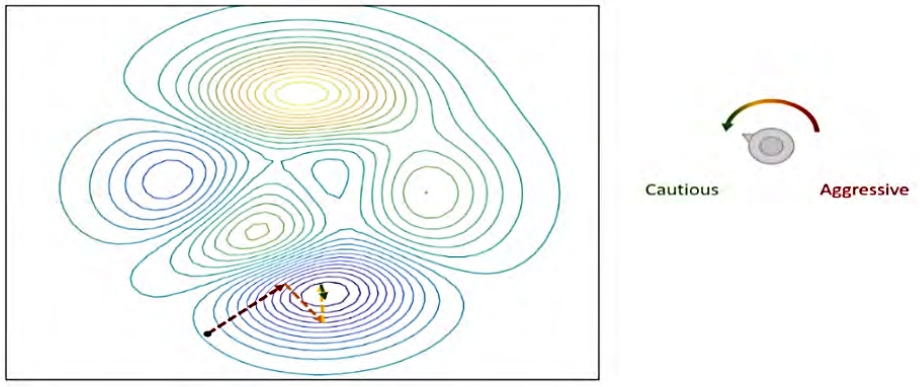

Figura 6 - *Percorso dell'operatore gradiente e della sua variazione all'interno dell'immagine.*

La dimensione dello *step* è chiamato *learning rate***,** il quale parte da un valore iniziale chiamato *initial learning rate*.
Durante l'addestramento viene prodotto un grafico (vedi fig. 7) in cui per ogni *epoch* è rappresentata la precisione e la perdita.

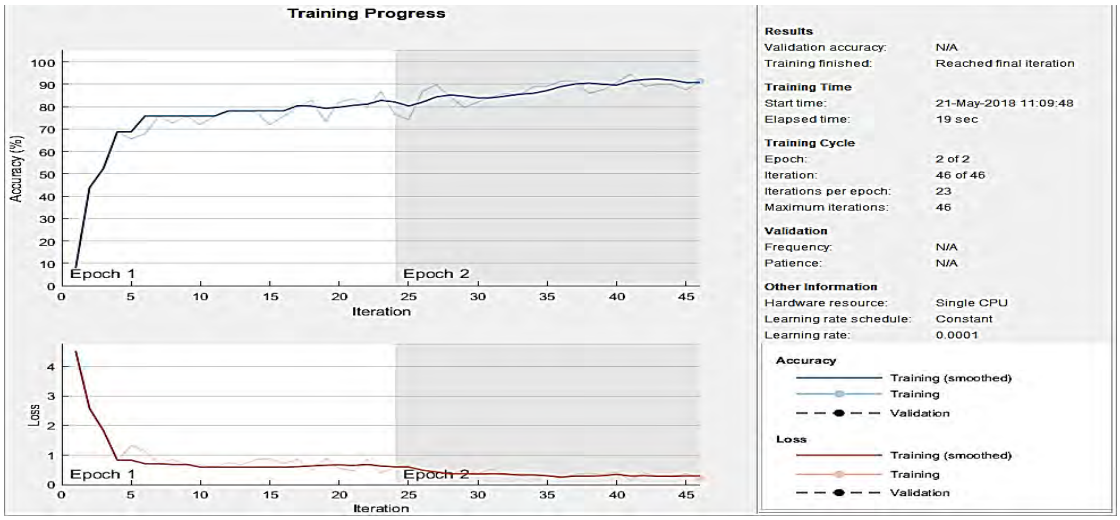

Figura 7 - *Esempio di grafico di training progress in cui sono visibili l'andamento di accuratezza e perdite durante l'addestramento della rete.*

2.3 Esportazione della rete addestrata

Al termine dell'addestramento è possibile esportare la rete addestrata inserendola successivamente come modello in algoritmi di IA. La esportazione nella forma di *compact model* permette anche, nell'ambito dello sviluppo di progetti in ambiente Matlab/Simulink, di implementare la rete in modelli di IA più complessi adatti alla traduzione di codice, per esempio alla creazione di app per sistemi operativi mobili (Android e iOS) funzionanti, quindi, su smartphone e tablet e al di fuori dell'ambiente Matlab/Simulink [21, 22].

3. Elaborazione di segnali audio per la classificazione con IA

Dalla panoramica sui metodi di IA concludiamo che è possibile effettuare riconoscimento di immagini tramite DL e/o ML effettuando in maniera automatica (con il DL) o manuale (con il ML) l'estrazione delle caratteristiche o *features*, per poi eseguire il riconoscimento ovvero la classificazione.
Affinché questo procedimento possa essere applicato ai dati di tipo audio occorre trasformarli in immagini. Si rende necessario, quindi, chiarire come possa avvenire in maniera efficace questa trasformazione.
Un segnale audio è un'onda di pressione che si propaga in un mezzo trasmissivo come l'aria. La frequenza di campionamento è tipicamente di 44,1 kHz ovvero 44.100 campioni al secondo. Un metodo di elaborazione di segnali audio, molto utile applicato congiuntamente ai modelli di IA, è la trasformata di Fourier (Fast Fourier Transform, FFT).
La FFT è uno strumento matematico attraverso il quale è possibile calcolare la trasformata di Fourirer discreta (DFT, Discrete Fourier Transform) o la sua inversa, ovvero convertire un segnale variabile nel tempo in una rappresentazione tempo-frequenza. Tale rappresentazione descrive il contenuto spettrale (cioè in frequenza) del segnale stesso e come esso si evolve al variare del tempo.
Di seguito verranno descritte diverse tecniche basate sulla rappresentazione tempo-frequenza che si sono rivelate particolarmente utili per la trasformazione in immagini di segnali audio e per la conseguente classificazione tramite DL:

- Spettrogramma Mel [23] e i suoi coefficienti (MFCC) [24];
- Spettrogramma Gammatone [25] e i suoi coefficienti (GTCC) [26];
- Scalogramma e coefficienti Wavelets (CWT) [27-29].

Oltre a queste tecniche ve ne sono altre che richiedono l'utilizzo di reti LSTM.
Tra le altre tecniche disponibili vanno citate la *Pitch* e la *Cepstral Descriptors*.
Le tipologie di immagini in cui possiamo convertire i dati di tipo audio sono tipicamente due: spettrogrammi e scalogrammi, e da queste immagini vengono estratte le *features* per il riconoscimento tramite DL. Tuttavia, le stesse *features*, a loro volta, possono essere rappresentate in forma di immagini. Si tratta in questo caso di immagini ottenute da *features* che sono i coefficienti MFCC, i coefficienti GTCC ed i coefficienti della CWT. Anche queste immagini possono poi essere analizzate tramite algoritmi di DL.
Esaminiamo, quindi, sia le immagini ottenute in forma di spettrogrammi e scalogrammi sia le immagini ottenute dalle *features* degli spettrogrammi e degli.scalogrammi.

3.1 Spettrogrammi e scalogrammi

Lo spettrogramma è la rappresentazione grafica dell'intensità di un suono in funzione del tempo e della frequenza. È dunque un grafico, nel quale sono riportate le frequenze che compongono l'onda sonora al passare del tempo. Lo spettrogramma contiene informazioni sull'ampiezza dell'onda (e quindi sull'intensità del suono), espresse mediante un codice di colori.
In figura 8 ad esempio è rappresentato lo spettrogramma di una nota "Do" emessa da una chitarra acustica.

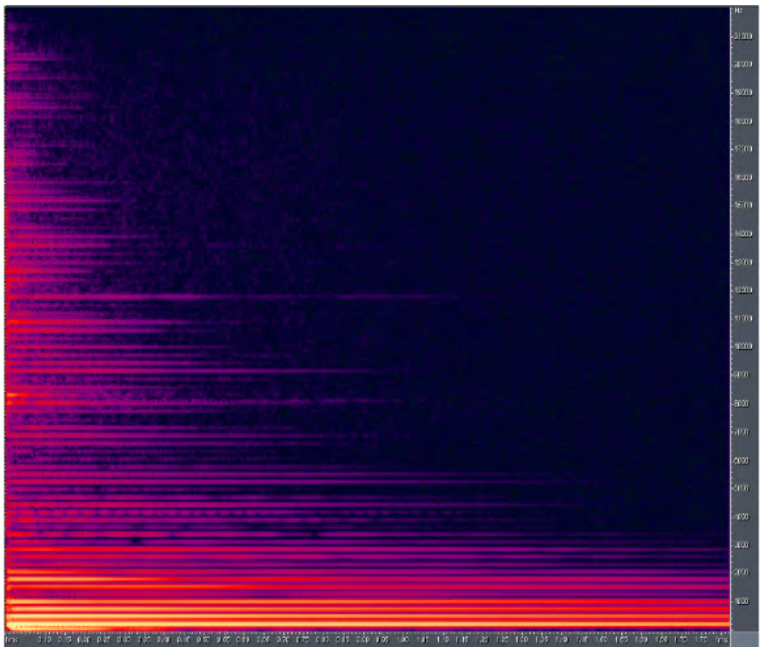

Figura 8 - *Spettrogramma di un Do emesso da una chitarra acustica. I colori più chiari (giallo) indicano una maggiore intensità sonora rispetto a quelli più scuri (viola)*

Sull'asse delle ordinate (verticale, asse y) vi sono le frequenze, su quello delle ascisse (orizzontale, asse x) il tempo. La presenza di più righe orizzontali, cioè di più frequenze, indica che non si tratta di un suono puro cioè monofrequenziale. Gli strumenti musicali, infatti, sono caratterizzati dai loro timbri, dovuti alla sovrapposizione di onde sonore di più frequenze accanto a quella "più importante", o dominante, che determina la nota. La frequenza dominante si chiama anche "altezza" (*pitch*) del suono. Lo spettrogramma della figura 8 mostra che la nota emessa contiene diverse frequenze, tuttavia i colori più chiari, associati a onde di maggiore ampiezza (e quindi a suoni più intensi), si concentrano intorno a determinate frequenze. Il suono è dunque piuttosto "pulito", cioè riconducibile quasi ad un'unica frequenza, poiché al suono di maggiore intensità corrisponde un intervallo di frequenze piuttosto "stretto".
Osserviamo inoltre che, al passare del tempo, il suono tende ad essere sempre più puro perché le frequenze lontane da quella dominante si attenuano maggiormente.
Diversamente accade quando la stessa identica nota è emessa da un banjo. Il Do prodotto dal banjo, il cui spettrogramma è mostrato in figura 9, contiene molte frequenze di elevata intensità

diverse tra loro, distribuite su un intervallo più ampio. Il suono è dunque meno puro, più "rumoroso", e inoltre ha una durata più limitata nel tempo.

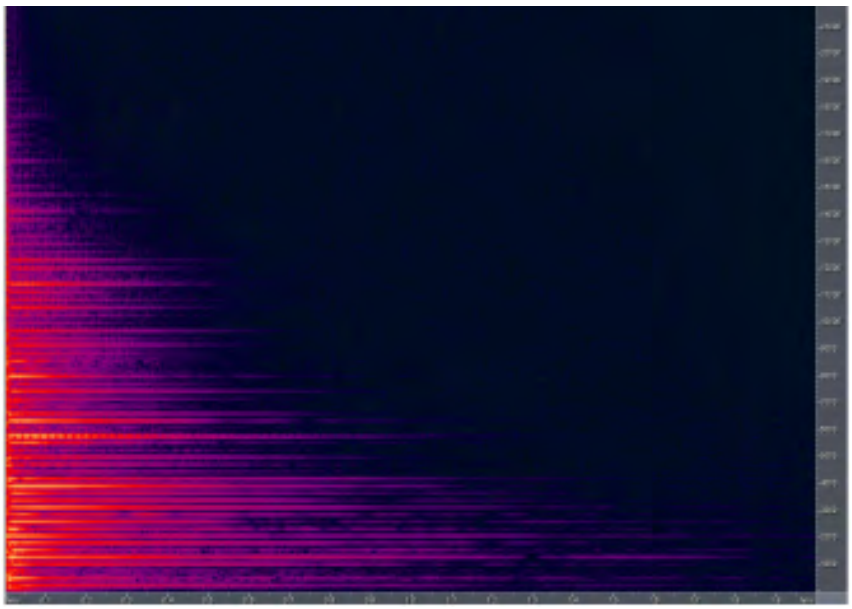

Figura 9 - *Spettrogramma di un Do emesso da un banjo. Un intervallo di frequenze più ampio, rispetto alla chitarra, è caratterizzato da una elevata ampiezza dell'onda sonora e quindi da un suono più intenso*

3.1.1 Generazione di uno spettrogramma e spettrogramma MEL

Uno spettrogramma si ottiene suddividendo la durata totale dell'intera forma d'onda da analizzare in sottointervalli uguali (detti finestre temporali) di durata tipica da 5 a 10 ms e calcolando la trasformata di Fourier della parte di forma d'onda contenuta in ciascuna finestra (solitamente si usa la FFT), che fornisce l'intensità del suono in funzione della frequenza. Le FFT relative alle diverse finestre temporali vengono poi assemblate a formare lo spettrogramma, come una sequenza di FFT impilate una sopra l'altra.
In uno spettrogramma generalmente l'asse delle ordinate viene generalmente convertito in una scala logaritmica e l'ampiezza viene convertita in decibel, dB, che è la scala logaritmica dell'ampiezza.
La scala di rappresentazione delle frequenze, tuttavia, non sempre è logaritmica e in base al modo in cui viene rappresentata otteniamo diversi tipi di spettrogrammi. Ad esempio, l'orecchio umano ha maggiore sensibilità alle frequenze più basse rispetto alle frequenze più alte per cui non percepisce le frequenze su una scala lineare. Questo significa che può facilmente distinguere un suono a 500 hz da uno a 1000 hz, ma difficilmente sarà in grado di distinguere un suono a 10.000 hz da uno a 10.500 hz.
Per questo motivo è definita la scala Mel, mostrata in figura 10. Il nome Mel deriva dalla parola melodia per indicare che la scala si basa sul confronto delle altezze dei suoni.

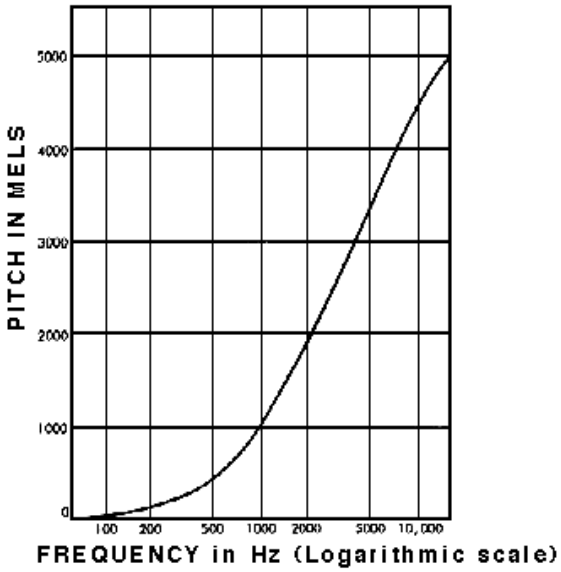

Figura 10 - *Scala Mel*

Infatti, la scala Mel è una scala percettiva dell'altezza di un suono. Il punto di riferimento tra questa scala e la normale misurazione della frequenza è definito assegnando un valore percettivo di 1000 Mels a un tono di 1000 Hz, con una pressione sonora di 60 dB sopra la soglia di ascolto della coclea umana. Al di sopra di circa 500 Hz, infatti, l'orecchio umano non riesce più a distinguere gli incrementi di frequenza. Di conseguenza, quattro ottave sulla scala hertz sopra 500 Hz comprendano circa due ottave sulla scala Mel.
Uno spettrogramma Mel è uno spettrogramma in cui le frequenze vengono convertite nella scala Mel. A scopo esemplificativo in figura 11 è mostrato lo spettrogramma MEL di un segnale audio generico e quello della registrazione di suoni cardiaci (toni cardiaci).

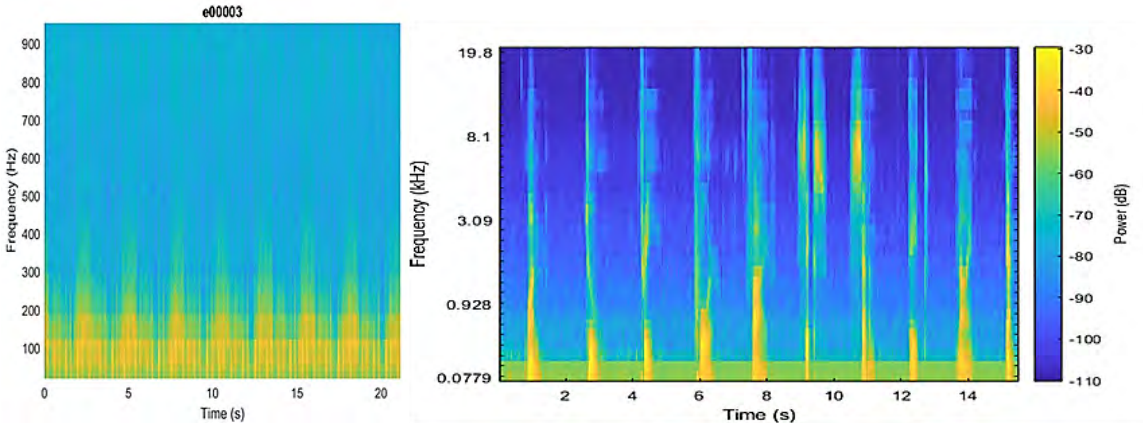

Figura 11 - *Spettrogramma Mel di un segnale audio cardiaco (toni cardiaci) a sinistra, e di un segnale audio generico a destra*

L'asse delle ordinate rappresenta la scala Mel e la variazione del colore rappresenta la variazione della densità di potenza (proporzionale all'ampiezza) del segnale espressa in dB, la quale viene rappresentata graficamente come di consueto con una differente tonalità di colore.

3.1.2 Spettrogramma Gammatone

Lo spettrogramma Gammatone è molto simile allo spettrogramma Mel, con la sola differenza che viene calcolato su una scala diversa, definita ERB (larghezza di banda rettangolare equivalente). La scala di frequenze ERB corrisponde all'incirca a posizionare un filtro ogni 0.9 mm nella coclea, come sarà meglio precisato successivamente.
In figura 12 viene mostrato un esempio di spettrogramma Gammatone di un segnale audio cardiaco e di uno generico.

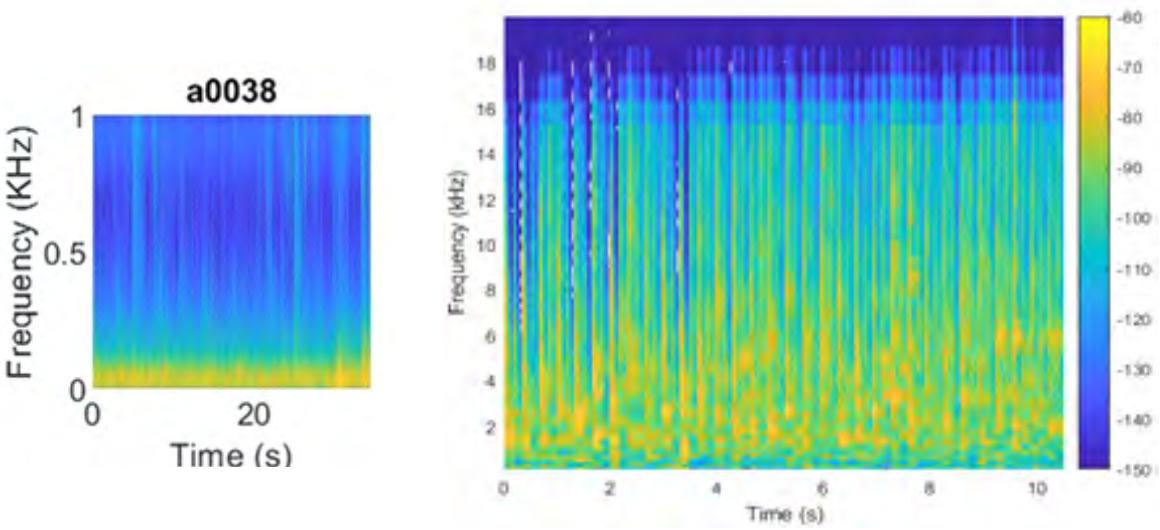

Figura 12 - *Spettrogramma Gammatone di un segnale audio cardiaco (a sinistra) e di uno generico (a destra).*

3.1.3 Trasformata Wavelet e scalogramma

La trasformata *wavelet* è la rappresentazione di un segnale mediante l'uso di una forma d'onda oscillante di lunghezza finita o a decadimento rapido (nota come *wavelet* madre). Questa forma d'onda è scalata e traslata per adattarsi al segnale in ingresso.
La trasformata *wavelet* è spesso paragonata alla trasformata di Fourier, dove i segnali sono rappresentati come somma di armoniche. La differenza principale è che le *wavelet* sono localizzate sia nel tempo sia nella frequenza mentre la trasformata di Fourier standard è localizzata solo in frequenza.
Anche la trasformata di Fourier a tempo breve (Short Time Fourier Transform, STFT) è localizzata in tempo e in frequenza, ma la trasformata *wavelet* offre generalmente una migliore rappresentazione del segnale grazie all'uso dell'analisi multirisoluzione.
La trasformata *wavelet* inoltre è anche meno complessa computazionalmente.

La trasformata *wavelet* di un segnale audio può essere rappresentata come immagine in forma di scalogramma che è il valore assoluto della trasformata *wavelet* continua (CWT) di un segnale, in funzione del tempo e della frequenza.
Esso si usa quando si desidera una migliore localizzazione temporale per eventi di breve durata e ad alta frequenza e una migliore localizzazione della frequenza per eventi a bassa frequenza e di lunga durata. Lo scalogramma può essere più utile dello spettrogramma, ad esempio, per analizzare segnali che variano lentamente punteggiati da transitori improvvisi.
In figura 13 è raffigurato un esempio di scalogramma di un segnale audio cardiaco.

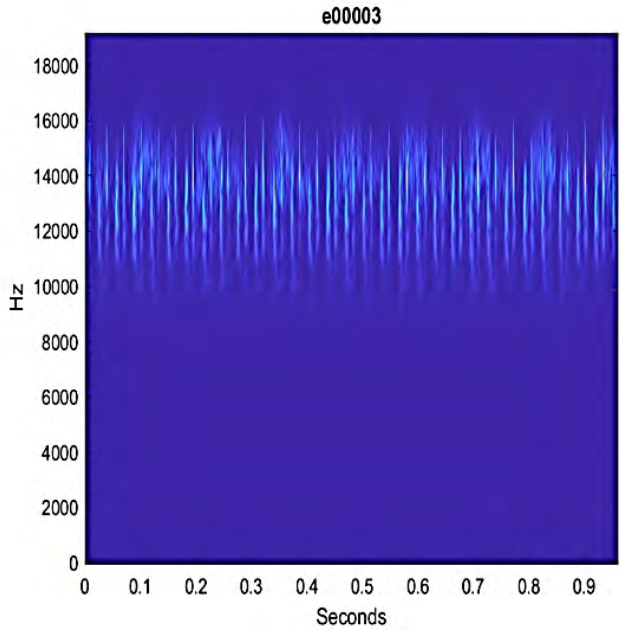

Figura 13 - *Spettrogramma Gammatone di un segnale audio cardiaco (a sinistra) e di uno generico (a destra).*

3.2 Immagini da features

3.2.1 Features dello spettrogramma MEL e immagine da MFCC

Lo spettrogramma MEL viene calcolato sottoponendo il segnale ad un filtraggio con un opportuno banco di filtri (fig. 14). Si tratta tipicamente di filtri triangolari sovrapposti a metà equidistanti tra loro sulla scala Mel, come visibile in figura 15.

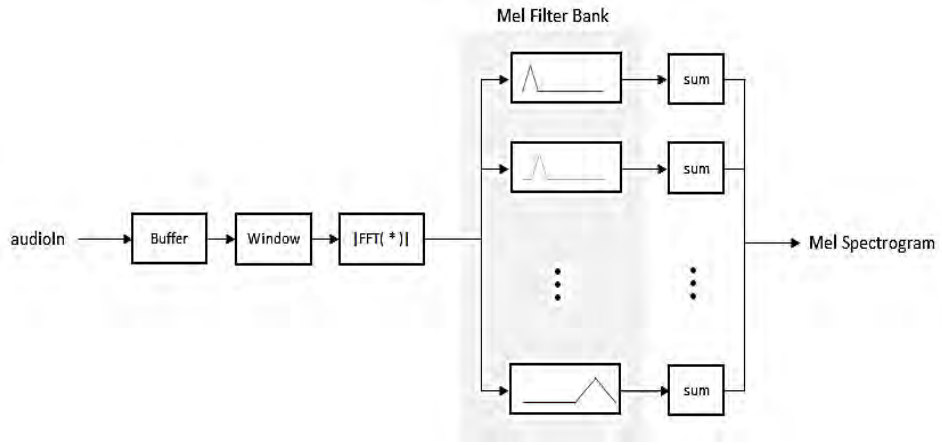

Figura 14 - *Algoritmo generatore dello spettrogramma Mel*

I seguenti tracciati mettono a confronto la degradazione provocata dalla singola presenza dei segnali LTE Uplink a 10 MHz centrati nelle frequenze di 708 MHz, 718 MHz e 728 MHz e la degradazione provocata dalla copresenza dei tre segnali 3x10 MHz, quest'ultimi a pari livello di potenza. La rappresentazione grafica avviene attraverso il rapporto I/C misurato all'ingresso del terminale di testa di un impianto TV impostato a guadagno massimo (≃ 37 dB) e con un livello di segnale utile (DVB-T2, Code Rate 2/3, Guard Interval 1/16, Modulazione 256 QAM ruotata) pari sia a -75 dBm che a -55 dBm. Attraverso la parte terminale del banco, composta da un attenuatore variabile e due matching pad 50/75 ohm, è stato fissato a -50 dBm il segnale utile all'ingresso RF del televisore.
Il primo filtro è molto stretto e dà un'indicazione di quanta energia è presente vicino alla frequenza continua (0 hz); man mano che le frequenze aumentano, i filtri si allargano in quanto è importante sapere solo approssimativamente quanta energia si trova in corrispondenza di frequenze sempre più alte.

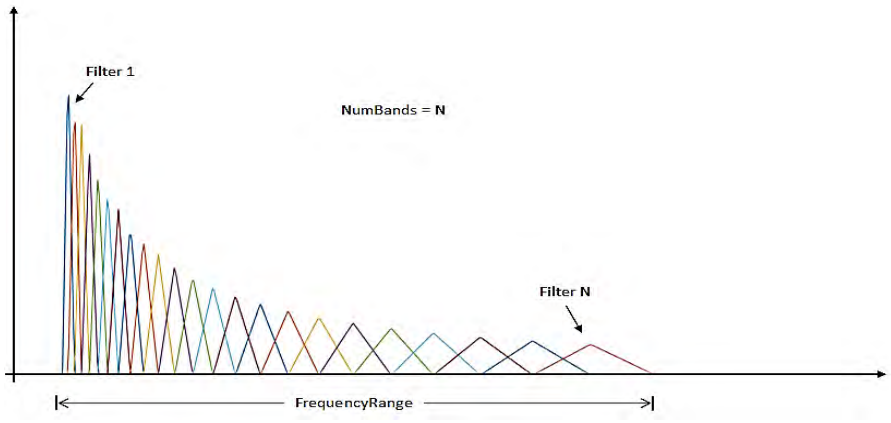

Figura 15 - *Mel filter bank*

Dallo spettrogramma Mel di un segnale audio si possono estrarre gli elementi caratteristici, o *features*, noti come *Mel-Frequency Cepstral Coefficients* (MFCC).
Gli MFCC permettono una rappresentazione del *cepstrum* reale di un segnale.
Il *cepstrum* di un segnale nasce come la trasformata di Fourier del logaritmo della trasformata di Fourier del segnale. A volte viene chiamato lo spettro dello spettro. In seguito, ha preso il sopravvento il calcolo del *cepstrum* come la trasformata di Fourier inversa applicata allo spettro del segnale espresso in scala logaritmica di Mel.
In figura 16 è rappresentato l'algoritmo relativo al calcolo dei coefficienti *cepstral*, il quale risulta essere uguale all'algoritmo visto nella generazione dello spettrogramma, con la sola differenza che in uscita al banco dei filtri viene inserito l'operatore DCT (Trasformata di coseno discreta), attraverso il quale è possibile ricavare proprio gli MFCC.

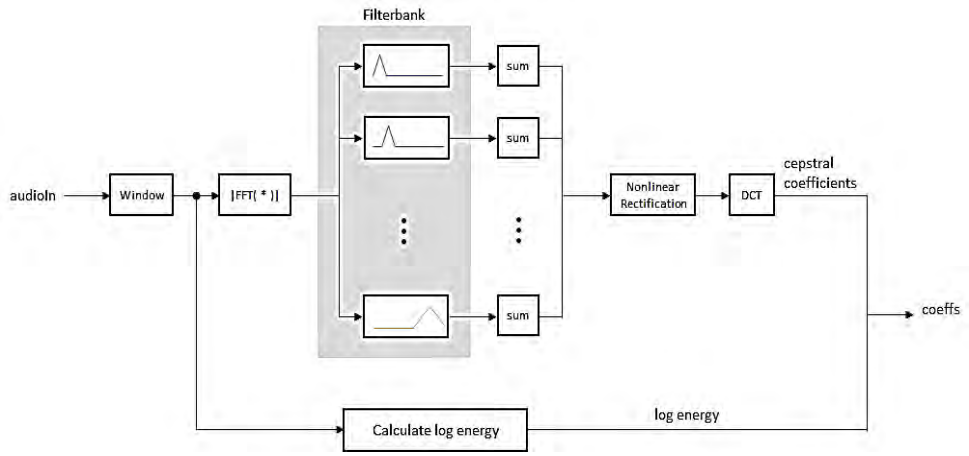

Figura 16 - *Algoritmo per l'estrazione di MFCC*

Gli MFCC a loro volta possono essere rappresentati come immagini che diventano, quindi, input per una CNN a scopo di classificazione con IA. Un esempio di immagine da MFCC è rappresentato in figura 17.

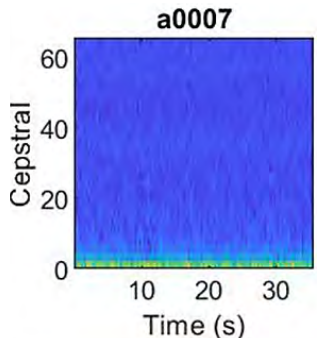

Figura 17 - *Esempio di immagine ottenuta rappresentando i coefficienti cepstral di uno spettrogramma di Mel in funzione del tempo*

La differente tonalità di colore è relativa alla diversa potenza del segnale al variare del tempo, fattore principale utilizzato dagli algoritmi di DL nella fase di addestramento della rete e classificazione dell'immagine per distinguere un segnale biologico normale da uno patologico.

3.2.2 Features dello spettrogramma GAMMATONE e immagine da GTCC

Lo spettrogramma Gammatone ed i relativi coefficienti *cepstral* alla frequenza Gammatone (GTCC), sono molto interessanti perchè risultano essere meno vulnerabili rispetto ad altri tipi di spettrogrammi a componenti di rumore eventualmente sovrapposti al segnale.
I coefficienti *cepstral* alla frequenza Gammatone (GTCC) vengono calcolati sottoponendo il segnale audio ad un filtraggio con banco di filtri composto da filtri Gammatone spaziati linearmente sulla scala ERB in un *range* di frequenze compreso tra 50 e 8000 Hz.
Le varie fasi di elaborazione per il calcolo dello spettrogramma Gammatone e delle sue *features* (i coefficienti GTCC) sono delineate in figura 18 e seguono la stessa logica dell'algoritmo visto nel calcolo dello spettrogramma Mel con le sue *features*, i coefficienti MFCC.

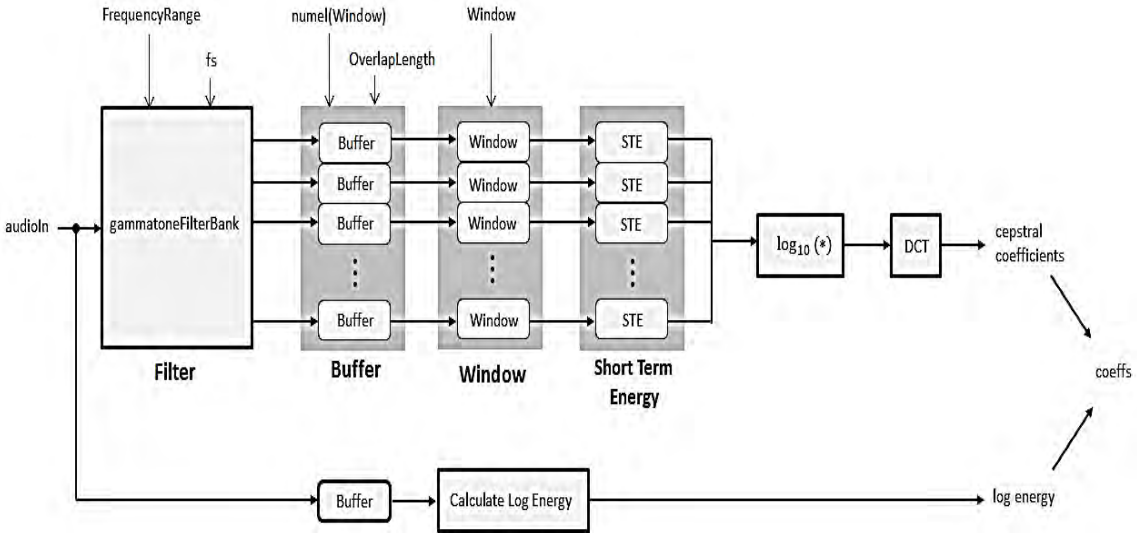

Figura 18 - *Algoritmo per l'estrazione di GTCC*

Un banco di filtri Gammatone viene spesso utilizzato come *front-end* di simulazione della coclea umana, trasformando suoni complessi in un modello di attività multicanale come quello osservato nel nervo uditivo, secondo la rappresentazione nel dominio della frequenza mostrata in figura 19.
La scala ERB definisce la spaziatura e la larghezza di banda dei filtri.

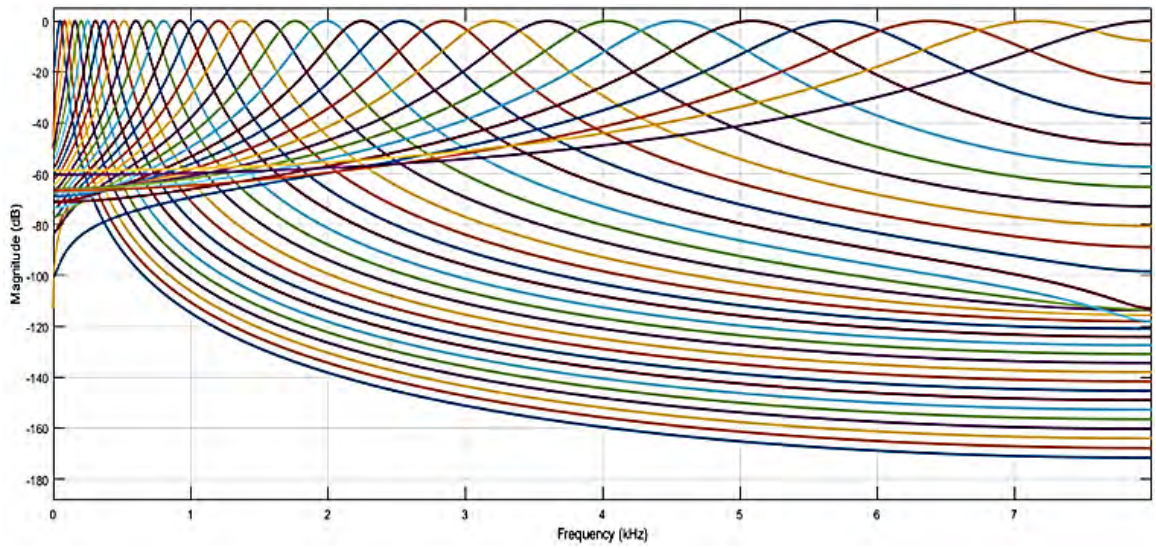

Figura 19 - *Gammatone filter bank*

L'uscita dal banco di filtri Gammatone è un segnale multicanale. Ogni canale di *output* dal banco di filtri viene bufferizzato in finestre di analisi sovrapposte e ne viene calcolata l'energia per ciascuna finestra di analisi.
Il segnale viene poi concatenato e fatto passare attraverso una funzione logaritmica e trasformata nel dominio *cepstral* utilizzando una trasformata discreta del coseno (DCT).
Anche per i coefficienti *cepstral* alla frequenza Gammatone (GTCC), *features* dello spettrogramma Gammatone, è possibile ottenere una rappresentazione in forma di immagine, nel dominio del tempo, come mostrato in figura 20, ed anche questa immagine può essere oggetto di classificazione tramite un modello di IA.

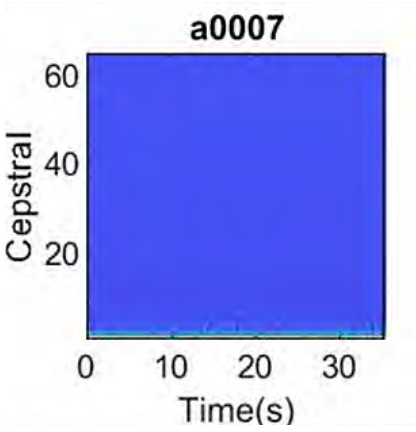

Figura 20 - *Esempio di rappresentazione nel tempo di coefficienti GTCC di un tono cardiaco*

3.2.3 Features dello scalogramma e immagini da CWT

Lo scalogramma, come già detto, è un grafico raffigurante il valore assoluto della CWT di un segnale audio, tracciato in funzione del tempo e della frequenza ed è particolarmente utile quando si desidera analizzare segnali con eventi di breve durata e ad alta frequenza e/o a bassa frequenza e di lunga durata.
Lo scalogramma si ottiene campionando il segnale con una *Window Length* di durata costante che viene spostata nel tempo e nella frequenza, a differenza dello spettrogramma in cui è fissa. Poiché lo spettrogramma utilizza una finestra costante, la risoluzione tempo-frequenza dello spettrogramma è fissa.
Per calcolare uno scalogramma è necessario innanzitutto campionare il segnale in segmenti sovrapposti e per ognuno di essi calcolare i coefficienti *Wavelet* costanti. In figura 21 è rappresentato un tipico scalogramma di segnale audio cardiaco con patologie.

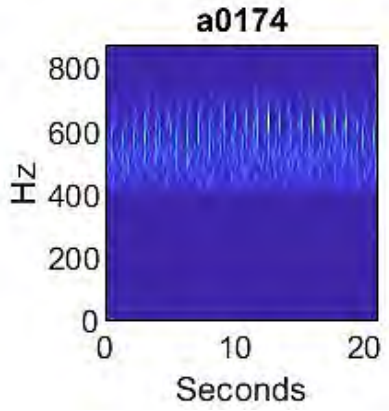

Figura 21 - *Scalogramma di segnale audio cardiaco con patologie valvolari. I coefficienti wavelet vengono calcolati processando il segnale con un banco di filtri*

In figura 22 è rappresentato il diagramma in frequenza relativo al banco di filtri utilizzati per calcolare lo scalogramma in ambiente Matlab, circa 10 filtri passa-banda per ottava.

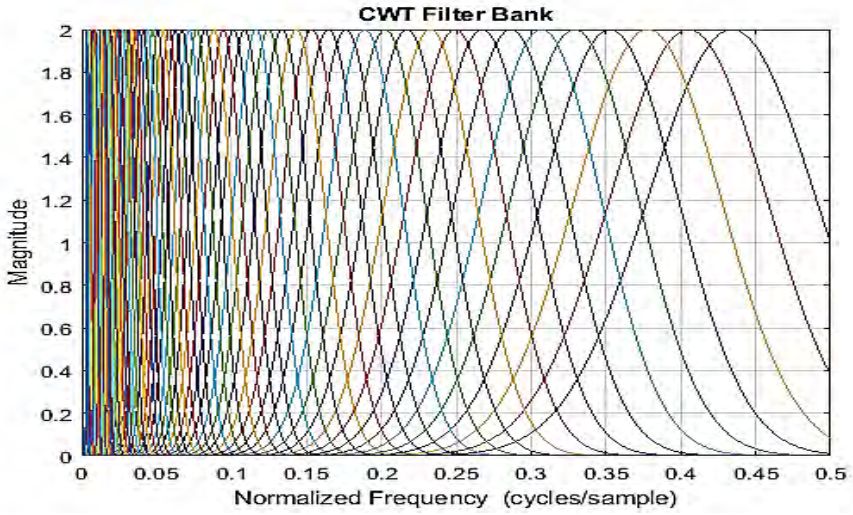

Figura 22 - *CWT filter bank*

Anche i coefficienti della CWT possono essere rappresentati come immagine, utile per essere classificata con strumenti di IA. In figura 23 è rappresentata l'immagine ottenuta dai coefficienti della CWT di un segnale audio cardiaco di un soggetto sano.

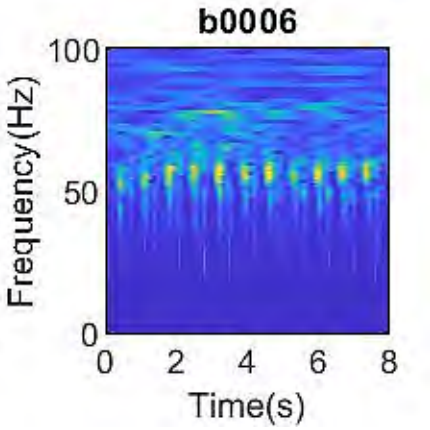

Figura 23 - *Immagine ottenuta rappresentando nel dominio tempo-frequenza i coefficienti della CWT di un soggetto sano*

3.3 Tecniche a confronto

Le tecniche presentate per la trasformazione di segnali audio in immagini risultano per certi aspetti simili tra loro, in quanto indicano diverse modalità di rappresentazione tempo-frequenza di un segnale audio; tuttavia, presentano delle differenze che ne consigliano per ciascuno uno specifico campo di applicazione.
Lo spettrogramma Mel e i suoi coefficienti MFCC sono tra le tecniche più utilizzate perché dimensionate sulla base della sensibilità uditiva umana. Tuttavia, presentano dei limiti legati alla bassa efficienza dei filtri Mel nell'eliminare il rumore additivo, soprattutto quello presente nei segnali audio del parlato e quindi in applicazioni di *speech recognition*; il problema è meno importante se si tratta di segnali biologici come i toni cardiaci ed il segnale respiratorio.
Il problema del rumore in applicazioni di *speech recognition* può essere risolto ricorrendo allo spettrogramma Gammatone e i suoi coefficienti GTCC, i quali riproducono meglio il comportamento della membrana della coclea umana, compreso il filtraggio delle frequenze in cui è collocato principalmente il rumore additivo.
I GTCC e il relativo spettrogramma Gammatone risultano quindi più adatti nell'identificazione e riconoscimento vocale, gli MFCC e il suo spettrogramma Mel invece, sono adatti per classificare segnali audio generici ma poco rumorosi ovvero battiti cardiaci e segnali biologici in generale, all'interno dei quali il comportamento al variare del tempo è ben definito e il campionamento risulta essere più facile, considerando anche che il rumore additivo risulta essere molto più attenuato rispetto agli altri perché si presume che siano acquisiti con hardware dedicato e con basso rumore.
L'altra tecnica presa in esame è quella relativa allo scalogramma e i suoi coefficienti *Wavelets*, attraverso la quale è possibile avere un buon compromesso tra risoluzione nel tempo e nella frequenza. L'analisi *Wavelet*, infatti, permette di elaborare informazioni con migliore risoluzione rispetto ad altre tecniche in quanto la finestra temporale di analisi non è fissa e permette di captare al meglio segnali audio con lunghi intervalli temporali a basse frequenze e intervalli temporali molto brevi ma ad alte frequenze. Tale tecnica sembra perciò particolarmente indicata per la classificazione di segnali respiratori dove si rilevano, soprattutto se patologici, suoni che si sovrappongono al murmure vescicolare, di durata breve e a frequenze elevate o prolungati e a frequenze più basse, come i *whezees* e i crepitii.
Le immagini ottenute con ciascuno di questi 6 metodi possono essere classificate tramite l'impiego di CNN ovvero con algoritmi di DL.
Pertanto, sono stati implementati e confrontati tutti i 6 metodi descritti, al fine di stabilire quale possa essere il più indicato per la classificazione del segnale prodotto dalla tosse da COVID-19 distinguendolo dalla tosse causata da altre patologie, al fine di poter formulare una diagnosi precoce attendibile di focolaio di polmonite da COVID-19.
Le immagini ottenute dai 6 algoritmi sono state classificate utilizzando più CNN al fine di determinare non solo il metodo di trasformazione del segnale audio in immagini maggiormente efficace ai fini di una accurata classificazione, ma anche il tipo di rete preaddestrata in grado di fornire una migliore accuratezza con l'utilizzo della tecnica del TL.

4. Classificazione di segnali audio biologici con modelli di IA

Riassumendo, i metodi di trasformazione dei segnali audio in immagini implementati e confrontati tra loro sono:

- Spettrogramma Mel
- Spettrogramma Gammatone
- calogramma (CWT)
- Immagine dei coefficienti MFCC
- Immagine dei coefficienti GTCC
- Immagine dei coefficienti CWT

I relativi algoritmi di elaborazione possono essere sintetizzati nello schema in figura 24

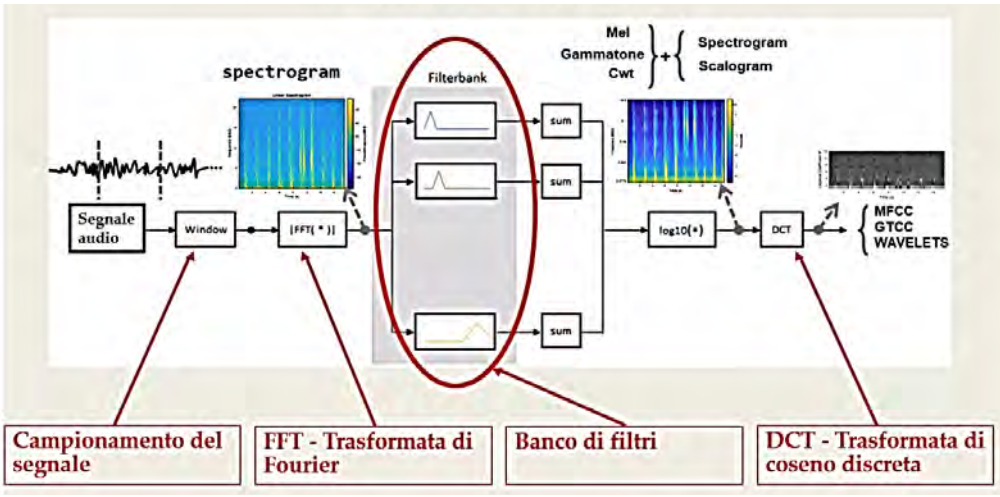

Figura 24 - *Rappresentazione sintetica degli algoritmi per la trasformazione di segnali audio in immagini. In base al tipo di banco di filtri utilizzati si ottiene spettrogramma Mel, spettrogramma Gammatone, CWT con scalogramma. Tramite il blocco DCT, in base al tipo di filtraggio eseguito a monte, si ottengono rispettivamente MFCC, GTCC, coefficienti della CWT*

Il primo database elaborato è di 3240 file audio di suoni cardiaci (i cosiddetti toni cardiaci), acquisiti tramite la tecnica della fonocardiografia (PCG) convertiti in immagini e successivamente dati come *input* alla rete neurale sia per l'addestramento che per il test di classificazione. Di questi file audio, 2574 sono relativi a toni cardiaci normali mentre 666 a toni cardiaci patologici. Il relativo database è disponibile online [30].
Successivamente, utilizzando un database [31] sia di toni cardiaci (817 normali e 183 patologici) che di suoni respiratori (35 normali e 885 patologici) è stato effettuato il confronto delle prestazioni tra varie reti preaddestrate, personalizzate con la tecnologia del TL, trasformando i file audio in spettrogrammi e scalogrammi.

4.1 Risultati e confronti

La prima rete preaddestrata utilizzata e riaddestrata secondo la tecnica del TL in ambiente Matlab, è GoogLeNet di cui sono stati modificati alcuni *layer* attraverso il *Deep Network Designer* del Matlab prima di procedere con l'addestramento.
È stato modificato il primo *layer* in quanto la dimensione dell'immagine dell'*imageInputLayer* di default della rete ha dimensione 224x224x3, invece le immagini da analizzare hanno dimensione 227x227x3; dopo di che è stato modificato il *fullyConnectedLayer* impostandolo a 2, in quanto le classi di uscita sono due, ovvero *normal* e *abnormal* (patologico), per lo stesso motivo è stato modificato anche l'ultimo *layer*, relativo al *classificationLayer*.
Infine, la rete è stata addestrata accedendo alle *training Options*, impostando un valore di *learning Rate* pari a 0.0001 e numero di *epoch* pari a 6.
Tale procedura è stata applicata per tutti i 6 metodi di trasformazione del segnale audio in immagini precedentemente descritti.
Dai risultati ottenuti un primo confronto può essere effettuato tra le tecniche relative alle rappresentazioni tempo-frequenza: spettrogramma Mel, spettrogramma Gammatone e scalogramma. Di seguito, in figura 25, sono mostrate le immagini relative allo stesso file audio derivante dall'acquisizione di toni cardiaci, preso come esempio e trasformato secondo ciascuno di questi tre algoritmi.

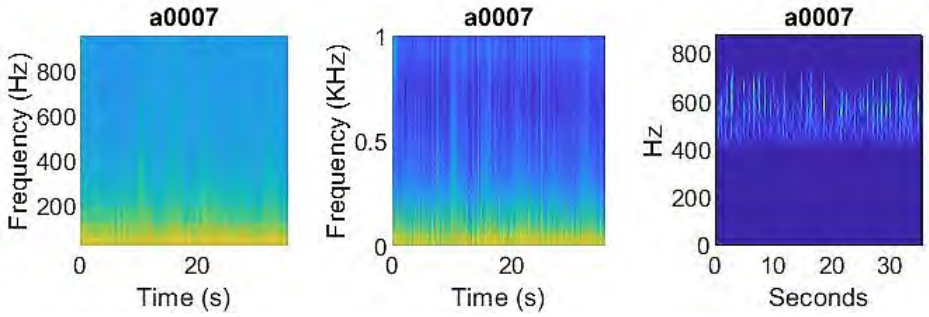

Figura 25 - *Spettrogramma Mel, Gammatone e scalogramma del tono cardiaco normale*

E' possibile notare che lo spettrogramma Mel (a sinistra in figura) rappresenta meglio questo tipo di segnale audio, qual è il tono del battito cardiaco, sin dalle basse frequenze, che sono le più importanti ai fini della corretta classificazione perché posseggono il maggiore contenuto informativo. Questo è dovuto principalmente al banco di filtri Mel che esalta queste componenti di segnale.
Un ulteriore confronto può essere effettuato estraendo le *features* dalle precedenti immagini, ovvero gli MFCC, GTCC ed i coefficienti Wavelets, e rappresentandole a loro volta in forma di immagini, come mostrato in figura 26.

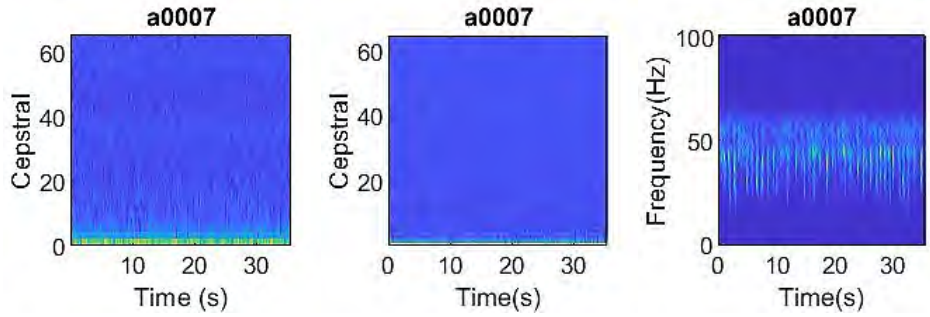

Figura 26 - *MFCC, GTCC e coefficienti della CWT del tono di un battito cardiaco normale*

È possibile notare che l'immagine ottenuta dagli MFCC (a sinistra) mostra variazioni di tonalità più marcate prestandosi, quindi, meglio alla classificazione tramite DL. Anche l'immagine ottenuta dai coefficienti *wavelets* (a destra) presenta una buona variazione della tonalità dei colori mentre le variazioni meno accentuate sono quelle presenti nella immagine ottenuta dai GTCC.
In tabella II sono confrontate le prestazioni, in termini di accuratezza e perdita per ogni *epoch*, della CNN basata sull'utilizzo della GoogleNet ed addestrata con il metodo del TL, relativamente ad ognuna delle tecniche di trasformazione di suoni in immagini sopra descritte.

Tabella 2. relativa al confronto tra le tecniche implementate con rete GoogleNet riaddestrata con TL

TECNICA UTILIZZATA	ACCURATEZZA	PERDITA
SPETTROGRAMMA MEL	**93 %**	**1.1**
SPETTROGRAMMA GAMMATONE	86.63 %	1.5
SCALOGRAMMA	89 %	3.5
MFCC	**93 %**	**1.2**
GTCC	91 %	1.3
WAVELETS	90 %	1.7

Come visibile in tabella e già preannunciato tramite analisi qualitativa, nella classificazione dei toni cardiaci la tecnica relativa allo spettrogramma Mel presenta un valore dell'accuratezza maggiore delle altre due tecniche ed un valore della perdita più basso, quindi tra le tre tecniche relative alle rappresentazioni tempo-frequenza questa risulta la più accurata e affidabile. Per lo stesso motivo tra le tecniche di estrazioni *features*, i coefficienti *cepstral* alla frequenza Mel (MFCC) risultano offrire un'accuratezza maggiore degli altri due (GTCC e coefficienti della CWT).
Successivamente, utilizzando un database [31] sia di toni cardiaci (817 normali e 183 patologici) che di suoni respiratori (35 normali e 885 patologici) è stato effettuato il confronto

delle prestazioni tra varie reti preaddestrate, personalizzate con la tecnologia del TL, trasformando i file audio in spettrogrammi e scalogrammi.
Le reti confrontate in ambiente Matlab sono state: GoogLeNet, SqueezeNet, AlexNet e ResNet50.
Il confronto delle prestazioni è mostrato in Tabella III
L'accuratezza maggiore (99.5%), per quanto riguarda il dataset dei toni cardiaci, è stata riscontrata nella rete GoogLeNet addestrata con *l'imagedatastore* degli spettrogrammi.

Tabella 3. Confronto delle prestazioni tra diverse reti preaddestrate e riaddestrate con il metodo del TL per classificare due tipi di suoni biologici: toni cardiaci e suoni polmonari

CNN (Convolutional Neural Network)	Validation accuracy spettrogrammi mel battiti cardiaci	Validation accuracy scalogrammi battiti cardiaci	Validation accuracy spettrogrammi mel respiri	Validation accuracy scalogrammi respiri
GoogLeNet	99.5%	97%	95.65%	100%
SqueezeNet	98.5%	98.59%	96.2%	100%
ResNet50	95%	99%	96.74%	100%
AlexNet	96.33%	97.67%	96.36%	100%

In figura 27 e 28 rispettivamente sono riportati i grafici dell'accuratezza e delle perdite rilevati durante l'addestramento della GooGleNet tramite TL con gli scalogrammi dei suoni respiratori (figura 27) e con gli spettrogrammi Mel dei toni cardiaci (figura 28), rispettivamente.

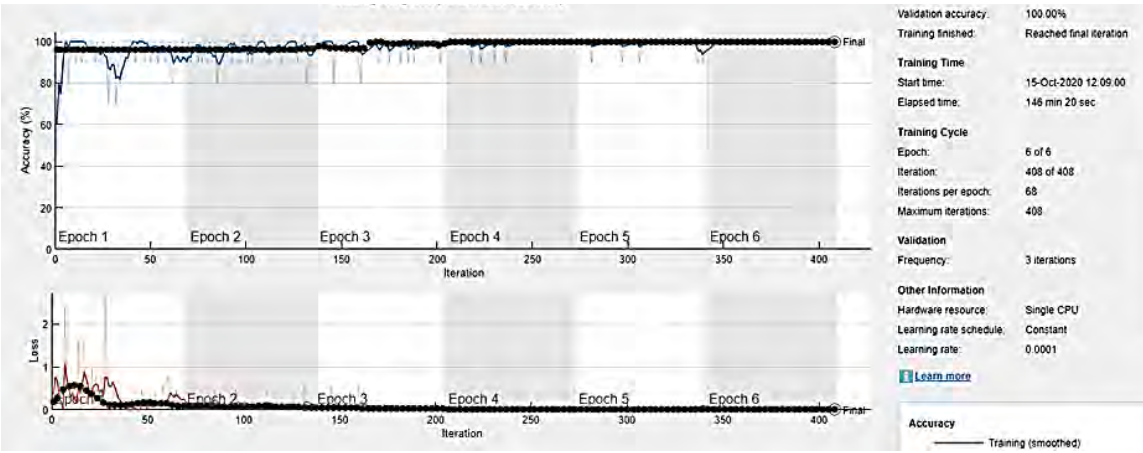

Figura 27 - *Accuratezza e perdite della CNN GoogLeNet in fase di addestramento con TL con gli scalogrammi dei suoni respiratori*

Per quanto riguarda invece il dataset dei suoni respiratori, l'accuratezza maggiore (100%) è stata riscontrata in tutte e 4 le reti addestrate con l'imagedatastore degli scalogrammi.

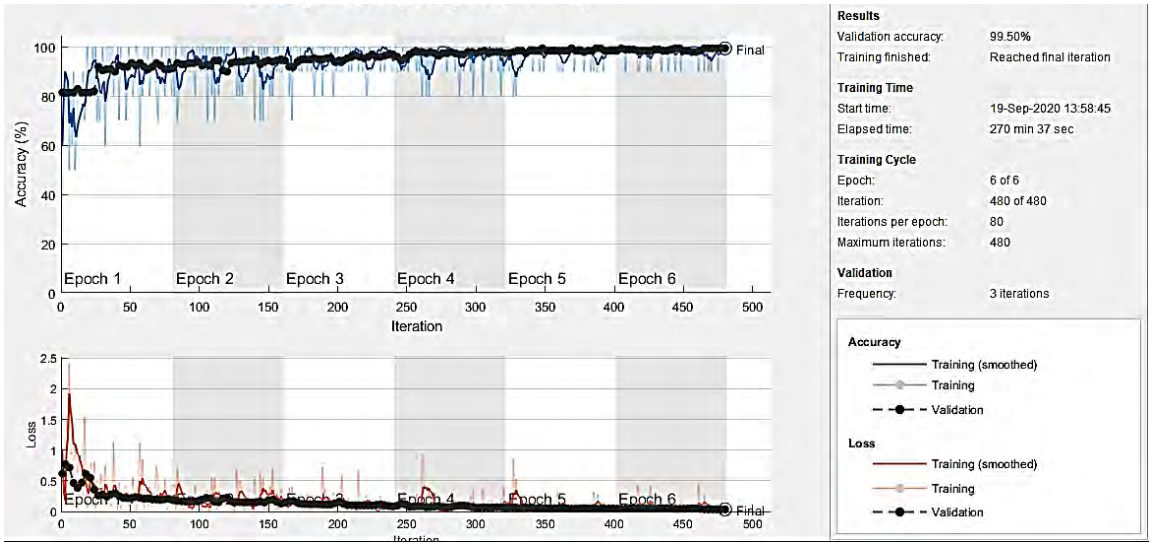

Figura 28 - *Accuratezza e perdite della rete CNN GoogLeNet in fase di addestramento con TL con gli spettrogrammi dei toni cardiaci*

Dai risultati ottenuti si evince molto chiaramente che lo spettrogramma Mel, i coefficienti MFCC, lo scalogramma ed i coefficienti *wavelets* sono i metodi di elaborazione dei suoni che meglio si prestano agli algoritmi di IA per riconoscere con elevato grado di confidenza i suoni biologici provenienti dall'apparato respiratorio classificandoli come normali o patologici, e che la rete GoogLeNet è la CNN preaddestrata, tra quelle prese in considerazione, che offre il più alto grado di confidenza nella classificazione.
Affinchè questa procedura possa essere applicata alla diagnosi precoce della polmonite da COVID-19 è necessario che si raccolga una quantità di file audio che sia la più grande possibile per applicare il metodo del TL per un addestramento fine di una delle CNN – presumibilmente la GoogleNet – al riconoscimento della tosse da COVID-19.
Studi preliminari [32] su un limitato numero di campioni dimostrano un'accuratezza non inferiore all'80% che, alla luce dello studio presentato in questo lavoro, ha potenziali ampi margini di incremento almeno sino al 90% ed oltre.

5. Sviluppo delle app per smartphone

La CNN addestrata tramite TL può essere implementata in modelli di IA eseguibili sia su PC che su smartphone permettendo così di sfruttare al meglio per scopi diagnostici di rilevante importanza le potenzialità computazionali e grafiche degli smartphone.
Per sviluppare app eseguibili sia in ambiente Android che in ambiente iOS occorre ovviamente essere esperti programmatori; tuttavia, almeno per uno sviluppo finalizzato alla verifica dell'idea ed al debug dell'algoritmo, ci sono comodi strumenti di traduzione di codice che permettono una programmazione di alto livello, spesso visuale, dunque abbastanza semplice, che non richiede conoscenze particolarmente approfondite dei linguaggi di programmazione. Questo è il caso dell'ambiente Matlab/Simulink [21, 22]. In particolare, il Simulink offre un tool di sviluppo di app per smartphone molto interessante ed utile, a partire dal *design* di un

modello a blocchi funzionali (dunque non direttamente scritto in linguaggio di programmazione) che poi viene automaticamente tradotto e convertito in app eseguibile su smartphone, come descritto di seguito.

A. Importazione della rete addestrata

Ci sono due modi in ambiente Simulink per implementare algoritmi di IA: uno è l'utilizzo del blocco funzionale *Image Classifier*, in cui si importa una CNN addestrata con TL dal tool di progetto delle reti neurali, ed esportata come modello; l'altro modo è l'utilizzo di un blocco funzionale Matlab personalizzato in cui viene inserito il codice per l'esecuzione di una CNN precedentemente addestrata ed esportata come *Compact Model*.
In ingresso al blocco funzionale, che sia l'uno o l'altro, viene fornita l'immagine da classificare (spettrogramma, scalogramma, immagine da *features*), in uscita si ottiene la classificazione (prediction) del dato fornito in ingresso ovvero segnale audio sano/patologico nel nostro caso.
Ovviamente per poter classificare i suoni occorre innanzitutto acquisirli.

B. Acquisizione audio

L'operazione di acquisizione dell'audio dei segnali biologici può avvenire tramite microfono dello smartphone o, qualora questo non risultasse di qualità adeguata, si può utilizzare un microfono esterno collegato allo smartphone. Il modello Simulink utilizzato allo scopo e direttamente traducibile in app per Android è mostrato in figura 29. Analogo modello potrebbe essere realizzato per traduzione in app per iOS.

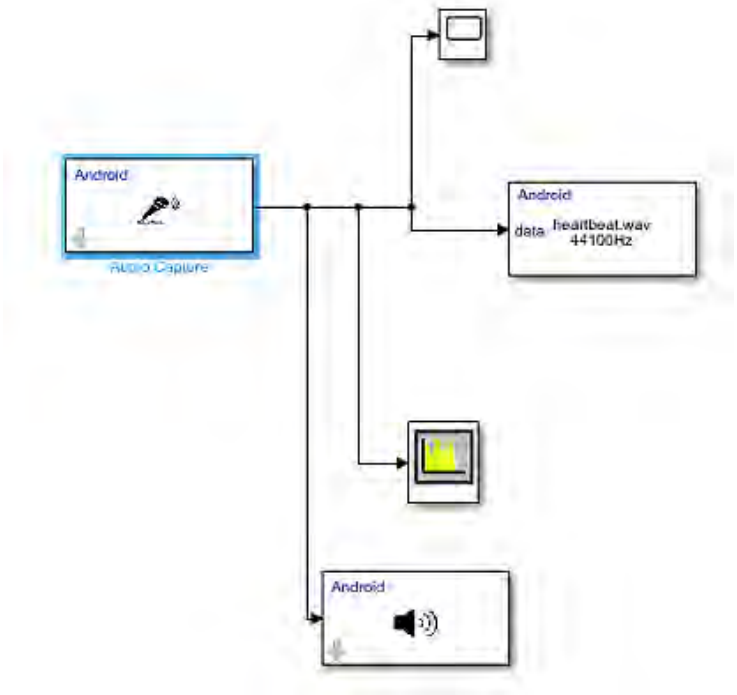

Figura 29 - *Modello Simulink per l'acquisizione audio*

Esso viene disegnato utilizzando il blocco funzionale *Audio Capture*, disponibile nella libreria del *Simulink Support Package for Android/iOS Devices*, che ci permette di acquisire l'audio dal microfono dello smartphone. La frequenza di campionamento scelta è di 44.1 kHz. In parallelo vengono inseriti i blocchi *Audio Playback* (per riprodurre sullo smartphone l'audio che si sta acquisendo), *Spectrum Analyzer* e *Time Scope*. Questi ultimi ci permettono di analizzare il segnale rispettivamente nel dominio della frequenza e del tempo simultaneamente all'acquisizione sul display dello smartphone. Infine, il blocco *Audio File Write* ci permette di salvare l'audio in formato *wav* sullo smartphone per eventuale, successivo, *post-processing*.
Il funzionamento di questo modello Simulink quando viene tradotto in app ed eseguito su smartphone Android è mostrato in figura 30.

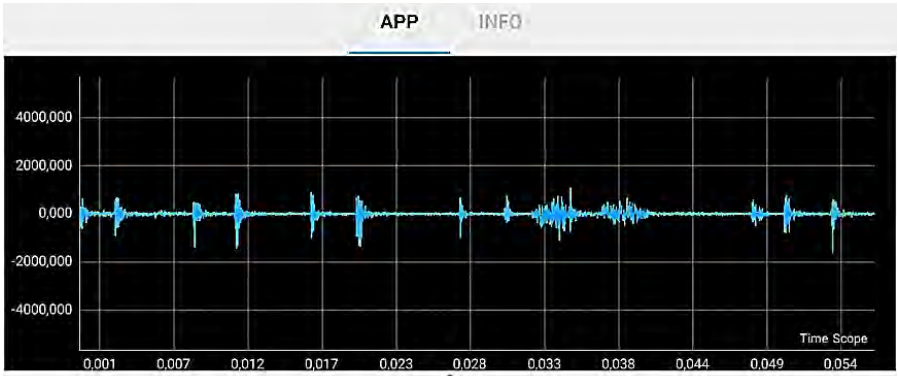

Figura 30 - *Screenshot dell'app progettata tramite Simulink, in acquisizione*

C. Trasformazione del file audio in immagine

Ogni file audio da classificare viene convertito in immagini tramite un ulteriore blocco funzionale appositamente sviluppato in Matlab ed inserito nel modello Simulink: in base alle considerazioni precedenti risulta più adatto l'uso dello spettrogramma di Mel e l'estrazione dei coefficienti MFCC per i toni cardiaci e l'uso dello scalogramma con i coefficienti della CWT per i suoni respiratori.

D. Classificazione con rete CNN

Si procede, infine, con l'inclusione della CNN addestrata con il TL ed esportata, in un blocco *Image Classifier* ovvero in un blocco funzionale *custom* di tipo *Matlab Function*, a completamento del modello, che viene poi tradotto in app installata ed eseguita su smartphone. Il modello risultante è mostrato in figura 31.

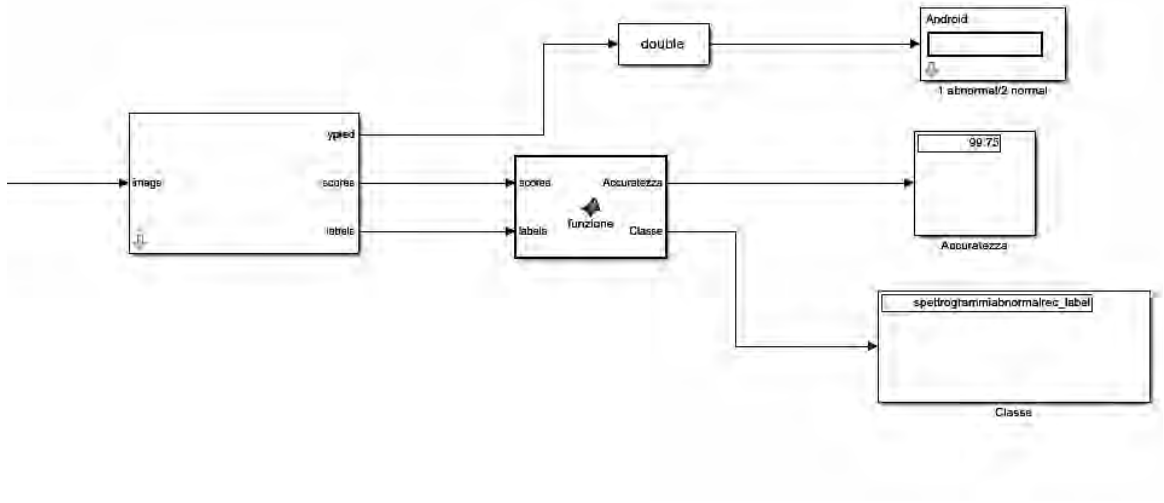

Figura 31 - *Modello simulink per la classificazione dei suoni biologici, tradotto in app ed eseguito su smartphone*

In questo modo si dispone di un'app in grado di monitorare automaticamente e continuamente lo stato di salute e di favorire una diagnosi precoce del COVID-19 a partire dai primi colpi di tosse.

6. Conclusioni e sviluppi futuri

Lo studio proposto in questo lavoro ha lo scopo di dimostrare come strumenti di IA possono essere applicati per uno degli obiettivi più importanti del trattamento del COVID-19 ovvero la diagnosi precoce della polmonite interstiziale. Tale diagnosi permetterebbe una riduzione dei ricoveri, un aumento della probabilità di sopravvivenza potendo intraprendere tempestivamente terapie adeguate ed una riduzione del rischio di contagio perché sarebbero individuati precocemente anche soggetti pauci-sintomatici.
La possibilità in termini di strumenti ingegneristici disponibili allo scopo è stata dimostrata, trattandosi peraltro di strumenti facilmente implementabili anche su smartphone tramite app dedicate che avrebbero, quindi, anche un costo assai accessibile.
Il passo ulteriore per completare questo studio con il progetto di un algoritmo finito di classificazione altamente affidabile è quello di disporre di un nutrito database di registrazioni della tosse di pazienti con di diverse patologie, incluso il COVID-19 ovviamente, perché indispensabile per un addestramento della rete neurale che consenta di ottenere livelli di confidenza della classificazione che siano il più possibile elevati, tendenti al 100%.
Per questo sarà necessario organizzare progetti coordinati tra gruppi di lavoro di medici e di ingegneri che speriamo possa essere attuata nel più breve tempo possibile.

Riferimenti bibliografici

[1] Grotberg, J. B. (2019). Crackles and Wheezes: Agents of Injury? Annals of the American Thoracic Society https://doi.org/10.1513/AnnalsATS.201901-022IP.
[2] https://www.healthline.com/health/breath-sounds
[3]http://www.scienzaegoverno.org/book/export/html/2144?fbclid=IwAR2kSmHDaxVVqkIjaKFtsGdTJ7Gtvo_5CYsZu5LaJ1krKTPJb2fqIjKRaFo
[4] https://www.facebook.com/100000562225270/videos/3255442694484439/
[5] https://global.techradar.com/it-it/news/covid-19-individuare-gli-asintomatici-con-smartphone-e-deep-learning-e-possibile?fbclid=IwAR3TvMaJb0-azObUUCbp_FhiAVgsiEb0URdmTMabZZoKRJNSUaor3VZGTRs
http://www.scienzaegoverno.org/book/export/html/2144?fbclid=IwAR1e-1JYZ4HiwJHRqsX41ycY8_1QKGUKFA1eG-9ew4IInpy-Wxhxhbdg3L0
[6] https://biomedicalcue.it/app-riconoscere-tosse-covid-19/22717/?fbclid=IwAR2SjT_iGlGa-7mpaaKpltVdu4ETdsmGeJKhvYPPjANJLHK_e7GjeBhvVZA
[7] https://it.mathworks.com/discovery/neural-network.html
[8] Speech Command Recognition using Deep Learning, Mathworks: https://www.mathworks.com/help/deeplearning/ug/deep-learning-speech-recognition.html
[9] Introduction to Deep Learning for Audio and Speech Applications, Webinar by Gabriele Bunkheila, MathWorks: https://www.mathworks.com/videos/introduction-to-deep-learning-for-audio-and-speech-applications-1560448385032.html
[10] Machine Learning and Deep learning for Audio, MathWorks: https://www.mathworks.com/help/audio/feature-extraction-and-deep-learning.html
[11] https://it.mathworks.com/discovery/deep-learning.html
[12] https://it.mathworks.com/discovery/machine-learning.html
[13] Deep Learning Onramp and Deep Learning with Matlab,
https://it.mathworks.com/learn/tutorials/deep-learning-onramp.html .
[14] Deep Learning for Signals and Sound, Webinar by Johanna Pingel and Emelie Andersson, MathWorks: https://www.mathworks.com/videos/deep-learning-for-signals-and-sound-1544467789023.html
[15] Deep Learning for Speech and Audio Processing with NVIDIA GPUs, Webinar by Gabriele Bunkheila, MathWorks: https://www.mathworks.com/videos/deep-learning-for-speech-and-audio-processing-with-nvidia-gpus-1586524417560.html
[16] Deep Learning Toolbox, Mathworks: https://www.mathworks.com/products/deep-learning.html
[17] Get Started with Transfer Learning, Mathworks: https://www.mathworks.com/help/deeplearning/gs/get-started-with-transfer-learning.html
[18] Transfer Learning with Deep Network Designer, Mathworks: https://www.mathworks.com/help/deeplearning/ug/transfer-learning-with-deep-network-designer.html

[19] https://it.mathworks.com/help/deeplearning/ug/pretrained-convolutional-neural-networks.html#mw_45a8c0b2-26fa-48e9-905a-a7ed7b87bfc8
[20] M. Plakal, D. Platt, R. A. Saurous, B. Seybold, M. Slaney, R. J. Weiss, and K.Wilson. 2017. CNN architectures for large-scale audio classification. In Proc.IEEE International Conference on Acoustics, Speech and Signal Processing (ICASSP).
131–135.
[21] Deep Learning in Simulink using Deep Neural Networks library, Mathworks: https://www.mathworks.com/help/gpucoder/ug/deep-learning-in-simulink-using-deep-neural-networks-library.html
[22] Getting Started with Android Devices, Mathwork: https://www.mathworks.com/help/supportpkg/android/examples/getting-started-with-android-devices.html
[23] Mel Spectrogram, Mathworks: https://www.mathworks.com/help/audio/ref/melspectrogram.html
[24] MFCC, Mathworks: https://www.mathworks.com/help/audio/ref/mfcc.html
[25] Gammatone filter bank, Mathworks: https://www.mathworks.com/help/audio/ref/gammatonefilterbank-system-object.html
[26] GTCC, Mathworks: https://www.mathworks.com/help/audio/ref/gtcc.html
[27] CWT,Mathworks: https://www.mathworks.com/help/wavelet/ref/cwt.html
[28] Wavelets, Mathworks: https://www.mathworks.com/help/wavelet/ref/cwtfilterbank.wavelets.html?searchHighlight=wavelet&s_tid=srchtitle
[29] Wavelet Scattering, Mathworks: https://www.mathworks.com/help/wavelet/ref/waveletscattering.html
[30] https://physionet.org/content/challenge-2016/1.0.0/
[31] https://www.kaggle.com/vbookshelf/respiratory-sound-database
[32] Chloë Brown, Jagmohan Chauhan, Andreas Grammenos, Jing Han, Apinan Hasthanasombat, Dimitris Spathis, Tong Xia, Pietro Cicuta, and Cecilia Mascolo. "Exploring Automatic Diagnosis of COVID-19 from Crowdsourced Respiratory Sound Data." Proceedings of the 26th ACM SIGKDD International Conference on Knowledge Discovery & Data Mining (KDD 2020)

Principali Applicazioni Biomedicali della Tecnologia RFID

Main Biomedical Applications of RFID Technology

Roberto Marani ♦, *Anna Gina Perri* □

♦ *Consiglio Nazionale delle Ricerche, Istituto di Sistemi e Tecnologie Industriali Intelligenti per il Manifatturiero Avanzato (STIIMA), Bari*
□ *Laboratorio di Dispositivi Elettronici, Dipartimento di Ingegneria Elettrica e dell'Informazione, Politecnico di Bari*

Sommario

In questo articolo, dopo una breve descrizione del principio di funzionamento e della struttura base della tecnologia RFID, vengono esaminate alcune tra le principali applicazioni di tale tecnologia in ambito biomedicale.

Abstract:

In this paper, after a brief description of the operating principle and basic structure of RFID technology, we present some of the main applications of this technology in biomedical field.

1. Introduzione

L'acronimo RFID (Radio Frequency IDentification) sta ad indicare la funzione di identificazione di oggetti, persone, ecc. attraverso una trasmissione di segnali a radiofrequenza. L'identificazione implica l'assegnazione di un'identità univoca ad un oggetto che consenta di distinguerlo in modo non ambiguo. Il fine principale di questa tecnologia, pertanto, è quello di assumere, da parte di un "identificatore", varie informazioni su oggetti, animali o persone, per mezzo di piccoli apparati radio, associati ai medesimi. L'assunzione di informazioni è relativa ad operazioni di ricerca, identificazione, selezione, localizzazione spaziale e tracciamento. Identificatore ed identificato comunicano mediante segnali a radiofrequenza, quindi senza necessità di contatto fisico (a differenza, ad esempio, delle carte a banda magnetica) e senza che gli apparati siano né visibili (a differenza, ad esempio, dei codici a barre), né in visibilità reciproca (non-line-of-sight).
Negli ultimi anni tale tecnologia è diventata una delle tecnologie più diffuse data la grande varietà di applicazioni a cui si presta.
A differenza dei più comuni codici a barre, le etichette RFID (tag) supportano un ben più grande set di ID unici rispetto ai codici a barre. Inoltre possono memorizzare informazioni aggiuntive come il "produttore" o il "tipo di prodotto" oltre a poter misurare fattori esterni che indicano lo stato dell'oggetto come la temperatura o l'acidità [1-3].
In questo articolo, dopo una breve descrizione del principio di funzionamento e della struttura base della tecnologia RFID, vengono esaminate alcune tra le principali applicazioni di tale tecnologia in ambito biomedicale.

2. La tecnologia RFID

Un sistema RFID è composto da etichette denominate **tag** e **lettori** [1]. Le informazioni sono memorizzate nei tag che le trasmettono poi al lettore. Ogni lettore è in grado di ricevere dati da differenti tag simultaneamente senza che tra loro ci sia un contatto visivo. Successivamente invia tali dati ad un server per essere processati e analizzati.
Un tag RFID è un particolare microchip con un'**antenna integrata** per comunicazioni wireless. L'involucro è generalmente una lamina plastica ma spesso anche una capsula di vetro.
I diversi sistemi RFID sono classificati in due categorie: **sistemi attivi** e **sistemi passivi**.

Quelli **attivi** richiedono una fonte di alimentazione, pertanto possono essere connessi a una rete che li alimenta, oppure possono utilizzare dell'energia immagazzinata in una **batteria integrata**.
D'altra parte però, il tempo di vita di tali tag è limitato dalla quantità di energia immagazzinabile, in genere calcolata in base al numero di letture che il dispositivo deve sostenere.
Un esempio di questo tipo di tag è proprio il transponder che si trova sugli aeroplani per l'identificazione della nazione d'origine. In ogni caso, è proprio la batteria ad incidere su costo, dimensioni e durata di questi dispositivi, rendendoli poco adatti al mercato di consumo.

I sistemi RFID **passivi** risultano di maggior interesse in quanto non richiedono batterie e quindi manutenzione. Pertanto i tag godono di un **indefinito tempo di vita** e sono di **dimensioni abbastanza ridotte** da adattarsi a più pratiche etichette adesive. In generale questo tipo di tag è costituito da tre parti: un'antenna, un chip a semiconduttore connesso all'antenna, e qualche tipo di involucro o supporto. In questo caso è il lettore ad essere responsabile dell'alimentazione e della comunicazione con il tag. L'antenna cattura l'energia emessa dal lettore e risponde inviando l'ID del tag (il tutto coordinato dal chip).

Esistono due differenti approcci progettuali per il trasferimento dell'energia dal lettore al tag: a **induzione magnetica** e ad **onda elettromagnetica**.

Entrambe le tecniche si basano sulle proprietà elettromagnetiche associate a un'**antenna RF** (Radio-Frequenza, **RF**). Esistono diverse tecniche di modulazione che sfruttano segnali di **campo vicino** o **campo lontano** per trasmettere e ricevere dati. Nel contempo entrambi i tipi di segnali possono trasferire sufficiente energia da sostenere queste operazioni, tipicamente tra i 10 μW e 1 mW, in base al tipo di tag [4].

3. Struttura di un sistema RFID

Un sistema RFID prevede l'interazione di tre elementi: uno o più tag RFID (detti anche **transponder**), un lettore ed un sistema di backend (sistema per l'elaborazione dei dati) [1].
Il sistema di backend può essere costituito sia da un vero e proprio PC sia da un microcontrollore programmato per operazioni specifiche.
Il lettore invece comprende un apparato per la ricezione e l'invio dei segnali da e verso il tag, e un microcontrollore che legge e verifica le informazioni trasmesse. Tutti i dati sono poi memorizzati in un database.
I tag passivi si differenziano in base alla banda di frequenze in cui lavorano. I tag a **bassa frequenza** (124 KHz ÷ 135 KHz) presentano un raggio di azione fino ad 1 metro, quelli ad **alta frequenza** (13.56 MHz) presentano un raggio di azione più ampio ma ancora limitato

rispetto ai tag **UHF** (860 MHz ÷ 960 MHz), che hanno il maggior raggio di azione potendo operare fino a 10 metri.
Un lettore RFID è un dispositivo attivo, **portatile** o **fisso**, in grado di connettersi con uno o più tag contemporaneamente, e di trasferire le informazioni d'interesse ad un server. Esso è costituito da un'unità di controllo, un modulo a radiofrequenza e un'unità di accoppiamento con i tag. Dopo aver attivato il tag inviando un segnale di richiesta, e di alimentazione per i tag passivi, modulano un segnale con i dati da inviare al tag e demodulano quello con i dati ricevuti dal tag.
Un tag RFID generalmente è diviso in due sezioni: la prima, che provvede alla comunicazione con il lettore, e la seconda, che memorizza l'ID e altri tipi di informazioni.
Quando il tag passa attraverso il raggio d'azione del lettore, questo rileva il segnale di risposta generato dal tag, invia così un **impulso di sincronizzazione**, che assicura l'alimentazione per un tag passivo e la connessione tra lettore e tag, ed infine elabora le informazioni trasmesse.
Caratteristiche come potenza e larghezza di banda, variano da Paese a Paese in base alle normative vigenti.
Spesso, per la loro natura omnidirezionale, vengono largamente utilizzati tag con antenne a mezza lunghezza d'onda.
La Fig. 1 rappresenta la tipica struttura di una etichetta RFID su substrato plastico e antenna a **bobina planare** [1].

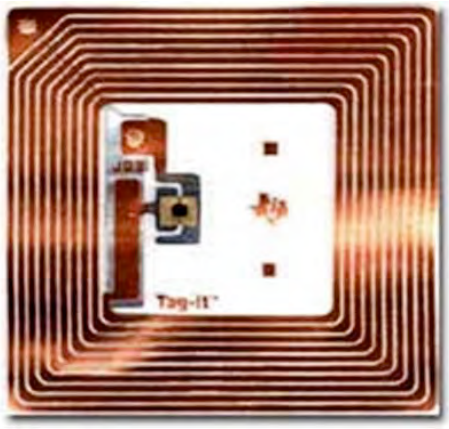

Figura 1 - *Tipica struttura di una etichetta RFID*

Tutte queste componenti base di un sistema RFID sono combinate in maniera differente, con qualche piccola differenza, in tutte quelle applicazioni che prevedono il tracciamento di un oggetto e, in base alla tipologia, si sceglie se utilizzare un tag passivo, semi-passivo o attivo.
Per quanto riguarda i lettori, il processo è simile, data la tipologia dell'applicazione per cui si sta realizzando il sistema: si decide se è meglio l'uso di lettori fissi, come per esempio il caso di un controllo di accessi, o di lettori portatili, come nel caso dell'organizzazione di un inventario. Se si opta per una zona di azione con lettori fissi si tiene conto anche di fattori quali potenza di segnale necessaria e tipo di antenna utilizzata sia per il lettore sia per il tag.
Certamente il processo di realizzazione di tag passivi è molto economico. Tuttavia questo si scontra con la necessità di un segnale molto più potente e ad alta frequenza rispetto all'uso di tag di tipo attivo [1].

4. Principali applicazioni dei sistemi RFID in campo biomedico

I campi di applicazione dei sistemi RFID sono numerosi, molti dei quali si sono sviluppati negli ultimi anni [1]. In questo articolo ci limitiamo a descrivere le applicazioni più diffuse in campo biomedicale.
La versatilità della tecnologia RFID, con particolari tag attivi, ha consentito di giungere al progetto di apparati RFID con funzioni di monitoraggio, identificazione, cura di patologie legate all'uomo [5].
Per ottenere questi risultati, la ricerca ha orientato i propri sforzi verso la progettazione di vere e proprie capsule di dimensioni ridottissime con funzionalità RFID, dotate di caratteristiche tecnologiche e di compatibilità elettromagnetica che le rendono perfettamente compatibili all'impianto all'interno dell'organismo umano.
La tecnologia RFID orientata alle applicazioni all'interno del corpo umano si basa generalmente su dispositivi passivi (*batteryless*) e permette di raggiungere distanze di lettura molto brevi, di solito 10 cm o meno.
Per le applicazioni biomedicali è previsto anche lo sviluppo di dispositivi RFID impiantabili per trasmettere vari parametri biologici o chimici misurati all'interno del corpo.
Tali dispositivi possono essere utilizzati da chi soffre di diabete: una unità di allarme wireless, impiantato nella regione addominale del paziente, legge continuamente i dati di un chip sensore sensibile alla concentrazione di glucosio nei fluidi circostanti. Recentemente si è utilizzata la tecnologia degli RFID impiantabili per la raccolta di dati *in vivo* e la trasmissione wireless di elettroencefalogrammi, acquisiti durante la registrazione su animali.
Dal punto di vista delle **applicazioni terapeutiche**, sono previsti dispositivi RFID da impianto per il monitoraggio e la manipolazione dell'attività biologica o funzioni fisiologiche del corpo umano. Un esempio è costituito dal monitoraggio delle funzioni cerebrali mediante sonde impiantate, in grado di comunicare tramite un transponder incorporato all'interno del cranio.
Una serie di 16 microelettrodi di iridio attivati (5-6 mm di lunghezza all'interno di un cluster di circa 1,8 mm di diametro), adatti per l'impianto a lungo termine nel cervello, registra il segnale di singoli neuroni e fornisce inoltre una microstimolazione localizzata.
Questi microelettrodi possono anche essere utilizzati terapeuticamente. Tuttavia tali applicazioni di impianti RFID sono ancora in fase di "*proof of concept"*, nel senso che i benefici di tale tecnologia in termini di miglioramento della qualità di vita o di cura del paziente, devono ancora essere dimostrati.
Ciononostante, l'avanzamento attuale della tecnologia è realisticamente in grado di consentire il monitoraggio remoto delle funzioni biologiche in un essere umano.
Secondo alcuni studi [5], un sistema radio a singolo chip (comprendente l'antenna) con sensori montati a bordo di dimensioni complessive di 100 x 100 x 1 μm^3 sembra essere fattibile con la tecnologia disponibile. Conseguentemente, la comunicazione wireless con piccoli impianti RFID all'interno dell'organismo per l'acquisizione di informazioni circa la presenza di sostanze chimiche o l'entità di determinate grandezze fisiche nei sistemi biologici o anche la attivazione/disattivazione remota dell'attività biochimica all'interno di una singola cellula vivente, sembrano essere obiettivi raggiungibili.
Inoltre, utilizzando le nanotecnologie, è stato realizzato un apparato radio FM usando un singolo nanotubo (Carbon NanoTube, CNT) di lunghezza 1μm e 10 nm di larghezza [5]. Questo apparato potrebbe essere inserito all'interno di cellule umane e costituire una interfaccia di controllo subcellulare in *real-time*.

Tale risultato di miniaturizzazione dei radio-chip potrebbe anche trovare applicazione nella fabbricazione di *smartdusts*, cioè di piccoli oggetti con capacità di rilevamento e comunicazione, che possono essere massicciamente distribuiti su una certa zona per il controllo remoto a livello biomolecolare, il cui studio di fattibilità è stato riportato in [6].
In particolare il controllo della ibridazione delle molecole di DNA è stato realizzato attraverso il monitoraggio del riscaldamento di nano-particelle di oro legate al DNA [7]. Il riscaldamento locale controllato, ottenuto per accoppiamento elettromagnetico alla frequenza di 1 GHz, induce la ibridazione/de-ibridazione reversibile del DNA, lasciando relativamente inalterate le molecole circostanti. Sebbene gli effetti fisici del riscaldamento di particelle di dimensioni nano-metriche siano stati ancora poco esplorati e saranno sicuramente oggetto di studi futuri, questo esperimento dimostra, per la prima volta, il controllo diretto, per mezzo di segnali a radiofrequenza, di reazioni biomolecolari in modo specifico e pienamente reversibile. Il controllo remoto su tale scala sembrerebbe non alterare eventi biomolecolari, che hanno luogo nel mezzo circostante.

5. Requisiti tecnici per dispositivi destinati all'impianto umano

Affinché un dispositivo, dotato di sensori e funzionalità di computazione e comunicazione, sia impiantabile in un essere umano, devono essere soddisfatti numerosi requisiti tecnici [1].
Innanzitutto impianti *in vivo* devono essere più piccoli possibile. Inoltre potrebbe risultare impraticabile l'uso di batterie per fornire potenza a un dispositivo elettronico iniettato nel corpo: le grandi dimensioni delle batterie impediscono il loro utilizzo e per questo potrebbe risultare preferibile un dispositivo passivo (detto anche *batteryless* o *fully autonomous*).
Un altro requisito riguarda la selettività del controllo remoto di funzioni biologiche umane. Per esempio, il controllo remoto di uno specifico evento biomolecolare all'interno di una cellula deve essere spazialmente ben localizzato per non influenzare altre attività biologiche nella cellula.
In aggiunta è necessario usare materiali biocompatibili per la fabbricazione del dispositivo e del suo package per evitare l'insorgere di reazioni indesiderate dei tessuti.
Un'altra eventualità da impedire, o al più da tenere sotto controllo, è la possibilità che il dispositivo si sposti dal sito in cui è stato impiantato in altre regioni all'interno dell'organismo.
Altro requisito essenziale è rappresentato dalla necessità di realizzare una trasmissione wireless di dati personali e riservati, che sia il più possibile sicura ed affidabile. Al fine di implementare tale tecnologia wireless è indispensabile dare la massima priorità a criteri di riservatezza ed elevata affidabilità.
Infine, per le problematiche di sicurezza legate all'impianto di antenne nei tessuti umani, l'energia elettromagnetica irradiata (o reirradiata, *backscattered*) da un dispositivo per la comunicazione senza fili con il mondo esterno deve attenersi alle specifiche imposte dallo standard IEEE per l'esposizione dei tessuti umani ai campi elettromagnetici [8].
Per soddisfare tali raccomandazioni di sicurezza, è stata progettata un'antenna impiantabile, funzionante a 868 MHz, per garantire un **SAR** (*Specific Absorption Rate*) minore di 2 W/kg.
In tempi recenti sono state progettate antenne impiantabili che operano nella banda di frequenze del *Medical Implant Communications Service* (402-405 MHz), che è regolamentata dalla *Federal Communications Commission* e dal *European Radiocommunications Committee* per antenne impiantabili ultra-low power. Affinché vengano soddisfatti i requisiti imposti da queste istituzioni, sono state progettate antenne che ammettono un SAR di picco pari a solo 1.6 mW/g.

Le onde elettromagnetiche LF (a bassa frequenza) non sono molto attenuate dai tessuti corporei. Tuttavia la distanza massima di lettura associata a dispositivi RFID operanti a bassa frequenza (135 KHz) è generalmente inferiore ad 1 m a causa della rapida attenuazione del campo magnetico con la distanza e la sezione trasversale dell'antenna, che deve essere necessariamente molto piccola. A questo si aggiunge il fatto che questi apparati hanno una larghezza di banda molto stretta; ciò implica: un basso data-rate (lento trasferimento dei dati), impossibilità per il reader di leggere simultaneamente più tag RFID, scarsa robustezza del collegamento in presenza di un forte rumore elettronico ambientale e difficoltà a implementare una qualsiasi forma di crittografia del segnale trasmesso (sebbene il range di lettura estremamente corto di questi segnali potrebbe risultare di un qualche interesse per la realizzazione di canali di comunicazione sicuri).
Numerosi studi ed esperimenti affrontano il problema dell'efficienza delle onde ad alta frequenza (HF) per le comunicazioni con dispositivi impiantati nel corpo umano. Si è riscontrato che le onde nel range di frequenze che va da 1 a 20 MHz non subiscono un'attenuazione significativa nei tessuti umani e dunque sono adatte allo scopo.
Dall'analisi dello stato dell'arte nel settore, si osserva che l'accoppiamento induttivo in HF (da 13,56 MHz in giù) è attualmente uno dei metodi più comuni per inviare, in modalità wireless, alimentazione e dati dal reader verso il dispositivo RFID impiantato all'interno del corpo umano.
La progettazione di sorgenti di alimentazione di dimensioni millimetriche e sub-millimetriche che operano a 2 MHz e 20 MHz, per impianti neurali basati sull'accoppiamento induttivo, è stata dimostrata fattibile.
L'acquisizione dell'energia, da parte di dispositivi impiantati tramite accoppiamento induttivo, è stata eseguita con successo per varie applicazioni, ad esempio, per la registrazione dei segnali neurali da assoni usando il sistema di telemetria impiantato occupante una superficie di 4 x 6 mm^2 e funzionante a 2 MHz. Lo stesso sistema è stato anche usato per un apparato wireless impiantabile di micro-stimolazione neurale, o ancora per la sostituzione di fotorecettori difettosi nei pazienti, attraverso l'impianto di un chip retinico che realizzi il collegamento tra l'antenna extra oculare e quella intraoculare ad una frequenza compresa tra 1 e 10 MHz.
Dispositivi RFID operanti in *Ultra-High Frequency* (UHF) offrono larghezze di banda significativamente superiori rispetto ai dispositivi LF o HF. Questo permette, ad esempio, di raggiungere velocità di trasferimento dati elevate e l'incorporazione di protocolli crittografici per la privacy per la trasmissione senza fili al fine di proteggere le informazioni.
Inoltre, utilizzando onde elettromagnetiche UHF, può essere raggiunto un elevato livello di miniaturizzazione dei chip RFID (compresa l'antenna).

Tuttavia le onde UHF possono essere problematiche per gli impianti RFID umani, a causa dei seguenti motivi:

- i campi UHF e microonde sono fortemente attenuati dall'acqua (che è il costituente primario di tessuti umani) e di conseguenza una soluzione RFID passiva permette un raggio di comunicazione molto limitato (in genere meno di 1 m);
- il campo UHF trasmesso da un interrogator situato al di fuori del corpo umano è soggetto a molteplici riflessioni dovute ad oggetti ambientali, che creano interferenze e zone d'ombra indesiderate (in cui un chip RFID non è rilevabile dal dispositivo di lettura), nonché picchi o *hot spot* nella distribuzione del campo;
- le frequenze HF (in particolare 2.45 GHz) possono essere pericolose per l'uomo per esposizione a lungo termine e/o quando sono coinvolte alte densità elettromagnetiche.

Nella banda UHF, il corpo umano, composto essenzialmente da acqua, ossa e tessuti, può essere visto come un canale di propagazione elettromagnetica ad elevato *scattering* e dissipativo, nel quale si verificano riflessioni multiple (*multi-path*) e una forte attenuazione.
In particolare l'impedenza d'ingresso e il diagramma di radiazione dell'antenna transponder possono essere legati alla posizione dell'antenna impiantata all'interno del corpo.
Al fine di effettuare un'analisi dell'efficienza di comunicazione wireless in UHF e per analizzare le caratteristiche elettromagnetiche di antenne inserite all'interno del corpo umano, deve essere elaborato un modello elettromagnetico realistico dello stesso (con i suoi vari tessuti e geometrie). Questo permetterà la progettazione di un sistema di comunicazione wireless affidabile.

6. Sistema RFID per il monitoraggio continuo del glucosio nel sangue

Il sistema presentato in questo paragrafo è un *System-on-chip* (SoC) impiantabile, in tecnologia RFID dotato di un sensore per il monitoraggio del glucosio nel sangue [9].
Il chip in questione comprende un tag RFID ad alta frequenza, l'interfaccia per la gestione di un bio-sensore, nonché gli elettrodi. Il sensore rileva il livello di zucchero nel sangue e questo segnale viene convertito in dati digitali, che vengono crittografati e trasmessi ad un lettore RFID posto a contatto con la pelle.
Per misurare i deboli segnali di corrente, il chip è stato progettato con un circuito di lettura della corrente, uno splitter di corrente, un ADC e un potenziostato.
Il circuito di lettura della corrente è implementato con la tecnologia CDS (*Correlated Double Sample*) per ridurre il rumore 1/f e l'offset dell'op-amp. In tal modo il sistema può misurare deboli correnti nell'intervallo 10 fA-100 pA.
Tradizionalmente, le persone con diabete di tipo I misurano il livello di zucchero nel sangue mediante un test eseguito con una leggera puntura del dito. Ma questo tipo di misura non è in grado di garantire che non vi sia alcuna escursione del livello di zucchero nel sangue di una persona, al di fuori del range fisiologico normale.
La ricerca mostra che il monitoraggio continuo della glicemia può contribuire a ridurre più del 40% dei sintomi associati al diabete. Un approccio promettente al monitoraggio continuo del glucosio consiste nell'impiantare un sensore di glucosio, insieme ad un micro-sistema wireless, nel corpo umano.
Affinché questo metodo risulti efficace, un ruolo chiave è rivestito da un piccolo dispositivo impiantabile con un sensore di glucosio accurato e veloce, affiancato da un modulo per la comunicazione a radiofrequenza efficiente. Inoltre, dal momento che il livello di glucosio

viene trasmesso ad un ricevitore al di fuori del corpo in modalità wireless, la privacy del paziente deve essere protetta.
Questo apparato, proposto da due gruppi di ricerca della *Fudan University* di Shanghai e della *Michigan State University* negli USA, propone un sistema impiantabile *on chip* (SoC), che include un tag RFID, operante ad alta frequenza (HF, 13.56 MHz), un'interfaccia per un sensore di glucosio ed elettrodi *on chip*.
L'unità di acquisizione dati (DAQ), compresa nell'interfaccia del biosensore, può funzionare in quattro diversi range, attraverso il cambiamento della frequenza di lavoro ed è in grado di misurare segnali di corrente deboli nell'intervallo 10 fA-100 pA.
È stato progettato un sistema RFID HF passivo basato sul protocollo ISO/IEC 15693 ed inoltre nel chip è implementato l'algoritmo di crittografia denominato *Hummingbird* per crittografare i dati prima di inviarli al lettore RFID wireless.
Il tag RFID con sensore di glucosio è composto da una interfaccia per la comunicazione a radiofrequenza (RF), un'interfaccia per il bio-sensore e una circuiteria per l'elaborazione digitale del segnale. Il tag ad alta frequenza funziona passivamente e ricava potenza dall'energia RF irradiata dal lettore. La banda ad alta frequenza è stata selezionata, in quanto si tratta di una banda di frequenze dedicata ad applicazioni industriali, scientifiche e mediche (ISM) ben più adeguata per impianti *in vivo* rispetto alla banda UHF.
L'interfaccia RF rettifica e trasforma il segnale ricevuto nella tensione di alimentazione DC e fornisce energia per la *baseband* (circuiti di elaborazione digitale) e per l'Interfaccia del bio-sensore.
Nell'interfaccia per il funzionamento del bio-sensore, un *current splitter* è progettato per fornire la corrente di riferimento necessaria alla calibrazione del guadagno e per definire i valori di corrente nei diversi range di rilevamento, allo scopo di effettuare dei test.
Il modulo di acquisizione dati, comprendente un potenziostato e un circuito di lettura, è progettato per rilevare, amplificare e trasformare la corrente di reazione (che veicola le informazioni sulla concentrazione di zucchero nel sangue) in un segnale di tensione. Un circuito elettronico (Analog to Digital Converter, ADC) converte questa tensione in un segnale digitale e lo trasmette al modulo per l'elaborazione dei dati.
In questo modulo, i dati saranno criptati da un motore crittografico, prima di essere inviati al lettore RFID.
Il chip sensore, dotato di tag, funziona secondo il seguente flusso di lavoro:

- il lettore esterno al corpo interroga l'etichetta-sensore, usando comandi conformi al protocollo ISO / IEC 15693;
- la *baseband* azzera i dati quando riceve il segnale di *power-on-reset* (POR);
- l'interfaccia del bio-sensore inizia l'auto-calibrazione quando riceve il segnale di "*power ready*" dal *frontend*, che significa che il bio-sensore ha abbastanza potenza per funzionare correttamente;
- quando il segnale di "*inventory*" viene ricevuto dal lettore, la *baseband* abilita l'interfaccia del bio-sensore;
- sotto il controllo del potenziostato, il sensore dà inizio alla reazione. La corrente viene misurata e i dati convertiti vengono salvati nella memoria. Allo stesso tempo, la *baseband* disabilita l'interfaccia del bio-sensore per risparmiare energia;
- la circuiteria crittografa i dati memorizzati e poi li invia al lettore quando il tag sensore riceve il comando *"send"* dal lettore;
- il sistema ripete i passaggi precedenti durante ogni ciclo di funzionamento.

Nell'interfaccia per il funzionamento del bio-sensore, un *current splitter* è progettato per fornire la corrente di riferimento necessaria alla calibrazione del guadagno e per definire i valori di corrente nei diversi range di rilevamento, allo scopo di effettuare dei test.
Il modulo di acquisizione dati, comprendente un potenziostato e un circuito di lettura, è progettato per rilevare, amplificare e trasformare la corrente di reazione (che veicola le informazioni sulla concentrazione di zucchero nel sangue) in un segnale di tensione. Un ADC converte questa tensione in un segnale digitale e lo trasmette al modulo per l'elaborazione dei dati.

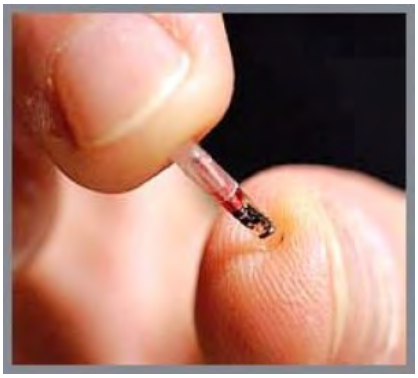

Figura 2 - *Dimensioni reali del GlucoChip*

Le ricerche sempre più estensive in questo settore hanno condotto alla realizzazione di un sensore di glucosio prototipale [9] (cfr. Fig. 2), da utilizzare in combinazione con un microchip RFID impiantabile, dotato di un biosensore per misurare i livelli di glucosio nel corpo.

7. Sistema RFID per il monitoraggio in remoto del battito cardiaco

Un sensore impiantato permette di ottenere i dati dall'interno del corpo, senza avere a che fare con fili o tubi, che penetrano la pelle. Questo riduce la possibilità di infezione, che è tra le maggiori cause di mortalità.
Alcuni dei segnali biologici, come il battito cardiaco, ECG, possono essere misurati mettendo il tag anche esternamente. Il lavoro svolto dai ricercatori in questo caso si è concentrato sul rilevamento del battito e la relativa trasmissione [10].
Il flusso di sangue attraverso le vene può essere rilevato da un sensore posizionato in una parte del corpo adatta, per esempio sul polso. Il blocco sensore converte il flusso di sangue nel segnale di battito cardiaco, che è l'equivalente elettrico del segnale fisiologico. Questa conversione può essere realizzata con l'ausilio di un sensore di pressione appositamente progettato.
Il blocco di elaborazione consiste nell'unità di elaborazione del segnale del battito cardiaco e in una unità di generazione del codice identificativo. I segnali rilevati dai sensori sono molto deboli e hanno bisogno di essere amplificati.
I segnali rilevati contengono anche componenti di rumore a larga banda, a causa delle altre attività biologiche del corpo e questi rumori possono essere eliminati utilizzando appositi circuiti. Il blocco di elaborazione del segnale comprende anche i circuiti per digitalizzare il segnale cardiaco.

Il segnale risultante fornisce la frequenza cardiaca dell'essere vivente in cui il tag viene impiantato.
Ogni tag ha un proprio codice ID, che viene trasmesso per fini identificativi. Il codice è memorizzato in una ROM, la cui dimensione dipende dal numero di cifre del codice ID. Il codice ed il segnale cardiaco digitalizzato vengono inviati al blocco di trasmissione tramite opportuni circuiti digitali.
Il segnale elaborato è trasmesso al lettore. Per la realizzazione di un modulatore digitale a bassa tensione e bassa potenza, si può adottare la modulazione BASK (*Binary Amplitude Shift Keying*).
Per implementare la modulazione BASK, si utilizza la commutazione ON/OFF di un loop di un oscillatore ad anello. Per applicazioni biomediche si preferiscono tag passivi, come in questo caso. Essi non hanno la batteria incorporata: la potenza necessaria per il tag viene fornita dal lettore attraverso l'accoppiamento magnetico.

8. Sensore RFID per il rilevamento precoce dell'infarto miocardico

Le malattie cardiovascolari sono la principale causa di morte nei paesi sviluppati. Milioni di persone muoiono ogni anno a causa di malattie cardiovascolari. Il tipo più comune di malattia cardiovascolare è l'infarto miocardico.
Questo evento, comunemente noto come attacco cardiaco, si verifica quando l'afflusso di sangue ad una parte del cuore è interrotto. In molti casi, ciò si verifica a causa dell'occlusione (blocco) di un'arteria coronaria a seguito della rottura di una placca aterosclerotica vulnerabile; questa placca si forma a causa di un accumulo instabile di lipidi (come il colesterolo) e di globuli bianchi (soprattutto macrofagi) sulla parete di un'arteria. La conseguente ischemia (limitato afflusso di sangue) e carenza di ossigeno, se non curata per un periodo sufficiente, può causare danni e / o la morte (infarto) del tessuto muscolare cardiaco (miocardio).
I sintomi classici da infarto miocardico acuto includono: improvviso dolore al petto (di solito si propaga verso il braccio sinistro o sul lato sinistro del collo), respiro corto, nausea, vomito, palpitazioni, sudorazione e ansia.
Tuttavia, circa un quarto di tutti gli infarti del miocardio sono silenziosi e senza dolore toracico o altri sintomi. Il problema è che, dopo un infarto miocardico silente, le persone non avvertono i loro servizi medici di emergenza, per il semplice fatto che non si sono resi conto di aver sperimentato un attacco di cuore. A volte le persone che hanno questi attacchi non sono in grado di riconoscere i sintomi classici e, senza avere informazioni sull'infarto, sono sottoposti al trattamento medico sbagliato.
La diagnosi dell'infarto miocardico è tradizionalmente effettuata integrando la storia della malattia che si manifesta con un esame fisico e con i risultati dell'elettrocardiogramma, nonché i *markers* cardiaci (esami del sangue per la valutazione dei danni alle cellule del muscolo cardiaco).
Vi è certamente una forte necessità di una più efficace diagnosi precoce delle malattie cardiache. Inoltre, gli strumenti pertinenti, progettati per l'esecuzione di tali misurazioni sono per lo più limitati all'uso in laboratorio e non sono disponibili negli ambienti in cui è più probabile che si debba affrontare la cura di un attacco di cuore, come in un pronto soccorso o in ambulanza.
Un gruppo di ricercatori russi della *National Research Nuclear University* ha sviluppato un dispositivo [11] che potrebbe aumentare significativamente le probabilità di riconoscimento

dell'infarto miocardico acuto. La novità principale è la grande mobilità del sistema di diagnosi proposto e le sue dimensioni; entrambi questi aspetti costituiscono un notevole miglioramento rispetto alle procedure previste dai moderni metodi di diagnosi.
Nel corso degli ultimi 20-30 anni, numerosi studi hanno convalidato l'efficacia dell'analisi della saliva come mezzo per misurare la quantità di proteine nel flusso sanguigno.
Queste ricerche, in tutto il mondo e in particolare in Russia, hanno permesso di compilare una lista di specifici biomarcatori cardiaci. Questi marcatori biochimici sono stati rilevati in un campione di saliva prelevato ad una persona, che ha un attacco di cuore in corso o in imminente pericolo di attacco. I vantaggi dell'analisi della saliva rispetto a tutti gli altri metodi di diagnosi sono evidenti.
L'analisi della saliva non è invasiva, è semplice, sicura, non stressante e indolore. Il metodo descritto è già utilizzato con successo negli sviluppi del team di ricerca della *Texas University*, che ha utilizzato l'analisi della saliva nello sviluppo di un sensore cardiaco.
Il meccanismo di analisi della saliva per determinare l'imminente infarto è fondamentale per il dispositivo descritto. Il gruppo di ricerca ha sviluppato un sensore per la saliva più piccolo possibile, progettato per rilevare gli specifici biomarcatori cardiaci presenti nella saliva.
L'idea principale è quella di implementare questo sensore all'interno di un impianto dentale, che si trova sempre nella bocca del paziente e quindi in costante contatto con la saliva.
L'aspetto particolare di questo sensore consiste nel fatto che esso è integrato con un chip RFID. L'intera apparecchiatura è racchiusa all'interno di una resina, che protegge il tag dal cibo e dalla saliva. Il sensore ottiene l'accesso alla saliva solo su richiesta attraverso piccoli tubi. Il tag RFID contiene una batteria di lunga durata e il chip, il quale non solo controlla l'accesso alla memoria, ma viene utilizzato anche per eseguire le analisi della saliva.
In questo apparato, il reader RFID è implementato sotto forma di bracciale con il microprocessore incorporato. Il bracciale è usato per generare il segnale di allarme in caso di attacco cardiaco.
Il chip integrato nel tag RFID memorizza i dati della precedente analisi della saliva nella memoria di solo 256 bit. Ogni bit codifica la presenza di almeno un biomarker cardiaco. Attualmente, solo 26 reazioni sono implementate nel sistema, ma in futuro il numero di tali reazioni può aumentare, dal momento che gli studi nel settore sono ancora in corso ed in continua evoluzione. Se il bit corrispondente ad una certa reazione vale 1, significa reazione positiva sul particolare biomarker cardiaco, se vale 0 la reazione è negativa.
Il lettore RFID interroga periodicamente il microchip e, in base all'analisi dei dati ricevuti, stabilisce se i risultati possono essere considerati come sintomo di un attacco di cuore imminente. Nel caso il risultato sia positivo o sospetto abbastanza, il braccialetto informa la persona dell'elevato rischio di attacco di cuore. La decisione sulla segnalazione dell'allarme è stabilita dal chip incorporato nel reader.
Lo stesso chip memorizza le informazioni sullo stato di carica della batteria del tag RFID e anche il numero di test rimanenti, prima della sostituzione della cartuccia per le analisi. Attualmente la cartuccia può funzionare per un mese senza bisogno di sostituzione, che sembra essere una durata ragionevolmente lunga.
Il braccialetto, inoltre, memorizza anche informazioni sul paziente come dati personali e speciali trattamenti raccomandati. In caso di attacco di cuore le istruzioni possono anche essere visualizzate su un display a LED, il quale può risultare utile sia per il paziente, sia per i soccorritori se il paziente è incosciente.

Il bracciale ha anche funzione di controllo remoto, per chiedere al sensore di saliva un'analisi immediata ed in tempo reale, in caso di necessità; infine esso è dotato di GPS per fornire agli ospedali la localizzazione immediata di pazienti sofferenti e la loro condizione.
Come già detto, il sistema di analisi è incapsulato all'interno di un impianto dentale (tipicamente una protesi ortodontica con una vite in titanio per l'ancoraggio all'osso); nei casi in cui l'impianto non sia la migliore soluzione, è possibile installare il sensore della saliva mediante dei semplici ponti dentali.

9. Sensore RFID per il monitoraggio di segnali neurali

Un gruppo di ricercatori del *Department of Electrical Engineering* e *Department of Computer Science and Engineering* della *University of Washington* hanno sviluppato un sistema [12], denominato **NeuralWISP** (*Neural Wireless Identification and Sensing Platform*), in grado di funzionare grazie alla energia raccolta dalle onde a radiofrequenza. Il NeuralWISP è compatibile con i lettori RFID commerciali e funziona fino alla distanza di lettura di 1 m.
Il sistema monitora il segnale neurale e trasmette periodicamente la densità di *spike* neurali rilevati, in una finestra temporale definibile dall'utente.
Siccome il cablaggio transcutaneo comporta un rischio significativo di infezione, è auspicabile che un'interfaccia neurale comunichi e riceva energia in modalità wireless.
Nei sistemi preesistenti, la funzionalità di comunicazione wireless è stata ottenuta utilizzando un collegamento induttivo a campo vicino per la trasmissione di energia e dati.
Tuttavia questi sistemi richiedono che la bobina esterna si trovi a pochi centimetri della bobina interna. Una interfaccia neurale wireless, con una distanza di lettura di 1 m o più, consentirebbe la rimozione dell'*interrogator* dalla testa e permetterebbe il posizionamento di tali interfacce wireless su piccoli animali, non in grado di trasportare l'hardware di lettura, come, ad esempio, i topi.
Il sistema progettato [12] ha una interfaccia neurale wireless, che raccoglie la potenza necessaria al funzionamento dalle onde a radio-frequenza (RF), irradiate da un lettore RFID UHF standard commerciale. Il sistema funziona a una distanza massima di 1 m dal lettore. L'apparecchiatura registra il conteggio dei picchi in una finestra temporale programmabile (tipicamente da 1 a 10 s) e successivamente trasmette il conteggio dei picchi al reader come parte del numero di identificazione del tag, che il lettore è progettato per acquisire.
Questo strumento fornisce al neuroscienziato un metodo wireless di registrazione della densità dei picchi di attività neurale, senza necessità di batteria, ogni volta che il cervello esegue vari compiti o vengono presentati dei particolari stimoli.
Il sistema NeuralWISP è composto da un tag RFID UHF completamente passivo, che utilizza un microcontrollore a 16 bit, di tipo general-purpose per il rilevamento, la computazione e la comunicazione RFID. L'uso di un microcontrollore programmabile permette all'apparato di essere facilmente configurato per diverse applicazioni, tra cui la misurazione della temperatura, il livello di illuminazione, deformazione, e l'accelerazione.
In applicazioni di monitoraggio, le uscite analogiche del sensore cambiano lentamente e quindi permettono una misurazione periodica, a bassa frequenza (da 1 a 50 Hz).
Tuttavia, una frequenza di campionamento molto elevata (almeno 8 kHz) è necessaria per rilevare i picchi neurali. Il raggiungimento di questa frequenza di campionamento, tenendo conto dei vincoli di potenza di un tag RFID, non è possibile con i microcontrollori general-purpose attualmente disponibili.

Per ridurre al minimo il consumo medio di corrente, è stato progettato un rilevatore di picco analogico tempo-continuo, che generi un segnale di interrupt, che comunichi al microcontrollore l'eventualità del verificarsi di un picco.
Questo fa sì che il microcontrollore rimanga in una modalità *sleep* a basso consumo durante i periodi di inattività e "si svegli" per elaborare il conteggio dei picchi o per comunicare con il lettore RFID. Il microcontrollore conta i picchi durante una finestra temporale programmabile e viene resettato dopo che il conteggio è stato trasmesso al lettore.

10. Sensore RFID per il monitoraggio della pressione intraoculare

Il glaucoma è una malattia cronica, non curabile. Essa colpisce tipicamente gli anziani e le persone con una storia familiare, ma si è anche osservato che pazienti sempre più giovani sviluppano la malattia a causa di altre patologie legate allo stile di vita.
Nel glaucoma, l'aumento della pressione intraoculare o fluttuazioni della pressione dinamica causano danni al nervo ottico. La degenerazione della malattia porta alla perdita della vista nel tempo ed eventualmente alla cecità, se non trattata adeguatamente.
Purtroppo non è possibile ripristinare un nervo ottico danneggiato o correggere la vista del paziente. Pertanto l'obiettivo primario di qualsiasi terapia, sia farmacologica, sia chirurgica è quello di ridurre o controllare la pressione intraoculare.
Ma la riduzione e il controllo della pressione intraoculare deve fare i conti con le pesanti limitazioni dell'attuale stato dell'arte dei metodi di misura della pressione intraoculare. I metodi attuali consentono solo la misura di tale parametro presso uno studio oculistico, poiché la procedura deve essere eseguita da uno specialista. Ciò comporta misurazioni molto meno frequenti del necessario per un adeguato monitoraggio e cura del paziente.
Attualmente non sono possibili misurazioni autonome da parte del paziente e misurazioni nelle normali condizioni di vita di tutti i giorni. Questo si traduce spesso in una bassa aderenza alla terapia da parte di molti pazienti, che causa un'ulteriore ed evitabile progressione della malattia.
Non è possibile ottenere informazioni cruciali sulla pressione oculare dinamica e le sue fluttuazioni. Ai fini curativi è importante anche conoscere la variabilità di questo parametro tra una visita ambulatoriale e la successiva, nonché nel corso di una singola giornata. Quindi i risultati di una terapia scelta non possono essere consultati in modo tempestivo e eventuali aggiustamenti della terapia, in molti casi, vengono notevolmente ritardati. Questo è il motivo per cui una determinata terapia non funziona e il paziente è costretto a constatare un ulteriore progressivo peggioramento della vista.
In questo panorama sono stati condotti numerosi studi per lo sviluppo di tecnologie per il monitoraggio della pressione oculare in tempi rapidi e con modalità facilmente eseguibili direttamente dal paziente stesso [13-14].
In particolare, i sistemi sviluppati (cfr. Fig. 3) sono costituiti da un micro sensore impiantabile per il rilevamento della pressione, una periferica esterna, che trasferisce energia al micro sensore e che è responsabile della lettura e memorizzazione dei dati. I sistemi sono, inoltre, dotati anche di un modulo GSM, che può essere collegato con il dispositivo palmare per il trasferimento dei dati di misura ad un database, al quale può accedere un medico oculista, per ottenere informazioni sullo stato della malattia.

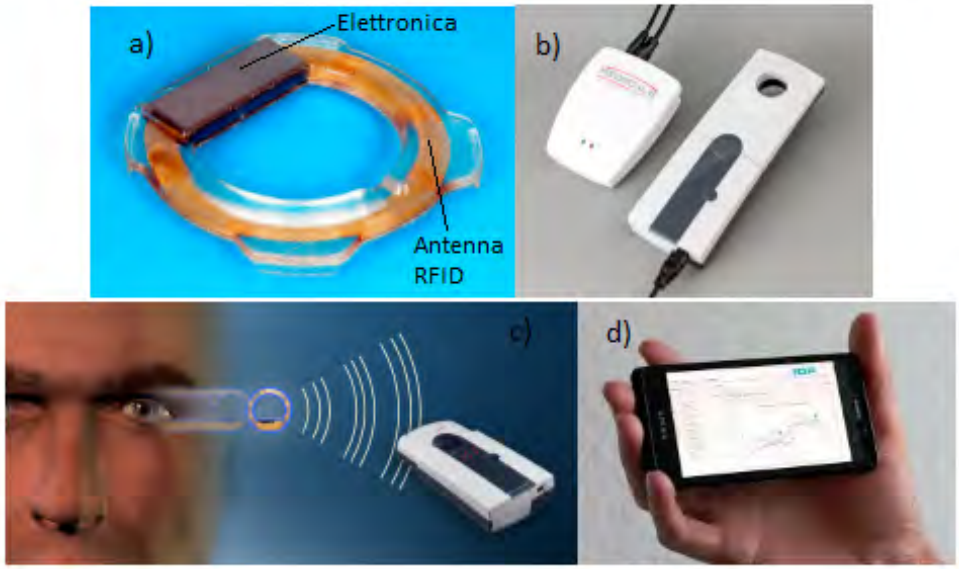

Figura 3 - *a) sensore di pressione intraoculare impiantabile con antenna ed elettronica; b) dispositivo palmare esterno per l'alimentazione dell'impianto, la lettura dei dati e l'immagazzinamento, insieme al modulo GSM per il trasferimento al database; c) misurazione wireless attraverso la tecnologia RFID; d) applicazione per smartphone con visualizzazione dei dati del paziente*

Tra gli sviluppi futuri di questa applicazione, si prevede di dare la possibilità al paziente di avere un accesso limitato a questi dati, tramite un'applicazione per smartphone, al fine di consultare i dati o consentire la comunicazione tra l'oculista e il paziente.

11. Sensore Tracking RFID della posizione del tubo endotracheale

Il posizionamento non corretto del tubo endotracheale durante l'intubazione rappresenta un grave rischio per la salute dei pazienti sottoposti ad operazioni chirurgiche o in grave pericolo di vita.
Sebbene esista un'ampia varietà di tecniche, che vengono utilizzate per confermare il corretto posizionamento del tubo, una radiografia del torace è solitamente impiegata per la verifica definitiva. La tecnologia RFID, in cui un lettore emette un segnale di interrogazione e "ascolta" il segnale riflesso da un tag, può essere utile nel valutare la posizione del tubo endotracheale.
Da tempo è stato approvato l'uso della tecnologia RFID negli esseri umani, come strumento sicuro ed efficace in numerose applicazioni.
Un'intubazione endotracheale non eseguita correttamente può portare a una serie di problemi significativi, dei quali i due più gravi sono l'intubazione esofagea e l'inserimento del tubo ad una profondità di inserimento non corretta.
Il rilevamento tempestivo e la correzione di questi problemi è dunque di importanza vitale. Sebbene i raggi X restino il *gold standard* per la conferma della adeguata profondità di inserimento del tubo, il paziente viene sottoposto a tale monitoraggio solo una volta al giorno: questo potrebbe non essere sufficiente per rilevare la migrazione del tubo, che può spesso verificarsi durante la cura ed osservazione del paziente in terapia intensiva.

In questo contesto, è stato sviluppato un sistema [15], che utilizza un tag RFID, fissato ad un tubo endotracheale orale di diametro interno 6 mm, come mostrato in Fig. 4.

Figura 4 - *Tag RFID collegato appena al di sopra del palloncino terminale del tubo endotracheale.*

Il tag cilindrico include un'antenna operante alla frequenza di 134,2 KHz e un microchip: il tutto racchiuso in un contenitore di 12 mm di lunghezza e 2.2 mm di raggio.
Il dispositivo è allineato parallelamente all'asse longitudinale del tubo endotracheale, lungo il suo bordo anteriore. Il reader RFID, anch'esso operante ad una frequenza di 134,2 KHz, è un dispositivo portatile con antenna incorporata, di dimensioni simili a quelle di un telecomando.
Il lettore, alimentato da una batteria standard da 9 V, è dotato un display LCD che indica la relativa vicinanza al tag RFID. Questo tag restituisce un picco di segnale man mano che il lettore si avvicina a ciascuna estremità e un minimo relativo quando il lettore è allineato con la parte centrale del tag.
Il lettore impiegato è stato progettato per rilevare esattamente la posizione del tag con una precisione di pochi millimetri, purché il lettore si trovi entro 4-5 cm dal tag.
L'intubazione *in vitro* è stata testata su un manichino, delle dimensioni di un adulto, costituito da strutture orali e laringee anatomicamente corrette. Il tubo endotracheale è posto nella trachea del manichino. Poiché il segnale del tag RFID è più intenso a ciascuna delle estremità longitudinali, il lettore RFID è stato usato per delimitare la posizione del tag RFID. Ciò può essere fatto passando il lettore RFID sul manichino e verificando la presenza di due posizioni, in corrispondenza delle quali si rileva un massimo del segnale emesso dal tag. Questa procedura viene ripetuta nella direzione opposta, come misura di conferma.
Anche a seguito della variazione della profondità di inserimento del tubo endotracheale, il reader riesce ugualmente ad individuare correttamente il tag RFID sul tubo.
I test effettuati hanno dimostrato le potenzialità della tecnologia RFID, finalizzata alla realizzazione di un semplice ed immediato monitoraggio della posizione del tubo endotracheale. L'utilizzo di questa semplice tecnologia potrebbe portare un netto miglioramento per le condizioni di lavoro di medici, infermieri e personale di assistenza nella cura di pazienti sottoposti a terapia intensiva.
Inoltre l'utilizzo della tecnologia RFID in questo ambito può diminuire la frequenza delle radiografie necessarie, può dare la possibilità di individuare immediatamente tubi non posizionati nel modo corretto e correggerne la posizione.
Il lettore e il tag funzionano a frequenze elettromagnetiche nella gamma delle onde a bassa energia, eliminando efficacemente il rischio di interazione dannosa dei campi con le cellule dell'organismo.

Inoltre, il tag stesso, essendo passivo, non ha attività elettromagnetica "residua" e produce solo un segnale in risposta all'interrogazione del lettore RFID.
I segnali riflessi dal tag non sono alterati da impianti in materiale plastico e quindi un'accurata protezione del tag, con package di questo materiale, non influisce negativamente sulle prestazioni. Inoltre, le piccole dimensioni del tag assicurano che le dimensioni del tubo non subiscano cambiamenti significativi.
Una potenziale limitazione di questa tecnica è rappresentata dall'interferenza con altri oggetti metallici, che possono essere impiantati nella regione del collo: uno strato metallico tra il lettore e il tag può essere in grado di schermare il segnale proveniente dall'interrogator, rendendo impraticabile la comunicazione.
Per quanto riguarda le interferenze con altri dispositivi elettronici presenti nell'unità di terapia intensiva o in sala operatoria, poiché il sistema RFID funziona a bassa frequenza (134.2 KHz), le ampiezze dei segnali coinvolti non influiscono apprezzabilmente su altri apparecchi vicini.

12. Conclusioni

In tempi recenti si è fatta sempre più pressante la richiesta, in ambito biomedico, di dispositivi meno invasivi possibile, per il controllo delle condizioni di salute di un paziente e, di conseguenza, per il monitoraggio di parametri vitali come, ad esempio, il battito cardiaco o la concentrazione di determinate sostanze nel sangue.
Questo è il motivo per cui lo sviluppo di apparecchiature che fanno uso della tecnologia senza fili, in generale, ha subito una forte accelerazione. Infatti è possibile rendersi conto della sterminata schiera di applicazioni e ricerche, riferite al settore medico, che, per soddisfare l'obiettivo primario, consistente nella non-invasività delle tecniche di indagine, fanno ricorso alle diverse tecnologie wireless ad oggi presenti sul mercato.
In particolare la tecnologia RFID, sebbene, in origine, fosse nata fondamentalmente per l'identificazione e il monitoraggio delle merci, nei vari comparti della catena di produzione (*supply chain*) di un certo prodotto, in realtà, si è rivelata una tecnologia che molto bene si presta al progetto di applicazioni orientate all'identificazione della persona, al monitoraggio, mediante sensori appositi, dei parametri vitali ed, in generale, al miglioramento della qualità della vita di pazienti, anziani e persone ospedalizzate.
Nelle applicazioni descritte in questo lavoro, tra le problematiche più significative, legate a questo tipo di tecnologia, bisogna, innanzitutto, tener conto della biocompatibilità dei materiali di fabbricazione dei tag, eventualmente impiantati nel corpo umano. Difatti l'utilizzo di materiali non appropriati potrebbe portare all'insorgenza di infezioni dei tessuti. Ma in tal senso, la tecnologia dei materiali ha fatto e continua a fare notevoli passi in avanti.
Un altro aspetto critico legato all'uso di dispositivi RFID, certamente non trascurabile, riguarda gli effetti che si potrebbero manifestare sul corpo umano a seguito dell'esposizione a campi elettromagnetici ad alta frequenza. Infatti, essendo l'organismo umano composto, per la maggior parte, da acqua e materiale liquido, tali elementi, come è noto, sono in grado di assorbire l'energia trasportata dalle onde elettromagnetiche ed un assorbimento eccessivo di energia potrebbe avere conseguenze dannose sull'organismo.
Strettamente legato all'aspetto di assorbimento dell'energia elettromagnetica da parte del corpo umano, è anche il problema dell'attenuazione che i segnali RF subiscono, propagandosi nei tessuti e rendendo così difficoltosa la comunicazione con gli apparati posti all'esterno.

Nonostante tutte queste difficoltà, la tecnologia RFID ha raggiunto un livello di maturità tale da poter essere tranquillamente utilizzata per l'impianto di "etichette intelligenti" all'interno del corpo, pienamente biocompatibili.
In definitiva, tenuto conto della grande versatilità di questa tecnologia e della miniaturizzazione sempre più spinta dei componenti e circuiti elettronici, è lecito attendersi, in futuro, lo sviluppo di applicazioni sempre più avanzate, per il monitoraggio di tutti quei parametri e grandezze, che possono contribuire in modi diversi al miglioramento delle condizioni di vita di malati, delle condizioni di lavoro degli addetti al settore sanitario e allo snellimento delle procedure sanitarie in generale.

Riferimenti Bibliografici

[1] Marani R., Perri A.G., "Una Introduzione alla Tecnologia RFID", La Comunicazione Note, Recensioni & Notizie, Istituto Superiore delle Comunicazioni e delle Tecnologie dell'Informazione, Ministero dello Sviluppo Economico, Roma, 2015, pp. 147-162.

[2] Perri A.G., "Fondamenti di Dispositivi Elettronici", Edizioni Progedit, ISBN 978-88-6194-080-2, 2017.

[3] Perri A.G., "Dispositivi Elettronici Avanzati", Edizioni Progedit, ISBN 978-88-6194-081, 2017.

[4] Want R., "An introduction to RFID technology", IEEE Pervasive Computing, vol. 5(1), pp. 25-33, 2006.

[5] Aubert H. "RFID Technology for Human Implant Devices", Comptes Rendus Physique, pp.1-19, 2011.

[6] Hamad-Schifferli K., Schwartz J.J., Santos A.T., Zhang S., Jacobson J.M., "Remote electronic control of DNA hybridization through inductive coupling to an attached metal nanocrystal antenna", Nature, vol. 415, pp. 152-155, 2002.

[7] Benchirouf A., Sowade E., Al-Hamry A., Blaudeck T., Kanoun O., Baumann R., "Investigation of RFID passive strain sensors based on carbon nanotubes using inkjet printing technology", Proceedings of 9th International Conference on Systems, Signals and Devices (SSD), pp. 1-6, 2012.

[8] "IEEE Standard for Safety Levels with Respect to Human Exposure to Radio Frequency Electromagnetic Fields, 3 kHz to 300 GHz," in *IEEE Std C95.1-1991* , vol., no., pp.1-76, 27 April 1992, doi: 10.1109/IEEESTD.1992.101091.

[9] Guan S., Gu J., Shen Z., Wang J.,, Huang Y., Mason A., "A Wireless Powered Implantable Bio-Sensor Tag System-on-Chip for Continuous Glucose Monitoring", Proceedings of 2011 IEEE Biomedical Circuits and Systems Conference (BioCAS), San Diego, USA, 2011.

[10] Sandeep Reddy M., Paily P.R., Rakesh Singh K., Genemala H., ManiKumar K., "Sensor Integration in an RFID tag for Monitoring Biomedical Signals"; Proceedings of the 2004 IEEE International Conference on Networking, Sensing & Control, pp. 1014-1020, 2004.

[11] Zhukov I. , Mikhaylov D. , Starikovskiy A., "Nano sensors integrated into dental implants for detection of acute myocardial infarction", International Journal of Emerging Trends & Technology in Computer Science, vol. 1(2), pp.85-87, 2012.

[12] Holleman J., Yeager D., Prasad R., Smith J.R., Otis B., "NeuralWISP: An Energy-Harvesting Wireless Neural Interface with 1-m Range", Proceedings of 2008 Conference on Biomedical Circuits and Systems (BioCAS), 2008.

[13] Araci, I., Su, B., Quake, S. *et al.* "An implantable microfluidic device for self-monitoring of intraocular pressure", Nature Medicine, vol.20, pp. 1074-1078, 2014.

[14] http://www.implandata.com/

[15] Reicher, J., Reicher, D. & Reicher, M., "Use of Radio Frequency Identification (RFID) Tags in Bedside Monitoring of Endotracheal Tube Position", Journal of Clinical Monitoring and Computing, vol. 21**,** pp.155-158, 2007.

Requisiti per una metodologia di Risk Assessment

Requirements for Risk Assessment Methodologies

Giancarlo Butti ♦, *Alberto Piamonte* □

♦ *ISACA Chapter Milano*
□ *ISACA Chapter Roma*

Sommario

Questo articolo, ispirato alla Guida tecnica di Open Group (Requirements for Risk Assessment Methodologies), fornendo un elenco di criteri di valutazione e di requisiti indispensabili chiaramente definiti, identifica e descrive quali siano le principali caratteristiche che una metodologia di valutazione del rischio deve possedere per essere efficace.

Ne vengono in questo modo indicate, sia le caratteristiche da individuare, che il valore che esse rappresentano.

Abstract

This paper, inspired by an Open Group Technical Guide, identifies and describes the key characteristics that make up any effective risk assessment methodology, thus providing a common set of criteria for evaluating any given risk assessment methodology against a clearly defined common set of essential requirements. In this way, it explains what features to look for when evaluating the capabilities of any given methodology, and the value those features represent.

1. Introduzione

Nel corso del tempo, sono stati sviluppati una varietà di metodi che consentono di analizzare e valutare i rischi presenti nell'ambito di un'organizzazione. Le esigenze alla base del metodo di valutazione scelto sono in genere molteplici e variabili, come risultato, l'approccio adottato varia ampiamente in termini di consistenza, accuratezza, ed utilizzo.

Questo articolo riprende una serie di concetti base dell'analisi dei rischi[1] e successivamente, *ispirandosi ad una analisi dell'organizzazione Open Group*[2]*,* si propone di individuare ed articolare gli aspetti più significativi e le caratteristiche delle metodologie utilizzate nella valutazione dei rischi.

2. Obiettivi

Nel complesso contesto della gestione del rischio, va sempre tenuto presente che il principale obiettivo dell'attività stessa è quello di individuare e stimare i livelli di esposizione ad eventi che possano causare danni di qualsiasi natura, in modo che i responsabili aziendali siano in grado di gestire questi rischi, accettandoli, o mitigandoli – con l'adozione di misure, ritenute sufficienti a ridurre la potenziale perdita ad un accettabile livello, oppure investendo in garanzie di carattere assicurativo.

Con questo in mente, le metodologie scelte dovranno, in particolare, garantire che:

- i risultati delle analisi possano, in modo affidabile, essere confrontati, sia tra diverse organizzazioni / scenari sia nell'ambito di una singola organizzazione,
- chi deve selezionare disponga di validi criteri di valutazione, in grado di differenziare tra le metodologie più efficaci e quelle meno efficaci,
- chi sviluppa le metodologie possa farlo tenendo conto di esigenze reali.

3. Utilizzo

Questo articolo può essere utilizzato per:

- valutare se una determinata metodologia di valutazione del rischio soddisfa le esigenze di gestione,
- dotarsi di elementi per poter differenziare le varie metodologie in modo per poter individuare quella che più da vicino soddisfi le nostre esigenze,

[1] Parte del testo, tabelle ed immagini sono tratte dal libro di G. Butti e A. Piamonte Governance del rischio - Dall'analisi al reporting e la sintesi per la Direzione ITER. 2020,

[2] Open Group è un consorzio globale nato con lo scopo del raggiungimento degli obiettivi di impresa attraverso gli standard tecnologici. é costituito da più di 800 organizzazioni include clienti, fornitori di sistemi e soluzioni, fornitori di strumenti, integratori, accademici e consulenti in più settori. Tra le quali: Fujitsu, HCL, Huawei, Intel, Micro Focus, Oracle, Accenture, Philips, Boeing, Capgemini, Microsoft, NASA, Google e molte altre

- verificare se una determinata metodologia valuta efficacemente il rischio (piuttosto che, semplicemente, alcuni sub-elementi di questo, quali ad esempio, il livello di implementazione dei controlli),
- costituire un riferimento per lo sviluppo o l'evoluzione di metodologie per la valutazione dei rischi.

4. Definizione dei termini

Questa guida utilizza la terminologia fornita in Open Group Standard Risk Taxonomy (O-RT), Version 2.0. Prendendo in prestito da quel documento, qui si applicano le seguenti definizioni chiave:

Risk	The probable frequency and probable magnitude of future loss.
Threat	Anything that can act in a manner resulting in harm to an asset and/or organization; for example, acts of God (weather, geological events, etc.), malicious actors, errors, failures.
Vulnerability	The probability that a threat event will become a loss event.[3]
Asset	Anything that may be affected in a manner whereby its value is diminished, or the act introduces liability to the owner. Examples include systems, data, people, facilities, cash, etc.

5. I limiti delle analisi dei rischi

Il primo aspetto da considerare è che l'analisi dei rischi non è una scienza esatta. Infatti, come evidenziato nel proseguo dell'articolo è opportuno considerare che il risultato che si desidera ottenere non è un valore preciso ed assoluto del rischio, ma una stima attendibile dello stesso.

Questo si traduce anche in una diversa modalità con cui rappresentare i risultati dell'analisi, che in luogo di valori assoluti si può esprimere, nel caso in cui si utilizzi una metodologia basata su valori quantitativi, con un range di possibili valori.

Nel caso si utilizzino metodologie basate su valori qualitativi, questi esprimono già un grado di incertezza, basato sulla scala di valori rappresentata nei termini.

Del resto, anche secondo la **ISO 31010** l'analisi dei rischi è caratterizzata da una serie di incertezze legate a numerosi fattori, fra i quali:

- le metodologie utilizzate,
- l'incertezza sul fatto che gli eventi futuri saranno simili al quelli del passato,
- la conoscenza imperfetta o incompleta delle minacce,
- le vulnerabilità ancora da scoprire,
- le dipendenze non riconosciute, che possono portare a impatti imprevisti.

[3] Questa definizione differisce da quelle date in altri documenti / standard

Analogamente il **NIST 800 30 R1** evidenzia che un'analisi del rischio non è uno strumento preciso ed è condizionata da:

- i limiti delle metodologie, degli strumenti e delle tecniche di valutazione specifici impiegati,
- la soggettività, la qualità e l'affidabilità dei dati utilizzati,
- l'interpretazione dei risultati della valutazione,
- le capacità e le competenze di quegli individui o gruppi che conducono le valutazioni.

6. Documentare l'analisi dei rischi

Per quanto sopra è opportuno identificare e documentare le fonti di incertezza sia in merito ai dati utilizzati, sia in merito alle metodologie.

Dovrebbero essere adeguatamente documentate:

- le scelte effettuate,
- la metodologia scelta,
- il momento,
- il perimetro di indagine,
- la completezza,
- l'accuratezza con cui si è svolta l'analisi dei rischi.

È infatti opportuno ricordare che un'analisi dei rischi viene effettuata su un ambiente dinamico ed in continua evoluzione e che quindi ognuno degli elementi fino a qui identificati può variare nel tempo, modificando il livello di rischio.

Al riguardo anche il momento del ciclo di vita, ad esempio di un progetto o di un'applicazione determina il livello di accuratezza della valutazione.

Diverso è infatti il caso di un'analisi condotta su un sistema in produzione, per il quale possono esistere anche dei dati storici in merito ad anomalie ed incidenti occorsi, rispetto ad un sistema in fase di progettazione.

7. Qualitativo o quantitativo

Nel precedente articolo[4] sono state presentate diverse metodologie, sia di natura qualitativa, sia quantitativa. Queste hanno pregi e limiti come già evidenziato e come ricorda anche il NIST nella Tabella 1.

Tabella 1. Vantaggi e svantaggi dei metodi quantitativi e qualitativi

Risk Analysis	Quantitative methods	Qualitative methods
Chosen advantages	Provides a measurement of the impacts' magnitude, which can be used in the cost-benefit analysis of recommended controls.	The main advantage of the qualitative impact analysis is that it prioritizes the risks and identifies areas for immediate improvement in addressing the vulnerabilities.
Chosen disadvantages	The disadvantage is that, depending on the numerical ranges used to express the measurement, the meaning of the quantitative impact analysis may be unclear, requiring the result to be interpreted in a qualitative manner. Additional factors often must be considered to determine the magnitude of impact. These may include, but are not limited to • An estimation of the frequency of the threat-source's exercise of the vulnerability over a specified time period (e.g., 1 year) • An approximate cost for each occurrence of the threat-source's exercise of the vulnerability • A weighted factor based on a subjective analysis of the relative impact of a specific threat's exercising a specific vulnerability.	The disadvantage of the qualitative analysis is that it does not provide specific quantifiable measurements of the magnitude of the impacts, therefore making a cost-benefit analysis of any recommended controls difficult.

Tratto da: NIST SP800 30

In realtà tali metodologie devono essere considerate non come fra loro alternative, ma con finalità diverse: vanno quindi utilizzate in funzione del risultato che si desidera ottenere, anche congiuntamente.

[4] G.Butti, A. Piamonte, Misurare la physical cyber security, Rivista - La Comunicazione - Note, Recensioni e Notizie 2016

Di fatto un'analisi dei rischi di tipo qualitativo può essere più veloce da svolgere e richiedere un numero più limitato di informazioni.

Può quindi essere molto utile per dare un inquadramento iniziale della situazione, ad esempio dei rischi relativamente ad una determinata categoria di asset.

In considerazione del costo e dell'impegno richiesto per un'analisi dei rischi puntuale, dopo questa prima valutazione ci si potrà concentrare, con analisi anche di tipo quantitativo, sulle aree di maggior rischio.

In tale contesto è particolarmente importante che, chi svolge l'analisi, sia cosciente dei limiti degli strumenti che decide di utilizzare, evitando di forzare l'uso di strumenti inadatti ai propri scopi.

Un errore questo che in realtà si riscontra molto frequentemente.

È emblematico in tale senso quanto sta accadendo con riferimento, ad esempio, al Regolamento Europeo sulla protezione dei dati (679/2016), il così detto GDPR.

Oltre a confondere l'analisi dei rischi (prevista obbligatoriamente da diversi articoli del GDPR, fra i quali il 24, 25 e 32 e per quanto riguarda gli aspetti di sicurezza in particolare da quest'ultimo) con la DPIA (articolo 35), moltissimi consulenti utilizzano per lo svolgimento dell'analisi quanto già messo in atto, ad esempio, la certificazione ISO 27001.

È evidente in questo caso l'errore del voler applicare una metodologia la cui finalità è valutare i rischi in merito alla sicurezza delle informazioni, ad un oggetto totalmente diverso, e cioè i diritti e le libertà delle persone fisiche: una notevole differenza.

La conoscenza delle possibilità e delle finalità degli strumenti utilizzati è quindi fondamentale e, come già indicato nei paragrafi precedenti, l'indicazione di tali informazioni dovrebbe essere parte integrante della documentazione a corredo dell'analisi dei rischi.

8. Informazioni per l'analisi dei rischi: metodi e fonti

Qualunque sia la metodologia utilizzata, l'analisi dei rischi si basa su una serie di informazioni che è necessario raccogliere e documentare.

Queste vanno dalla mappatura degli asset sui quali svolgere l'analisi, agli elementi che consentono di stimare l'impatto di un evento dannoso o la probabilità di accadimento dell'evento stesso.

È evidente che le varie metodologie di analisi dei rischi non fanno altro che mettere in relazione fra loro, secondo gli schemi e gli algoritmi che le contraddistinguono, le informazioni che sono state raccolte o elaborate; la qualità della valutazione dipenderà in larga misura dalla qualità delle informazioni raccolte, dalla loro completezza, aggiornamento, affidabilità, coerenza, etc..

Nessuna metodologia, per quanto complessa, può sopperire alla mancanza delle informazioni da cui partire; nemmeno metodologie basate sulla stima di esperti si sottraggono a questa regola.

Ci sono diverse pubblicazioni dedicate all'analisi dei rischi che suggeriscono modalità per la raccolta delle informazioni quali il **NIST 800 30** o la **Harmonized Threat and Risk Assessment (TRA) Methodology** realizzata fra gli altri dalla Royal Canadian Mounted Police.

Tabella 2. Tecniche per la raccolta di informazioni (Adattamento da NIST SP 800-30)

Questionnaire	To collect relevant information, risk assessment personnel can develop a questionnaire concerning the management and operational controls planned or used for the IT system. This questionnaire should be distributed to the applicable technical and nontechnical management personnel who are designing or supporting the IT system. The questionnaire could also be used during on-site visits and interviews.
On-site Interviews	Interviews with IT system support and management personnel can enable risk assessment personnel to collect useful information about the IT system (e.g., how the system is operated and managed). On-site visits also allow risk assessment personnel to observe and gather information about the physical, environmental, and operational security of the IT system. For systems still in the design phase, on-site visit would be face-to-face data gathering exercises and could provide the opportunity to evaluate the physical environment in which the IT system will operate.
Document Review	• Policy documents (e.g., legislative documentation, directives), • system documentation (e.g., system user guide, system administrative manual, • system design and requirement document, acquisition document), • security-related documentation (e.g., previous audit report, risk assessment report, system test results, system security plan, security policies) can provide good information about the security controls used by and planned for the IT system. • An organization's mission impact analysis or asset criticality assessment provides information regarding system data criticality and sensitivity
Use of Automated Scanning Tool	Proactive technical methods can be used to collect system information efficiently. For example, a network mapping tool can identify the services that run on a large group of hosts and provide a quick way of building individual profiles of the target IT system(s).

Sebbene riguardi le attività di audit, alcuni suggerimenti su metodi e fonti di informazioni possono essere mutuati anche dalla ISO 19011 che cita ad esempio:

- interviste,
- osservazioni,
- documenti,
- registrazioni,
- sintesi dei dati,
- indicatori di prestazione,
- informazioni sui piani di campionamento,
- informazioni di ritorno dai clienti e fornitori,
- indagini e misurazioni esterne,
- banche dati,
- siti web,
- simulazione,
- elaborazione di modelli, etc..

Alcune di queste informazioni sono oggettive e relativamente semplici da individuare, come ad esempio l'elenco degli asset (anche se sarà possibile decidere il livello di granularità da utilizzare); se l'analisi dei rischi riguarda un sistema IT è indispensabile una profonda comprensione dell'ambiente di elaborazione ed al riguardo è utile rifarsi alla già citata norma NIST 800 30.

Tabella 3. Informazioni in ambito ICT (NIST 800 30)

Hardware
Software
System interfaces (e.g., internal and external connectivity)
Data and information
Persons who support and use the IT system
System mission (e.g., the processes performed by the IT system)
System and data criticality (e.g., the system's value or importance to an organization)
System and data sensitivity.
The functional requirements of the IT system
Users of the system (e.g., system users who provide technical support to the IT system; application users who use the IT system to perform business functions)
System security policies governing the IT system (organizational policies, federal requirements, laws, industry practices)
System security architecture
Current network topology (e.g., network diagram)

Information storage protection that safeguards system and data availability, integrity, and confidentiality
Flow of information pertaining to the IT system (e.g., system interfaces, system input and output flowchart)
Technical controls used for the IT system (e.g., built-in or add-on security product that supports identification and authentication, discretionary or mandatory access control, audit, residual information protection, encryption methods)
Management controls used for the IT system (e.g., rules of behavior, security planning)
Operational controls used for the IT system (e.g., personnel security, backup, contingency, and resumption and recovery operations; system maintenance; off-site storage; user account establishment and deletion procedures; controls for segregation of user functions, such as privileged user access versus standard user access)
Physical security environment of the IT system (e.g., facility security, data center policies)
Environmental security implemented for the IT system processing environment (e.g., controls for humidity, water, power, pollution, temperature, and chemicals).

Per altre informazioni, come ad esempio quelle utili a valutare probabilità ed impatto, la loro raccolta e valutazione sarà molto più complessa.

Come vedremo, in questo caso non sarà tuttavia necessario disporre di moltissime informazioni per fare una utile stima dei rischi, ma nondimeno tale stima richiederà che i parametri che entrano in gioco siano valutati da esperti. In altre parole, in assenza di dati oggettivi saranno i dati implicitamente presenti nel know how[5] degli esperti che consentiranno di ottenere un risultato valido.

Va puntualizzato al riguardo che le organizzazioni dispongono di molteplici fonti dati dalle quali possono ricavare informazioni utili, ad esempio, a valutare la probabilità che una minaccia si estrinsechi.

Il problema è che tali informazioni sono solitamente ignorate, non classificate, non collezionate.

Fra queste troviamo:

- quelle certamente riconducibili direttamente al sistema informativo, quali ad esempio:
  - la segnalazione di anomalie e malfunzionamenti da parte di utenti sia interni che esterni,
  - le richieste di interventi da parte degli utenti per risolvere tali situazioni (errori nelle applicazioni e nei sistemi, degrado delle prestazioni, perdita ed alterazione di dati, rotture hw, etc.);

[5] Butti G., Tutela del capitale intellettuale e sistemi esperti: applicazioni pratiche di intelligenza artificiale, www.cybersecurity360

- quelle che possono in qualche modo derivare da problemi legati al sistema informativo, quali ad esempio:
  - reclami, in particolare dei clienti (ad esempio ritardi nelle consegne, errate evasione di un ordine, etc.);
  - reclami dei fornitori (ad esempio ritardi nei pagamenti).

Per poter fornire informazioni utili questi eventi vanno adeguatamente censiti in appositi database.

Per le segnalazioni direttamente riconducibili al sistema informativo le aziende più grandi dispongono di processi formalizzati e di apposite procedure per la gestione dei ticket di assistenza.

Tuttavia, spesso il livello di dettaglio con cui sono segnalati i problemi o meglio ancora il livello di dettaglio con cui viene censita l'identificazione della causa e la descrizione della soluzione non è sufficiente.

Si perde in questo modo la possibilità di effettuare un'analisi a posteriori di quali siano le aree del sistema informativo più esposte, piuttosto che le applicazioni più carenti.

Spesso chi analizza e risolve il problema è concentrato unicamente a fornire supporto nei tempi più rapidi possibili e non dedica un tempo adeguato alla fase, altrettanto importante, di corretta classificazione delle cause.

Tale mancanza è principalmente imputabile alla scarsa formazione del personale e alla bassa sensibilità del management aziendale che privilegia la soluzione immediata e "tattica" dei problemi, piuttosto che affrontarne alla radice le possibili cause.

Anche nel caso della gestione dei reclami provenienti dall'esterno, in particolare dai clienti, sono rari i casi in cui vi è una gestione informatizzata del processo di risoluzione.

Solo in aziende come le banche, che hanno specifici obblighi normativi, si procede di solito ad una gestione mediante un processo formalizzato che tiene traccia dell'iter seguito.

Anche in questo caso però è raro trovare un'idonea classificazione dei problemi e delle cause scatenanti, tali da poter effettuare un'analisi a posteriori delle aree più a rischio del sistema informativo.

I problemi in questo caso si pongono a diversi livelli; innanzi tutto ricondurre un reclamo esterno ad un malfunzionamento del sistema informativo non è immediato.

È necessario analizzare nel dettaglio il contenuto stesso del reclamo, interagendo da un lato con un cliente "ostile" e dall'altro con un insieme di strutture aziendali che partecipano al processo che non ha correttamente funzionato.

Restando in ambito bancario: un reclamo derivante da un errato calcolo della rata di un mutuo può derivare da diverse cause, una delle quali può essere un malfunzionamento

dell'applicazione che effettua il conteggio delle rate o di una qualunque delle applicazioni a monte e a valle della stessa.

Per verificare se si tratta effettivamente di un problema applicativo e non di un malfunzionamento isolato sarebbe necessario disporre di un sufficiente numero di segnalazioni opportunamente classificate cioè censite con modalità omogenee.

Le premesse per poter effettuare queste analisi sono comunque:

- una corretta segnalazione da parte dei clienti direttamente al call center o all'ufficio reclami della banca,
- una corretta segnalazione da parte della filiale nel caso in cui il cliente si rechi direttamente allo sportello.

Ulteriori fonti dati sono costituiti dai sistemi di monitoraggio; questi possono fornire dati in tempo reale o a scadenze prefissate, con diversi livelli di dettaglio ed aggregazione.

I sistemi di monitoraggio possono ad esempio verificare:

- la raggiungibilità di un sistema,
- l'esistenza in vita di un sistema,
- il corretto funzionamento di un sito web mediante robot di navigazione automatica che simulano un utente reale,
- la misurazione delle prestazioni della LAN,
- la misurazione delle prestazioni della WAN,
- la corretta replica dei dati verso i siti di DR.

In alcune aziende è formalizzata la gestione degli incidenti informatici, anche se con tale termine possono intendersi eventi molto diversi fra loro.

Ad esempio, un incidente potrebbe essere considerato un malfunzionamento applicativo che rende indisponibile l'applicazione per gli utenti, mentre a livello infrastrutturale si potrebbe considerare incidente ciò che provoca un disservizio generalizzato.

Anche in questo caso è importante censire correttamente le informazioni per procedere a posteriori con un'analisi delle stesse.

Ulteriori fonti informative sono costituiti da una serie di indicatori, quali ad esempio il numero di righe di codice modificate in un certo periodo, distinguendo fra quelle effettuate per attività di manutenzione risolutiva da quelle effettuate per attività evolutiva.

Nel primo caso gli interventi evidenziano la presenza di situazioni anomale che sono state o sono in fase di risoluzione. Il secondo caso introduce invece una possibile instabilità futura nei sistemi, a causa delle novità introdotte.

Il livello di obsolescenza di un sistema potrebbe renderlo inefficace rispetto ad una evoluzione delle esigenze introducendo elementi di rischio, quali ad esempio una caduta delle prestazioni in termini di capacità elaborativa, risorse disponibili, tempi di risposta, etc..

Si pensi ad esempio ad elaborazioni batch notturne che si allungano sempre di più e non rendono disponibile il sistema informativo in tempo per l'orario di apertura delle filiali di una banca.

Anche l'analisi dei log può essere utile per valutare a posteriori un incidente o comunque un evento insolito ed individuarne le cause.

Anche il sistema dei controlli interni (di linea e di secondo livello) e l'audit costituiscono, oltre che strumenti di controllo e di indagine, anche una fonte di informazioni per rilevare situazioni anomale, legate direttamente ai sistemi informativi ovvero potenzialmente derivanti da questi.

In realtà le attività di audit dovrebbero essere pianificate sulla base delle analisi delle informazioni precedentemente censite, le quali dovrebbero consentire l'individuazione delle aree del sistema informativo più a rischio, sulle quali è quindi maggiormente utile effettuare indagini.

Gli esempi riportati evidenziano tutti una serie di elementi comuni:

- la necessità di specifiche regole di rilevazione e classificazione (non interpretabili) degli eventi, ad esempio mediante strumenti che prevedano una adeguata alberatura che guidi nella compilazione coloro che effettuano la segnalazione e successivamente la risoluzione del problema,
- una corretta identificazione e classificazione delle cause,
- una analisi a posteriori dei dati raccolti, al fine di individuare la presenza di problemi endemici e non legati a fattori casuali, al fine di individuare le aree di rischio e predisporre opportuni interventi sia di controllo, sia correttivi,
- la necessità di adeguata formazione e sensibilizzazione di tutto il personale su questi temi,
- la necessità che il management aziendale dia adeguata importanza alla gestione di questi aspetti, affiancando alle soluzioni tattiche quelle strategiche.

Tabella 4. Possibili fonti dati per la valutazione delle probabilità

segnalazioni di malfunzionamenti da parte di utenti sia interni che esterni (errori nelle applicazioni e nei sistemi, degrado delle prestazioni, perdite o alterazioni di dati, rotture…);
rapporti su incidenti
reclami dei clienti (per ritardi nelle consegne, errate evasioni di ordini…);
reclami dei fornitori (ad esempio ritardi nei pagamenti)
reclami dei dipendenti (ad esempio ritardi nei pagamenti degli stipendi, errori nei rimborsi spese)
rapporti di audit
analisi dei log
ticket: consentono di individuare i fattori di rischio e i difetti che possono preludere ad un incidente. supporto all'analisi delle cause

Nell'uso delle informazioni sopra citate devono comunque essere presi in considerazione importanti fattori; l'utilizzo di dati storici per la valutazione della probabilità, nasconde infatti delle insidie e pertanto è necessario valutare attentamente qual è la profondità storica con cui utilizzare tali dati. Questa non è assoluta, ma va determinata per ogni singola tipologia di evento, considerando il contesto di riferimento.

Ad esempio, una serie di incidenti di sicurezza derivanti dal malfunzionamento di un apparato o dalla mancanza di contromisure, non possono essere presi in considerazione se nel frattempo l'apparato è stato sostituito ovvero se sono state realizzate delle contromisure.

Non ha quindi senso definire a priori di prendere in considerazione tutti gli eventi anomali ed incidenti registrati, né che si prendano in considerazione ad esempio solo quelli degli ultimi 6 mesi.

Deve essere, infatti, presa in considerazione la serie storica di eventi che ha ancora valore, cioè che è applicabile ad una situazione (ad esempio un componente del sistema informativo) che non è stata cambiata nel tempo.

9. Calcolare la probabilità

Continuiamo l'articolo prendendo in considerazione, fra i parametri che entrano nella valutazione del rischio, la valutazione della probabilità.

Nei paragrafi precedenti si è dato per scontato che chi sta effettuando l'analisi sia in grado di valutare direttamente tale parametro in base alle informazioni disponibili ed alla propria esperienza.

In realtà le metodologie di analisi dei rischi, pur riconoscendo tale possibilità, introducono ulteriori parametri.

Ad esempio, nel caso di un evento che prevede l'intervento intenzionale di un attaccante, la valutazione deve anche considerare la sua motivazione che è a sua volta condizionata:

- dal valore intrinseco del bene che potrebbe sottrarre o del danno che potrebbe provocare,
- dalle vulnerabilità che potrebbe sfruttare,
- dalle contromisure in atto per contrastare le minacce.

Nel seguito dell'articolo verrà illustrata la metodologia **FAIR** (Factor Analysis of Information Risk), nella quale la valutazione della probabilità risulta essere una funzione di:

- frequenza della minaccia, a sua volta funzione della frequenza di contatto e probabilità di attacco,
- vulnerabilità, a sua volta funzione della capacità di attacco e azioni di contrasto.

Il **NIST Special Publication 800-30 Rev 1** propone invece una valutazione articolata in 3 fasi:

- in primo luogo, viene valutata:
  - nel caso di minaccia di tipo deliberato, la probabilità che eventi di minaccia siano messi in atto da parte di un attaccante,
  - nel caso di minacce accidentali, la probabilità che eventi di minaccia si verifichino;
- in secondo luogo, viene valutata la probabilità che gli eventi di minaccia, una volta messi in atto o verificatisi, comportino effettivamente degli impatti negativi sugli asset/processi dell'organizzazione;
- infine, viene valutata la probabilità complessiva come una combinazione della due precedenti secondo lo schema riportato in Figura 1.

Più dettagliatamente per quanto attiene gli atti deliberati, una valutazione della probabilità di accadimento si basa sulle caratteristiche di chi porta avanti l'attacco:

- le sue capacità e competenze,
- le sue intenzioni,
- i suoi obiettivi.

Al riguardo, il **NIST (800 30 RV1)** propone le tabelle, riportate come esempi mantenendo la denominazione originale, D3, G2, G4, G5.

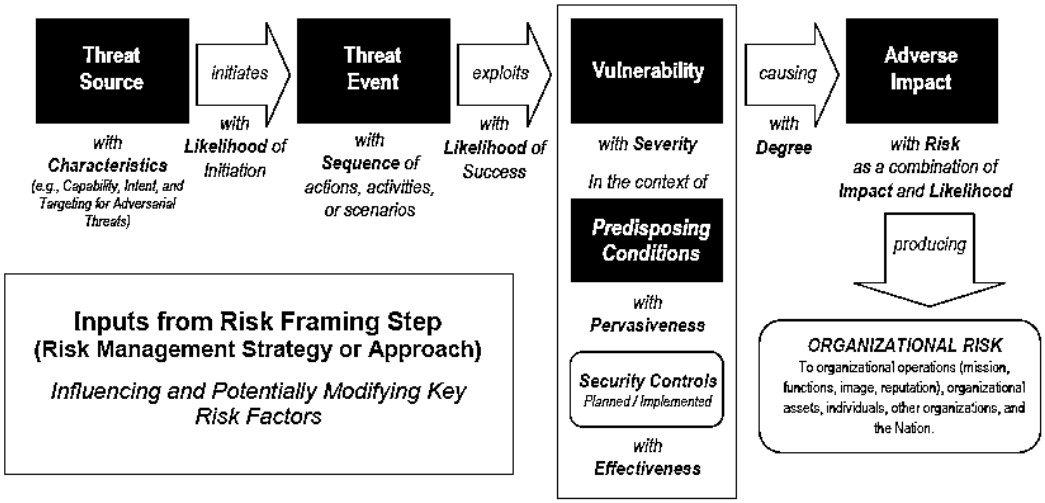

Figura 1

Per eventi diversi dagli atti deliberati, la probabilità che l'evento si verifichi si stima utilizzando:

- prove storiche,
- dati empirici o
- altri fattori.

Table D-3: assessment scale – characteristics of adversary capability

Qualitative Values	Semi-Quantitative Values		Description
Very High	96-100	10	The adversary has a very sophisticated level of expertise, is well-resourced, and can generate opportunities to support multiple successful, continuous, and coordinated attacks.
High	80-95	8	The adversary has a sophisticated level of expertise, with significant resources and opportunities to support multiple successful coordinated attacks.
Moderate	21-79	5	The adversary has moderate resources, expertise, and opportunities to support multiple successful attacks.
Low	5-20	2	The adversary has limited resources, expertise, and opportunities to support a successful attack.
Very Low	0-4	0	The adversary has very limited resources, expertise, and opportunities to support a successful attack.

Table G-2: assessment scale – likelihood of threat event initiation (adversarial)

Qualitative Values	Semi-Quantitative Values		Description
Very High	96-100	10	Adversary is **almost certain** to initiate the threat event.
High	80-95	8	Adversary is **highly likely** to initiate the threat event.
Moderate	21-79	5	Adversary is **somewhat likely** to initiate the treat event.
Low	5-20	2	Adversary is **unlikely** to initiate the threat event.
Very Low	0-4	0	Adversary is **highly unlikely** to initiate the threat event.

Table G-4: assessment scale – likelihood of threat event resulting in adverse impacts

Qualitative Values	Semi-Quantitative Values		Description
Very High	96-100	10	If the threat event is initiated or occurs, it is **almost certain** to have adverse impacts.
High	80-95	8	If the threat event is initiated or occurs, it is **highly likely** to have adverse impacts.
Moderate	21-79	5	If the threat event is initiated or occurs, it is **somewhat likely** to have adverse impacts.
Low	5-20	2	If the threat event is initiated or occurs, it is **unlikely** to have adverse impacts.
Very Low	0-4	0	If the threat event is initiated or occurs, it is **highly unlikely** to have adverse impacts.

Table G-5: assessment scale – overall likelihood

Likelihood of Threat Event Initiation or Occurrence		Likelihood Threat Events Result in Adverse Impacts			
	Very Low	**Low**	**Moderate**	**High**	**Very High**
Very High	Low	Moderate	High	Very High	Very High
High	Low	Moderate	Moderate	High	Very High
Moderate	Low	Low	Moderate	Moderate	High
Low	Very Low	Low	Low	Moderate	Moderate
Very Low	Very Low	Very Low	Low	Low	Low

La tabella G4 indica la probabilità che un evento, una volta avviato, possa provocare effettivamente un danno e la tabella G5 indica la probabilità complessiva.

Si rinvia al documento originale del NIST per una trattazione completa.

10. La metodologia FAIR: componente chiave: ontologia

In primo luogo, dobbiamo definire un modello che descriva come il rischio opera, indicandone i fattori costituenti e le loro relazioni. La descrizione, in termini matematici, di queste relazioni ci consentirà quindi di calcolare il rischio partendo dalla stima di tali fattori.

Nel paragrafo 12. Ontologia FAIR saranno descritti in dettaglio i fattori che costituiscono l'ontologia sviluppata in ambito Open Group.

11. Aspetti salienti per la valutazione

Questo paragrafo descrive le caratteristiche che sono indicative di una buona metodologia di valutazione del rischio. L'insieme degli elementi considerati non è in alcun modo completo od esaustivo, ma vuole stabilire alcuni concetti fondamentali.

11.1 . Probabilistico

Uno studio ed un'analisi del rischio è un compito difficile, infatti, spesso si deve partire da ipotesi fondate su informazioni incomplete, che contengono quindi un certo livello di incertezza. Tale "incertezza" non va mascherata, ma costituisce essa stessa parte dell'informazione. Essa va quindi misurata e registrata perché divenga parte di una corretta analisi del rischio.

L'incertezza può e deve essere intesa come un attributo dell'informazione, piuttosto che un limite della stessa. La sua comunicazione e il suo uso possono ottimizzare la gestione del rischio ed in particolare quella degli eventi dannosi e delle loro conseguenze.

Solo trattando il rischio come un problema di previsione probabilistica si può aggiungere il necessario rigore, controllo e struttura al processo di analisi.

Una buona metodologia per la valutazione del rischio deve quindi fornire all'analista gli strumenti per la stima delle sue probabilità e di quelle dei fattori costituenti.

11.2. Accurato

Una buona metodologia di valutazione del rischio dovrebbe fornire risultati accurati. Mentre sembrerebbe ovvio che i risultati del rischio valutato dovrebbero essere precisi, molte metodologie di valutazione del rischio si focalizzano maggiormente sugli aspetti tecnici di debolezza del sistema (vulnerabilità), invece che sulle probabilità di accadimento di un evento dannoso e sul conseguente impatto.

11.2.1. Precisione e accuratezza

Uno dei maggiori ostacoli all'adozione di un'analisi del rischio è l'idea che sia richiesta precisione. La precisione nella misura è desiderabile, ma non è necessaria. La precisione è

definita, in ambito dell'analisi dei rischi, come "la nostra capacità di fornire informazioni corrette ". Precisione, tuttavia, viene definita come "il grado di "convergenza" di dati rilevati individualmente (campione) rispetto al valore medio della serie cui appartengono". Poiché il rischio è un problema di probabilità, è estremamente difficile essere precisi nella misurazione, nel calcolo e nella rappresentazione, la precisione desiderata potrebbe non sempre essere raggiungibile.

Fortunatamente, per la maggior parte delle decisioni nella gestione del rischio delle informazioni non sono necessarie espressioni precise della probabile frequenza della perdita o della probabile entità della perdita, soprattutto quando la metodologia di valutazione del rischio è in grado di fornire costantemente risultati accurati. Uno degli obiettivi nella misurazione ed espressione del rischio dovrebbe essere quello di produrre e trasferire informazioni accurate.

Accuratezza e precisione sono due termini spesso utilizzati in modo errato nel contesto della misurazione, perciò è importante evidenziarne bene la differenza.

L'*accuratezza* indica quanto una misura è vicina al valore reale.

La *precisione*, invece, indica quanto vicini o quanto ripetibili siano i risultati. Uno strumento di misura preciso darà quasi lo stesso risultato ogni volta che viene utilizzato. In altre parole, la precisione di un esperimento, di uno strumento o di un valore è una misura dell'affidabilità e della coerenza.

Più in generale, l'accuratezza di un esperimento, di uno strumento o di un valore è una misura di quanto strettamente i risultati concordino con il valore vero. L'accuratezza si riferisce al grado di conformità e correttezza di qualcosa rispetto a un valore vero o assoluto, mentre la precisione si riferisce a uno stato di rigida precisione, cioè a quanto costantemente qualcosa è strettamente esatto.

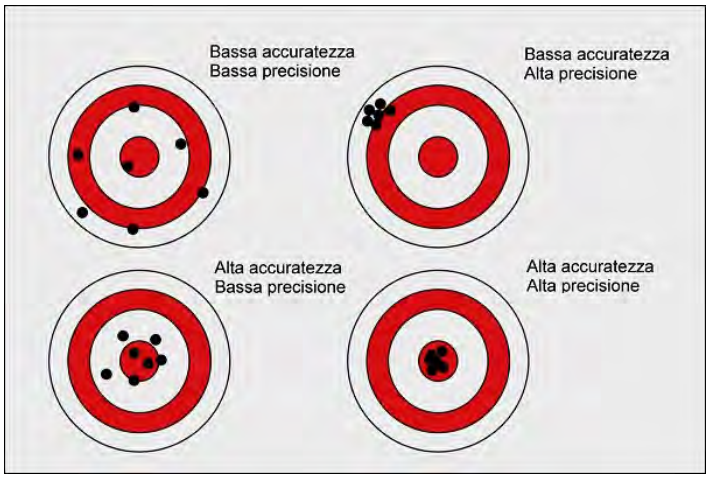

Figura 2 *- Accuratezza e precisione*

Quando una quantità viene misurata o calcolata, l'accuratezza della misurazione o il risultato calcolato danno il grado di vicinanza del valore al valore corretto. L'accuratezza, quindi, descrive una proprietà del *risultato*. La precisione, d'altra parte, quantifica il grado di efficacia con cui sono state effettuate le misure, o quanto bene sono stati effettuati i calcoli. La precisione dice qualcosa sul *processo di misurazione* o sul calcolo, ma non dice nulla sul risultato della misurazione o sul valore calcolato.

Spesso è possibile aumentare l'accuratezza di un risultato aumentando la precisione dello strumento di misura o del metodo di calcolo; tuttavia, se il modo di eseguire la misurazione o eseguire il calcolo non è corretto, aumentare la precisione non aumenterà necessariamente l'accuratezza del risultato. Inoltre, se il valore di una quantità è già noto con accuratezza, l'aumento della precisione non cambierà il suo valore.

11.3. Come riportare la precisione dei risultati

Esistono diversi modi per riportare (e valutare) la precisione dei risultati. Il più semplice è l'intervallo o *range* (ovvero la differenza tra i risultati più alti e quelli più bassi), spesso riportato come una differenza dalla media delle misure. Un modo migliore per evidenziare la precisione dei risultati – ma che richiede un'analisi statistica – sarebbe quello di valutare ed indicare la cosiddetta "deviazione standard".

La deviazione standard descrive come i risultati sono distribuiti intorno alla media. Se i risultati sono distribuiti normalmente, il 68% di questi sarà all'interno della deviazione standard. Una maggiore deviazione standard indica una maggiore dispersione nella precisione nei risultati. Una deviazione standard più piccola indica meno dispersione. Entrambe le serie di risultati hanno la stessa media.

11.3.1. Coerente (ripetibile)

Un indicatore significativo di una buona metodologia di valutazione del rischio è la ripetibilità delle misure. Essa consiste nel grado di concordanza tra una serie di misure della medesima grandezza quando le singole misurazioni sono effettuate lasciando immutate le condizioni di misura. In altre parole, se due analisti partono dalle medesime informazioni ed operano in modo indipendente dovrebbero arrivare a conclusioni simili.

Questa coerenza è importante per due motivi. In primo luogo, risultati ripetibili convalidano il grado di rigore e la logica della metodologia. In secondo luogo, rendono il risultato difendibile e credibile.

11.3.2. Difendibile

Affinché la valutazione del rischio sia difendibile, i risultati devono apparire accurati e logici. In caso contrario, quanto emerge dalla valutazione nonché il valutatore stesso perderanno inevitabilmente di credibilità.

11.3.3. Logico

L'utilizzo di una ontologia per la definizione del rischio consente anche di dimostrare e giustificare la "logica" utilizzata per trarre le conclusioni relative al rischio sia in termini dei fattori considerati, sia della matematica utilizzata per metterli in relazione

Una valida misurazione del rischio non deve utilizzare operazioni matematiche prive di senso. Ad esempio, molti metodi di valutazione del rischio che utilizzano scale ordinali, utilizzano anche operazioni aritmetiche per mettere in relazioni tali valori, ignorando il fatto che l'impiego di aritmetica con tali scale non porta a risultati logici e che quindi non è né accettabile né giustificabile ed andrebbe evitata.

11.3.4. Incentrato sul rischio

Le uniche metriche che contano davvero sono la probabile frequenza dell'evento perdita e la probabile entità della perdita. Ne consegue che, qualsiasi valutazione che non possa essere espressa in questi termini non è in realtà una misurazione del rischio, e non fornisce le informazioni necessarie per prendere le decisioni migliori nella gestione del rischio.

11.3.5. Conciso e significativo

L'espressione del rischio deve fornire le informazioni appropriate per i vari destinatari. Ad esempio, mentre i dirigenti dovranno essere messi in grado di scegliere se accettare, mitigare o trasferire il rischio, le informazioni tecniche fornite dovrebbero invece consentire alle parti interessate (tecniche) di realizzare le soluzioni selezionate. I risultati della valutazione del rischio dovrebbero essere espressi nel modo più conciso possibile per ridurre la possibilità di confusione. Le elaborazioni tecniche sui controlli e le tecniche di attacco dovrebbero essere utilizzate con giudizio.

Infine per essere significative, le raccomandazioni dovranno anche essere praticamente realizzabili per consentirne un utilizzo diretto, senza ulteriori eccessive elaborazioni.

11.3.6. Economicamente giustificato

Migliorare il livello di accuratezza di una misura ha un costo che cresce, in genere con un andamento simile a quello indicato in figura 3.

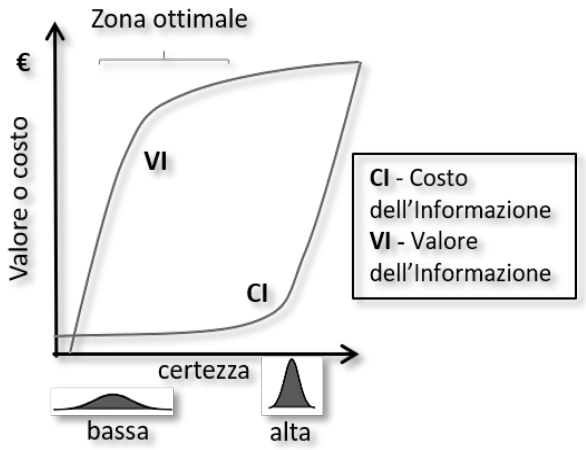

***Figura 3** - Costo / accuratezza analisi*

Migliorare le stime ha un costo progressivamente crescente. Di questo fenomeno va tenuto conto per evitare investimenti il cui ritorno, in termini di gestione del rischio, è progressivamente decrescente. In altre parole, esiste un livello di accuratezza oltre il quale non conviene andare.

11.3.7. Assegnazione delle Priorità

I risultati di una valutazione del rischio dovrebbero fornire chiare indicazioni relative alla priorità di intervento. La definizione delle priorità potrà essere basata sul rischio, sulle risorse necessarie per affrontare i problemi, e/o su altri criteri precedentemente previsti dal management.

12. Ontologia FAIR

L'ontologia FAIR costituisce la base per l'omonima metodologia e ne garantisce efficacia, praticità e concretezza. Detto semplicemente, possiamo affermare che l'ontologia costituisce un modello di come il rischio si genera, descrivendone i fattori costituenti e le loro relazioni. Queste relazioni possono essere descritte matematicamente consentendo quindi di calcolare il rischio partendo da misure e stime dei fattori stessi (v. **Errore. L'origine riferimento non è stata trovata.**4 e Figura 5).

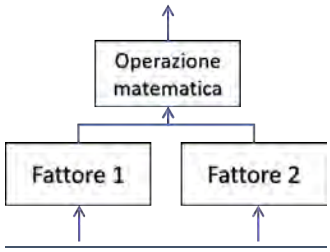

Figura 4 *- Relazione tra fattori FAIR*

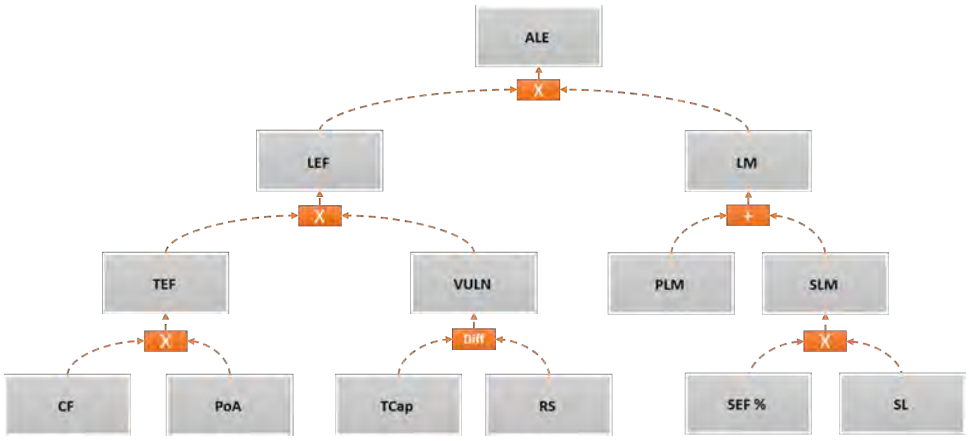

Figura 5*- Ontologia FAIR*

Tabella 5 - Fattori dell'ontologia FAIR

Sigla	Descrizione
ALE	Annual Loss Excpectation Perdita Totale Annua L'esposizione alla perdita totale è il rischio totale calcolato (valore della perdita atteso) che si verifica su base annua (se non è dimostrato che un evento di perdita si verifichi almeno una volta all'anno). Ciò significa che l'importo di un singolo evento di perdita viene ripartito negli anni precedenti. Gli scenari di rischio con eventi di perdita che si verificano una o più volte all'anno mostrano la somma degli eventi di perdita annuali.

Sigla	Descrizione
LEF	Loss Event Frequency Frequenza degli Eventi di Perdita La frequenza degli eventi di perdita è la frequenza probabile, entro un periodo di tempo, in cui una minaccia danneggerà un asset. Affinché questa misura abbia un significato, deve includere un periodo di tempo. Ex. quante volte all'anno gli hacker eseguono un attacco Denial of Service contro un sistema bancario online che si traduce in una perdita di utilizzo per i clienti o con la frequenza con cui i ladri rubano denaro.
TEF	Threat Event Frequency Frequenza degli Eventi Minaccia La frequenza degli eventi di minaccia è la frequenza probabile, entro un periodo di tempo, in cui una minaccia potrebbe causare una perdita. Rispetto alla LEF, questa misura descrive come una minaccia può, piuttosto che quanto spesso si tradurrà in una perdita. Ex. quante volte all'anno un ladro cerca di rubare i soldi o quante volte gli hacker eseguono un attacco Denial of Service al tuo computer.
CF	La Frequenza di Contatto (CF) è la frequenza probabile, entro un periodo di tempo, in cui una minaccia entrerà in contatto con una risorsa. Il contatto può essere fisico o "logico" (ad esempio, sulla rete).
PoA	La Probabilità di Azione (PoA) è la probabilità che una minaccia agisca contro una risorsa una volta che si verifica il contatto. Una volta che si verifica il contatto tra una minaccia e una risorsa, l'azione contro la risorsa può o meno aver luogo. Per alcuni tipi di agenti di minaccia, in particolare gli agenti di minaccia naturali, l'azione ha sempre luogo. Ad esempio, se un tornado entra in contatto con una casa, l'azione è una conclusione scontata. Tuttavia, le scansioni delle porte su un sito Web potrebbero non comportare ulteriori azioni da parte della minaccia.
VULN	La Vulnerabilità (VULN) è la probabilità che un evento di minaccia diventi un evento di perdita. La vulnerabilità esiste quando c'è una differenza tra l'attacco utilizzato dall'agente di minaccia e la capacità di una risorsa di resistere a quell'attacco. Un esempio di ciò è il malware rivolto a un server Windows senza patch.
TCap	La Capacità di Minaccia (TCap) è il probabile livello di forza che una minaccia è in grado di applicare contro una risorsa. Il contesto per questa misurazione è con le capacità e le risorse che una minaccia ha a disposizione per attaccare una risorsa. Nell'esempio degli attacchi degli stati-nazione, l'esperienza e la conoscenza dell'hacking definiscono le abilità e la quantità di tempo e denaro disponibile per finanziare gli attacchi sono le risorse.

Sigla	Descrizione
RS	La difficoltà misura la forza di un controllo rispetto al livello di sforzo richiesto dagli attacchi per una violazione riuscita. Ad esempio, un sistema bancario online che sfrutta l'autenticazione a più fattori ha una difficoltà maggiore per una comunità di hacker rispetto a uno protetto da una semplice coppia di nome utente e password.
LM	Loss Magnitude (LM) è la probabile entità della perdita risultante da un evento di perdita. L'altro lato della tassonomia in Frequenza degli eventi di perdita ha introdotto i fattori che determinano la probabilità che si verifichino eventi di perdita. Il lato Loss Magnitude della tassonomia descrive l'altra metà dell'equazione del rischio: i fattori che determinano l'entità della perdita quando si verificano gli eventi.
PL	La Perdita Primaria (PL) è il risultato diretto delle azioni di una minaccia su una risorsa e spesso rappresenta l'intenzione di agire contro la risorsa. Il proprietario degli asset interessati è considerato lo stakeholder principale in un'analisi. Ex. Il successo degli attacchi Denial of Service e della violazione dei dati di un sito di shopping online durante le festività natalizie si traduce in una perdita di entrate previste, che di solito si prevede saranno le più alte dell'anno, per l'azienda.
SL	Il Rischio Secondario (SL) è il risultato di stakeholder secondari, come clienti, azionisti, autorità di regolamentazione, ecc., Che reagiscono negativamente all'evento di perdita primaria che si traduce in un'ulteriore perdita per lo stakeholder principale. Un esempio sono i clienti che hanno fatto causa a un'azienda dopo una violazione dei dati o il costo dell'offerta di servizi di monitoraggio del credito ai clienti interessati da una violazione dei dati.

13. Conclusioni

Le organizzazioni di tutti i tipi hanno una crescente necessità di potersi avvalere di strumenti per una valutazione dei rischi che consenta loro di meglio indirizzare i propri investimenti in termini di sicurezza.

Nonostante le oggettive difficoltà, derivanti molto spesso dalla carenza delle informazioni necessarie allo scopo, sono oggi disponibili metodi che consentono, anche in tale contesto, di elaborare con relativa facilità e con l'uso di normali strumenti di office automation, risultati utili per tale finalità.

È quindi fondamentale che le organizzazioni rivedano il proprio approccio al rischio, per essere preparate ad affrontare le nuove sfide delle quali la recente pandemia costituisce un valido esempio.

Valutazione dei rischi per la sicurezza delle informazioni: sicuri della soluzione adottata?

Risk assessment for information security: are you sure about the adopted solution?

Fabrizio Cirilli ♦

♦*PDCA Srl*

Sommario

Strumenti di ogni tipo sono utilizzati da migliaia di aziende ma non sempre è chiaro se e come funzionino certi strumenti informatici rispetto alla sicurezza delle informazioni.

Abstract

Tools of all kinds are used by thousands of companies but it is not always clear if and how certain IT tools work with respect to information security.

Durante gli audit di terza parte per la ISO/IEC 27001 ci si imbatte continuamente nelle valutazioni dei rischi basate su minacce-vulnerabilità di asset tecnologici.
Cerchiamo di capire se questa soluzione sia o no in linea con la ISO/IEC 27001 e se sia, in qualche modo, richiesta dalla norma o una scelta delle aziende e, in quest'ultimo caso, se paga o meno.
Iniziamo con dire che la ISO/IEC 27001 riguarda la sola sicurezza delle informazioni, si occupa cioè della riservatezza, integrità e disponibilità delle informazioni. Fatta questa premessa entriamo nella norma e verifichiamo dove e come questa cosa è fissata.
A proposito della valutazione dei rischi al requisito 6.1.2.c.1 troviamo:
applicando il processo di valutazione del rischio relativo alla sicurezza delle informazioni per identificare i rischi associati alla perdita di riservatezza, di integrità e di disponibilità delle informazioni incluse nel campo di applicazione del sistema di gestione per la sicurezza delle informazioni;
Siamo quindi certi che la norma non tratta di apparati connessi, almeno per quanto concerne la valutazione dei rischi inerenti alle informazioni. In questo tralasciamo le ovvie considerazioni tra le informazioni e gli asset tecnologici che le gestiscono, ci torneremo più tardi.
Non sono citate minacce o vulnerabilità per determinare i rischi nella ISO/IEC 27001.
E allora da dove spuntano queste due? Dalla ISO/IEC 27005 che non è una norma ma un documento a supporto per quelle organizzazioni che non hanno esperienza specifica sul tema.
La ISO/IEC 27005 specifica però che:

minacce e vulnerabilità non sono più richieste dalla ISO/IEC 27001
a partire dalla versione 2013; a tal proposito occorre precisare che l'attuale versione nazionale della norma del 2017 non modifica la versione originale.
Quindi non abbiamo ancora capito il perché minacce e vulnerabilità siano presenti in alcune valutazioni dei rischi delle aziende. Un'altra spiegazione possibile è che siano stati utilizzati dei tool o delle metodologie che ne fanno ancora uso. Spesso è così infatti.
Cosa fare? Niente, se funziona. Altrimenti basta tornare alla norma.
Una delle modifiche fondamentali del 2013 alla ISO/IEC 27001 è stata proprio quella di cercare di staccare la sicurezza delle informazioni dalla sicurezza informatica. È inevitabile parlando di minacce e vulnerabilità associare queste due chiavi di lettura agli apparati, dimenticando l'informazione che invece deve essere il centro della valutazione.
Perché continuare a parlare di rischi se ho le soluzioni tecnologiche più evolute? Perché dovrei spendere ulteriori risorse per incrementare i livelli di sicurezza dopo aver speso una montagna di denaro? Queste sono due delle domande più comuni che gli amministratori delle aziende si pongono in questi casi. Dal loro punto di vista è perfettamente logico: se ho la soluzione più evoluta i rischi dovrebbero essere gestiti.
Purtroppo, non è così perché gli apparati si concentrano su alcune dimensioni della sicurezza informatica ma non gestiscono altre parti tipiche della sicurezza delle informazioni (ad es. le competenze e la consapevolezza del personale, l'organizzazione aziendale, l'integrazione con i processi aziendali, il coinvolgimento del top management ecc.). Questi argomenti sono coperti dalla sicurezza delle informazioni, in un processo top down e non bottom up come nella sicurezza informatica.
Nella sicurezza informatica sono i tecnici, l'ICT a fare considerazioni, analisi, scegliere contromisure ecc. Nella sicurezza delle informazioni sono i risk owner. Ma chi sono i risk owner?
Per risk owner si intende quella *persona o entità che ha l'accountability e l'autorità per gestire i rischi*, non degli apparati ma i *rischi per le informazioni incluse nel campo di applicazione*.
Ora la domanda diventa: chi nella mia organizzazione ha autorità e accountability (è intraducibile quindi lo lasciamo come è nella norma)? Temo che la risposta si trovi nei vertici aziendali.
Non parliamo del Data Owner o del Process Owner, sono altre funzioni. Non è detto nemmeno che queste figure possano coincidere con i Risk Owner.
Quindi cosa devo fare? Ripensare al campo di applicazione e al contesto per identificare quali informazioni vanno protette e perché. Poi possiamo porci le domande: quali impatti avrei se perdessi la riservatezza di ogni informazione protetta? E se perdessi l'integrità? E se perdessi la disponibilità?
Non necessariamente gli impatti sono gli stessi; ad esempio, perdendo la riservatezza di dati personali (sempre che questi siano inclusi nel campo di applicazione) è chiaro il riferimento alle conseguenze in termini di GDPR e Privacy. Lo stesso vale per le penali nei contratti, per le sanzioni dovute a direttive e regolamenti applicabili alle informazioni nel campo di applicazione.

Quindi, più che un'analisi di minacce e vulnerabilità, qui si tratta di analizzare sanzioni, penali ecc. includendo danni di immagine e simili. Stiamo parlando di valutazioni di alto livello, indipendenti dagli apparati.
Altro discorso è quello della determinazione della *verosimiglianza realistica* (così è definita, non probabilità che riporterebbe a considerazioni di altra natura e fonte). Quanto è verosimile (possibile) che io possa perdere la riservatezza di una determinata informazione? E l'integrità? E la disponibilità?
Anche qui poco abbiamo a che fare con gli apparati, siamo piuttosto nel campo dei dati storici dell'azienda, delle informazioni esperienziali o della letteratura in materia. E di nuovo ad un livello alto che prescinde da minacce e vulnerabilità.
In definitiva, per ogni informazione inserita nel campo di applicazione del Sistema di Gestione per la Sicurezza delle Informazioni si devono determinare i rischi per la perdita di riservatezza, integrità e disponibilità delle informazioni e non degli apparati in quanto tali.
La formula per il calcolo del rischio è semplice:

$$R = I \times P$$

Dove I è l'impatto e P è la possibilità di accadimento (leggendola come RIP è mnemonicamente più facile e in qualche modo riconduce alle potenziali conseguenze per la mancanza di gestione del rischio). La formula va ripetuta per riservatezza, integrità e disponibilità per tutte le informazioni incluse nel campo di applicazione.
Posso fare una valutazione aggregata in termini di riservatezza, integrità e disponibilità delle informazioni? È poco efficace per il corretto dimensionamento del rischio ma possibile, specie nei tentativi iniziali può dare un'idea macroscopica del tutto. Poi però diventerà inefficace per la scelta delle contromisure da applicare.
Contromisure, questo era il termine originale e più consono, poi per un inglesismo siamo passati ai controlli, anche se il termine controllo tende a confondersi in italiano con un sostantivo che poco ha a che fare con il termine contromisura. Anche qui avremmo bisogno di qualche pagina per spiegare il caos che un termine improprio può generare per i non addetti ai lavori!
Torniamo alla valutazione dei rischi, c'è un altro punto che merita attenzione, il requisito 6.1.2.b:
assicuri <u>che ripetute</u> valutazioni del rischio relativo alla sicurezza delle informazioni producano risultati coerenti, validi e confrontabili tra loro
La parola magica è: "ripetute", quindi più di una! Considerando che quanto descritto nella norma avviene all'interno del ciclo PDCA, la valutazione dei rischi deve essere ripetuta (quindi almeno 2 volte) all'interno di ciascun ciclo PDCA. Ciò per assicurare *risultati coerenti, validi e confrontabili tra loro.*
Questo perché la prima valutazione mi misura, la seconda mi permette di capire se i trattamenti posti in atto hanno dato i loro effetti e se la valutazione dei rischi si sia effettivamente modificata come atteso.
Per dirla in modo semplice: mi peso prima della dieta, faccio la dieta (le mie contromisure) e poi mi ripeso per vedere se la dieta funziona o no come atteso.

Sembra un concetto facile ma implica una serie di considerazioni importanti che spesso sfuggono alle organizzazioni.
Non abbiamo dimenticato i nostri termini iniziali: minacce e vulnerabilità. Diciamo che anche l'ordine non è del tutto corretto. Se parliamo di asset informatici l'elemento primario è la vulnerabilità che potrebbe essere sfruttata da una minaccia per concretizzare un rischio.
Una chiave non è di per sé una minaccia, almeno fin quando non incontra la serratura adatta. Non posso dire che le chiavi costituiscano in senso assoluto una minaccia se non ho una porta dotata di serratura.
Quindi, le valutazioni dei rischi dovrebbero partire dalle vulnerabilità degli asset coinvolti (ma siamo di nuovo nel campo della sicurezza informatica). Infatti, una piattaforma come CVE (https://cve.mitre.org/) ha proprio questo compito: aiutare a comprendere quali vulnerabilità note sono collegate ai miei asset. Dopo potrò fare riflessioni sulle minacce in grado di sfruttarle. Spesso in audit emergono vulnerabilità come Spectre e Meltdown, è facile immaginare le considerazioni in merito a minacce e contromisure applicabili al caso.
Un altro punto per considerare il giusto ordine di analisi è lo "0day". Partiamo dalle vulnerabilità note, quando una minaccia riesce a sfruttare la vulnerabilità il gioco è fatto. Ora dovrebbe essere più chiaro il rapporto tra vulnerabilità, minacce e informazioni.
Allora perché il 90% di queste valutazioni parte dalle minacce? È come dire che siccome il furto esiste lo si applica a tutti gli asset aziendali. Bene, proviamo: il building? Il generatore elettrico? Gli UPS? Il sistema di condizionamento? Il NAS? Il Cloud!?
Qualcosa non torna. Probabilmente si parte dalle minacce perché sono l'argomento percepito dalle persone coinvolte nelle interviste. In questo caso è come chiedere una qualsiasi opinione alle persone, senza alcuna base di partenza. Ciò potrebbe causare alcuni effetti:

1. il risultato della valutazione conduce a un rischio *percepito,* che non necessariamente è correlato alle vere vulnerabilità;
2. sullo stesso asset, persone con esperienza diversa, potrebbero avere visioni diametralmente opposte, ampliando la scala del rischio a valori pressoché infiniti;
3. essendo tutto basato sulle minacce, se una minaccia non ha fondamento mi troverò ad avviare contromisure inutili, disperdendo soldi ed energie.

Per gli interessati recupero questo schema, tratto dalla ISO/IEC 13335 (lontana parente della sicurezza delle informazioni ritirata nel 2005, all'uscita della prima edizione della ISO/IEC 27001):

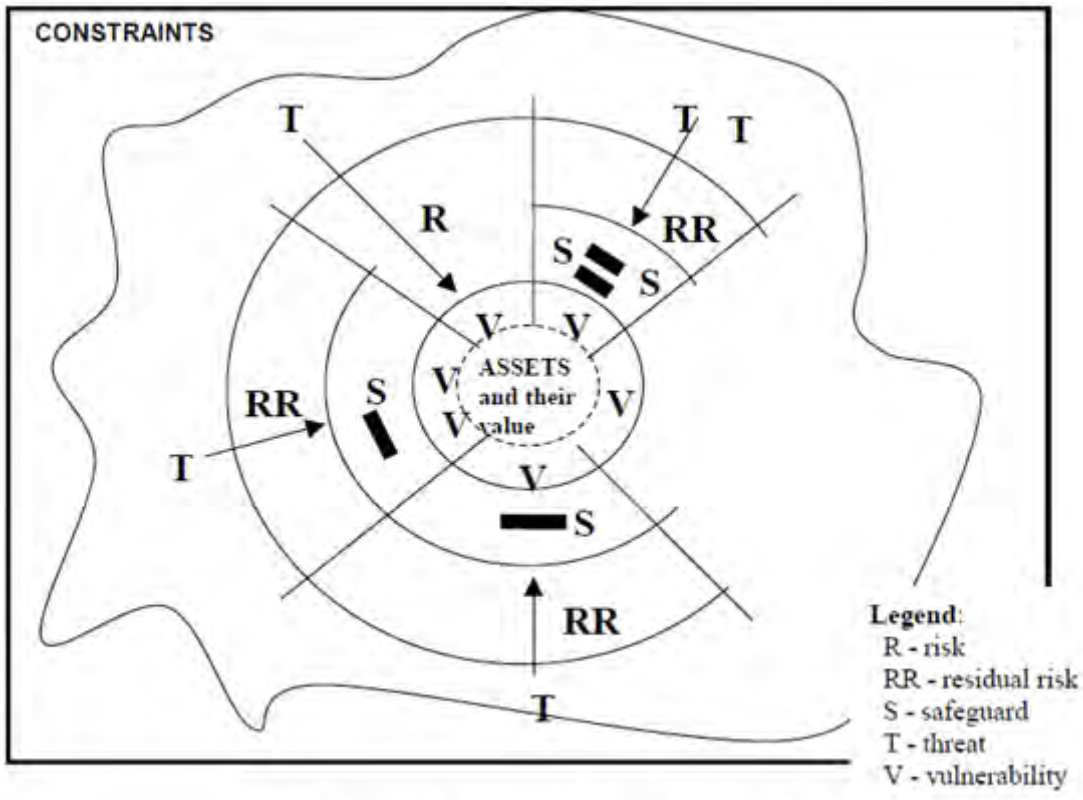

Figure 1 – Security element relationships

Dallo schema è chiaro che le vulnerabilità sono il centro dell'analisi e, quelle che non hanno ancora minacce in grado di sfruttarle, non necessariamente generano rischi (l'esempio fatto prima su Meltdown/Spectre e 0Day).

Quindi cosa fare se si ha una valutazione dei rischi che include minacce e vulnerabilità? Semplicemente capirne i contenuti e l'aderenza con la norma, decidere se vale comunque la pena di mantenerla come è oppure modificare il processo per adattarlo ai requisiti della ISO/IEC 27001.

È un errore parlare di minacce e vulnerabilità in una valutazione dei rischi per una ISO/IEC 27001? No, se assicura comunque la copertura delle informazioni e non diventa fuorviante per uno dei potenziali errori sopra descritti.

Cosa si fa se siamo incappati in uno di questi errori? Si riparte dalla ISO/IEC 27001 e poi si riconsidera il tutto per valutare se l'errore impatta o meno sulla sicurezza delle informazioni in modo significativo (esistono il livello di rischio accettabile e l'accettazione consapevole del rischio che possono venirci in aiuto in questi casi).

Cosa si rischia lasciando le cose come sono? Dal punto di vista formale, una non conformità come minimo, che può diventare maggiore/critica/bloccante in base al tipo di conseguenze sul Sistema di Gestione. Dal punto di vista sostanziale si avrebbe un Sistema concentrato su elementi errati e un dispendio di energie che non necessariamente assicura il grado di protezione atteso.

Un argomento così complesso non può essere risolto in queste poche righe ma da qualche parte dobbiamo pur iniziare a rimettere ordine. Partire da queste considerazioni può aiutare molte organizzazioni.

Nuovi approcci per garantire la sicurezza nei sistemi hardware.

Analisi delle vulnerabilità: tecniche di rilevazione e mitigazione

New approaches to guarantee security in hardware systems.

Analysis of Vulnerabilities: Detection and Mitigation Techniques

Alessandro Palumbo ♦*, Kerem Arıkan* □*, Giuseppe Bianchi* ♦*, Marco Ottavi* ♦

♦ *Università degli Studi di Roma Tor Vergata*
□ *TOBB University of Economics and Technology*

Sommario

Il tema della sicurezza dei sistemi di calcolo elettronici, in seguito per brevità chiamati hardware, comprende problemi di sicurezza e fiducia ad ampio raggio, che abbracciano l'intero ciclo di vita di un dispositivo e tutti i suoi livelli di astrazione (chip, PCB, sistemi e sistema di sistemi). Con l'aumento delle vulnerabilità della sicurezza e dei problemi di fiducia, il ruolo dell'hardware come punto riferimento di sicurezza di un sistema informatico è messo in discussione.

A causa della tendenza di affidare le differenti fasi di progettazione e fabbricazione del circuito a diverse strutture e di fare sempre più affidamento su core di proprietà intellettuale (IP) di terze parti, i sistemi su chip (SoC) stanno diventando sempre più vulnerabili ad attività dannose e alterazioni denominate Hardware Trojan. Le modifiche circuitali da loro introdotte possono far trapelare informazioni sensibili (o private) e consentire la fattibilità di attacchi, che hanno lo scopo, ad esempio, di interrompere il funzionamento del sistema e la riduzione della sua affidabilità.

D'altra parte, osservando alcune caratteristiche del circuito, spesso vengono esposte vulnerabilità inaspettate che lanciano nuove sfide a progettisti e ingegneri della sicurezza. Ad esempio, le differenze temporali introdotte dalle cache o dall'esecuzione speculativa di un programma possono essere sfruttate per far trapelare informazioni o rilevare potenziali attività. Un circuito con componenti la cui origine è affidabile (ovvero fidati, in inglese "trusted") potrebbe essere comunque attaccato; così come un circuito a prova di attacco non ha necessariamente componenti che non siano stati manomessi.

I problemi di fiducia (inglese trust) dell'hardware derivano dal coinvolgimento di entità potenzialmente non affidabili nel ciclo di vita di un hardware, inclusi IP non attendibili o fornitori di strumenti CAD (Computer-Aided Design) e strutture di progettazione, fabbricazione, test o distribuzione. I problemi di sicurezza hardware derivano dalla sua stessa

vulnerabilità agli attacchi (ad esempio, attacchi tipo side-channel o Trojan) a diversi livelli (come chip o PCB), nonché dalla mancanza di un solido supporto hardware per la sicurezza del software e del sistema. Proteggere i microprocessori dalle minacce esistenti non è banale ed è reso ancora più difficile dalla continua comparsa di nuovi attacchi (ad esempio Spectre [1], Meltdown[2]).
Le sfide sono due: rilevare (e possibilmente non innescare) modifiche dannose ai circuiti e proteggere l'hardware dagli attacchi. In questo articolo presentiamo due architetture e un nuovo approccio, basato su strutture dati probabilistiche, per garantire la sicurezza del circuito. Il primo è in grado di rilevare modifiche indesiderate dell'hardware; il secondo protegge il processore dagli attacchi architetturali di tipo side-channel (MSCA). L'idea è di aggiungere ai microprocessori moduli per il controllo della sicurezza, con lo scopo di osservare le istruzioni eseguite, identificare e segnalare possibili attività sospette.
Per valutarne l'efficacia, gli approcci proposti sono stati integrati sul core RISC-V disponibile liberamente per lo sviluppo. Riguardo il trust dell'hardware abbiamo dimostrato che il nostro design è in grado di rilevare se ci sono state manomissioni tra memorie e core; sulla sicurezza dell'hardware abbiamo dimostrato la sua efficacia nel rilevare gli attacchi Spectre [1], Orchestration [31] e Battery Drain [32]. Inoltre esso è configurabile in fase di progettazione (e riconfigurato dopo l'installazione da parte dell'utente) in modo da mantenere sempre aggiornato l'elenco degli attacchi che il checker è in grado di identificare.

Abstract

The topic of hardware security encompasses wide-ranging security and trust issues, which span the entire lifecycle of electronic hardware, and all its abstraction levels (chips, PCBs, systems, and system of systems). With increasing security vulnerabilities and trust issues, the role of hardware as a trust anchor of a computing system is being challenged.
Due to the emerging trend of outsourcing the design and fabrication services to external facilities and increasing reliance on third-party Intellectual Property (IP) cores, Systems on chip (SoCs) are becoming increasingly vulnerable to malicious activities and alterations referred to as Hardware Trojans. The modification introduced by them can leak sensitive (or private) information as well as enable launching other possible attacks, for example, denial of service and reduction in reliability.
On the other hand, observing some features of the circuit, often are exposed unexpected vulnerabilities that pose new challenges to designers and security engineers. For example, the timing differences introduced by caches or speculative execution can be exploited to leak information or detect activity patterns.
A circuit with trustable components could be attacked; an attack-proof circuit does not necessarily have components that have not been tampered with. Hardware trust issues arise from involvement of untrusted entities in the life cycle of a hardware, including untrusted IP or computer-aided design (CAD) tool vendors, and untrusted design, fabrication, test, or distribution facilities. Hardware security issues arise from its own vulnerability to attacks (e.g.,

side-channel or Trojan attacks) at different levels (such as, chip or PCB), as well as from lack of robust hardware support for software and system security. Protecting microprocessors from existing attacks is an extremely and it is made even harder by the continuous rise of new attacks (e.g. Spectre [1], Meltdown [2]).
The challenges are two: detecting (and possibly bypassing) circuit malicious modifications and protecting the hardware from attacks. In this paper we present two architectures and a new approach, based on probabilistic data structures in order guarantee the safety of the circuit. The first one is able to detect undesidered modification of the hardware; the second one protects microprocessor against Microarchitectural Side-Channel Attacks (MSCA). The idea is to add to microprocessor-based systems a security checking modules in charge of observing the fetched instructions and of identifying and signaling possible suspicious activity.
We integrated the proposed approaches in a RISC-V core. About the trustable of the hardware we proved that our design is able to detect design-time by the designer (and reconfigured after deployment by the user) in order to always keep updated the list of the attacks the checker is able to identify.if there have been any modifications between memories and core; about the hardware security we showed its effectiveness in detecting the Spectre [1], Orchestration [31], and Battery Drain [32] attacks. In addition it is configurable at design-time by the designer (and reconfigured after deployment by the user) in order to always keep updated the list of the attacks the checker is able to identify.

1. Introduzione

La sicurezza informatica è diventata una parte essenziale del mondo elettronico moderno. I requisiti di un sistema, affinché sia sicuro, sono stringenti e di vitale importanza in ogni settore, come ad esempio nei settori di *Internet of Things (IoT)/Edge Computing* [3], Industria 4.0 [4] o *Automotive* [5].
La sicurezza delle informazioni, in generale, fornisce riservatezza, integrità e disponibilità dei dati mediante la protezione dai processi (accesso, uso, modifica, distruzione) non "autorizzati". La sicurezza della rete si concentra sugli attacchi alle informazioni condivise dai dispositivi che sono connessi alla medesima rete e sui meccanismi per garantire l'usabilità e l'integrità dei dati, designati da potenziali attacchi. La sicurezza del software si concentra sugli attacchi "dannosi" all'esecuzione del programma, spesso sfruttando bug di implementazione, (come ad esempio la gestione degli errori incoerente e gli *overflow*) e sulle tecniche adibite a garantire un funzionamento affidabile dell'algoritmo eseguito dal programma stesso, anche in presenza di potenziali rischi per la sicurezza.
Per garantire l'esecuzione sicura di un qualsiasi software, è necessario espletarla su un circuito dal processo produttivo affidabile. L'*Hardware Security* è la scienza che si occupa della sicurezza dell'hardware, andando a proteggere i vari componenti elettronici che detengono dati sensibili e privati. Costituisce la base della sicurezza del sistema, fornendo un punto di ancoraggio alla fiducia per altre componenti di altro sistema che interagiscono strettamente con esso. Comprende la definizione dell'architettura del circuito, l'implementazione e la successiva

convalida. Il focus della sicurezza dell'hardware si concentra sull'annientare attacchi predisposti per boicottare o compromettere risorse e sul progettare approcci per proteggere queste ultime. Le risorse in esame sono i componenti dello stesso hardware, ad esempio circuiti integrati (di tutti i tipi), componenti passivi (come resistori, condensatori, induttori) e PCB; così come i dati memorizzati all'interno di questi componenti (ad esempio chiavi crittografiche, dati utente sensibili, firmware, dati di configurazione).
Le proprietà di sicurezza tradizionali (riservatezza, integrità e confidenzialità dei dati), sono generalmente garantite dagli algoritmi crittografici (ad esempio AES [6] e RSA [7]) e dalle funzioni di *hashing* (ad esempio SHA 3 [8]). Matematicamente tali algoritmi risultano robusti, ma le loro possibili implementazioni possono soffrire di falle di sicurezza. Negli ultimi anni, diversi acceleratori hardware crittografici hanno dimostrato di essere predisposti a numerosi attacchi, tra cui *Differential Fault Analysis* (DFA) [9] e *Side-Channel Analysis* (SCA) [10]. Di conseguenza, i sistemi implementati possono essere vulnerabili, sebbene siano dotati di moduli dedicati alla sicurezza.

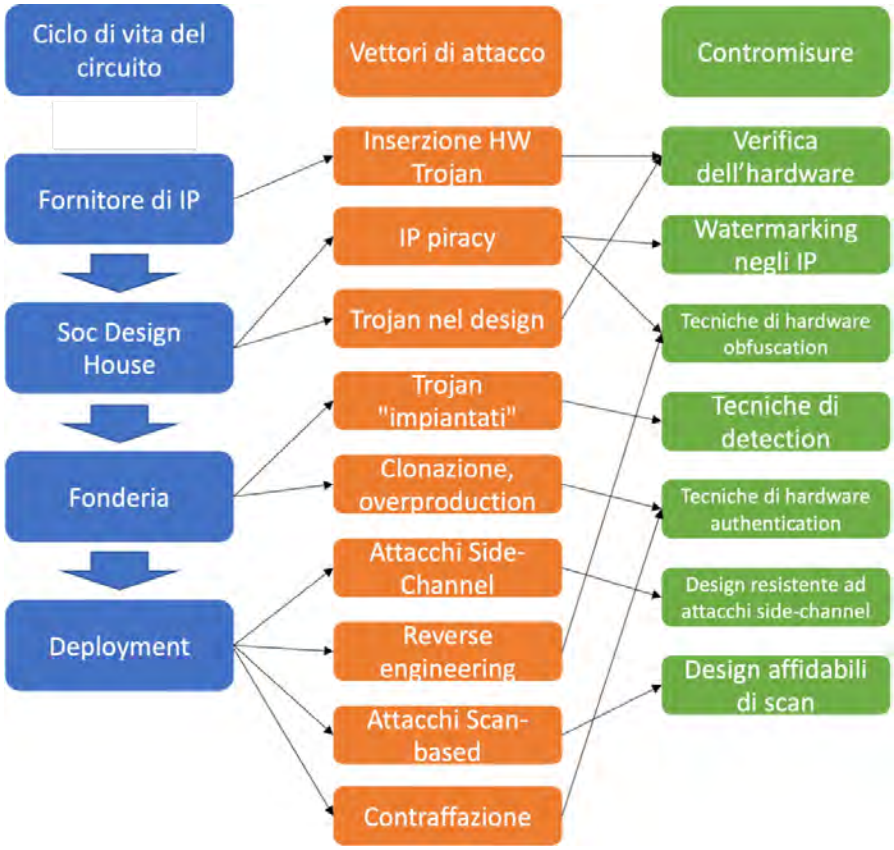

Figura 1 - *Problemi di sicurezza derivanti da differenti processi produttivi con eventuali e relative tecniche di contromisure*

2. Modelli per la sicurezza

Per descrivere un potenziale problema del circuito soggetto ad un attacco, e di conseguenza pensare ad una possibile soluzione, è fondamentale descrivere in modo univoco il modello di sicurezza corrispondente. A questo proposito vanno specificati, il *modello di trust*, che indica quali parti o componenti del circuito sono affidabili e sicuri e il *modello della minaccia*, che descrive lo scopo e il meccanismo di un attacco. Questo modello descrive l'obiettivo dell'attacco e la modalità tramite la quale viene innescato. Ad esempio, far trapelare dati da un SoC (o boicottare il suo comportamento funzionale), mediante l'inserimento malizioso di un trojan, o sfruttando una vulnerabilità del circuito non prevista dai progettisti.

2.1. Vulnerabilità

Le vulnerabilità si riferiscono alle debolezze dell'architettura hardware, dell'implementazione o dei processi di progettazione e/o di test. In una di queste fasi un operatore malintenzionato può attivare un attacco, o modificare la funzione per la quale il circuito è stato progettato. Questi punti deboli possono essere funzionali o non funzionali e variano in base alla natura di un sistema e ai suoi scenari di utilizzo. Un attacco tipico consiste nell'identificazione di una o più vulnerabilità, seguita dal loro sfruttamento per un attacco riuscito. L'identificazione è la prima delle fasi dell'iter di qualsiasi tipo di attacco.
Più in dettaglio, possiamo differenziare le tipologie di vulnerabilità in:

- **criticità funzionali:** la maggior parte delle vulnerabilità sono causate da pratiche di progettazione e di test inadeguate. Includono un'implementazione hardware crittografica debole e una protezione insufficiente delle risorse in un SoC. Gli aggressori possono rilevare queste vulnerabilità analizzando la funzionalità di un sistema per diverse condizioni di input per cercare eventuali comportamenti anomali;
- **criticità da side-channels:** rappresentano problemi a livello di implementazione. In questo contesto possono trapelare informazioni critiche memorizzate all'interno di un componente hardware attraverso diverse forme di canali laterali [11]. Gli aggressori possono rilevare queste vulnerabilità andando ad analizzare caratteristiche del circuito (anche durante il funzionamento dello stesso), apparentemente non correlate all'elaborazione della funzione che sta eseguendo l'hardware;
- **infrastrutture di test / debug:** in sede di test un operatore malintenzionato potrebbe utilizzare le infrastrutture adibite al debug del circuito in modo inappropriato. In particolare potrebbe estrarre informazioni sensibili dal momento che ha un accesso completo al sistema, concessogli dal momento che si è nel contesto di test e debug;

- **controllo degli accessi o flusso di informazioni:** un sistema potrebbe non distinguere tra utenti autorizzati e non autorizzati. Questa vulnerabilità può consentire a un utente malintenzionato di accedere a risorse e funzionalità private che possono essere sfruttate o utilizzate in modo improprio. Scenario peggiore sarebbe se si andasse a monitorare il flusso di informazioni durante il funzionamento del sistema, per poi decifrare informazioni critiche per la sicurezza (come il flusso di controllo di un programma e l'indirizzo di memoria di una regione protetta dell'hardware).

2.2. Contromisure

Le possibili contromisure possono essere impiegate nelle fasi di progettazione o di test.
Il flusso di manifattura di un SoC è costituito da quattro fasi concettuali: progettazione, pianificazione, sviluppo e produzione. Nelle prime due fasi viene definita l'architettura del circuito e quindi delineate le funzioni che l'hardware dovrà implementare. La fase di sviluppo consiste nella verifica degli obiettivi delineati in sede di progettazione. Se soddisfatti si procede con la fabbricazione dei chip.
La valutazione della sicurezza viene eseguita durante la fase di pianificazione, che identifica le risorse in un SoC, i possibili attacchi ad esse e i requisiti per l'esecuzione sicura del software. Questo passaggio va a creare una serie di requisiti di sicurezza. Successivamente, viene definita l'architettura ed eseguita la convalida della sicurezza per assicurarsi che l'implementazione soddisfi adeguatamente i requisiti desiderati. Un'analoga convalida della sicurezza viene eseguita dopo la fabbricazione dei chip, per garantire che gli stessi, una volta prodotti, non abbiano vulnerabilità. Queste tecniche includono la revisione del codice, la verifica formale durante la convalida, il *fuzzing* e i test di penetrazione [12].
Le pratiche di progettazione per la sicurezza (*Design for Security*, DfS) sono emerse come potenti contromisure e offrono spesso soluzioni di implementazione a basso *overhead* ed efficaci che forniscono una difesa attiva o passiva contro vari attacchi. Le tecniche DfS, come l'offuscamento [14][15], l'uso di primitive di sicurezza affidabili, la resistenza del canale laterale (ad esempio tecniche di mascheramento e occultamento) e schemi di protezione avanzata contro l'inserimento di trojan, possono proteggere in modo affidabile da molti dei principali vettori di attacco. Allo stesso modo, l'architettura di sicurezza SoC, resistente ad attacchi software, rappresenta la sicurezza del circuito stesso.

3. Hardware Trojans

Un HT viene definito come una modifica intenzionale e dannosa di un progetto di circuito che si traduce in un comportamento indesiderato quando il circuito viene distribuito [17]. I SoC "infettati" potrebbero subire modifiche nella loro funzionalità o specifiche. Ciò porterebbe alla divulgazione di informazioni sensibili dell'utente, o il circuito soffrirebbe di prestazioni degradate o inaffidabili. Il trojan hardware rappresenta una seria minaccia per qualsiasi progetto hardware implementato.

Essendo gli HT modifiche apportate direttamente al circuito, le contromisure software (*antivirus*) potrebbero essere inadeguate per affrontare la minaccia rappresentata dal trojan. Inoltre, il rilevamento di quest'ultimo in un progetto hardware non è banale dal momento che non sempre è disponibile una versione del circuito dove siamo sicuri non vi siano state manomissioni e con cui confrontare un determinato progetto durante la verifica.

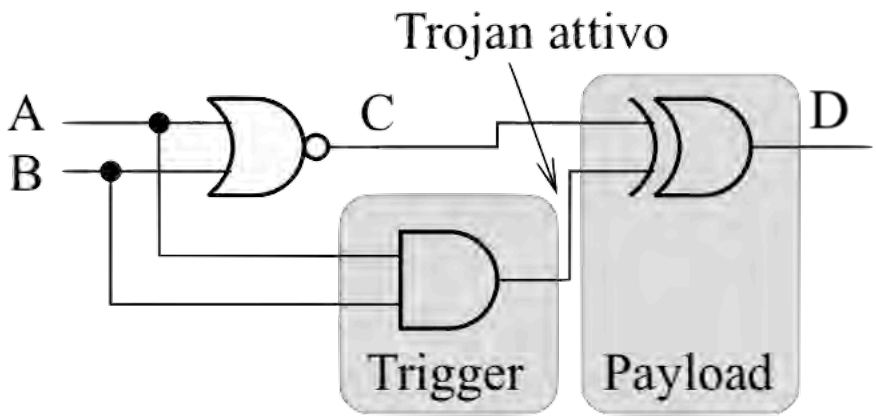

Figura 2 - *Esempio di implementazione di un HT*

La struttura di base di un HT può includere due parti principali, trigger e *payload* [16]. Il primo monitora segnali e/o una serie di eventi nel circuito. Il payload, invece, attinge ai segnali dal circuito originale e dall'uscita del trigger.
Nel momento in cui il trigger rileva un evento o una condizione per cui è stato predisposto l'innesco del trojan, il payload si attiva e viene boicottata l'esecuzione della funzione. Se il trojan è silente (ovvero quando il trigger non innesca il payload) il circuito si comporta come se fosse privo di manomissioni.

Tabella 1. Tabella della verità riferita al circuito in figura 2

A	B	C	D	Payload
0	0	1	1	Non attivo
0	1	0	0	Non attivo
1	0	0	0	Non attivo
1	**1**	**0**	**1**	**Attivo**

Come notiamo dalla tabella, il payload viene attivato nel momento in cui il valore di entrambi gli ingressi A e B è 1, altrimenti è silente. L'uscita del circuito (D) coincide con il segnale C, tranne quando il payload viene innescato. Un HT, quindi, può essere nascosto durante il normale funzionamento del chip e attivato solo quando viene applicata la condizione di innesco.

A questo proposito il trojan può essere attivato internamente (un evento verificatosi all'interno del circuito, o una particolare condizione circuitale, innesca il payload), o esternamente (una particolare valore di un input o un output di un componente del circuito).
Le possibili conseguenze del funzionamento di un circuito con un trojan attivo possono essere:

- **modifica delle funzionalità originarie:** il payload può modificare la funzionalità del dispositivo di destinazione e causare errori che potrebbero essere difficili da rilevare durante il test di produzione. Ad esempio, un trojan potrebbe far sì che un modulo di rilevamento degli errori accetti input che dovrebbero essere rifiutati;

- **fuga di informazioni:** un trojan può far trapelare dati attraverso canali sia nascosti che palesi. I dati sensibili possono essere diffusi tramite radiofrequenza, potenza ottica o termica, canali laterali di temporizzazione e interfacce I/O. Ad esempio, un trojan potrebbe far fruire all'attaccante la chiave di un algoritmo crittografico attraverso interfacce di uscita del sistema della vittima.

A quest'ultimo proposito, potrebbero essere estrapolati dati sensibili e/o privati, andando ad analizzare canali laterali. Anche se un circuito non è stato manomesso, un utente malintenzionato potrebbe fruire informazioni sui dati elaborati, andando ad osservare caratteristiche apparentemente non correlate all'esecuzione della funzione dell'hardware [18] (potenze dissipate, temperatura del chip, tempi di esecuzione, radiazioni elettromagnetiche).

4. Attacchi di tipo Side-Channel

Gli attacchi di tipo side-channel (SCA) sfruttano le informazioni fisiche che si osservano da fonti o canali indiretti, che apparentemente non dipendono dal funzionamento del circuito. Le informazioni fruite dall'analisi di questi parametri dipendono da valori intermedi, calcolati durante l'esecuzione di un algoritmo sull'hardware, e sono correlate con gli input del circuito stesso [19]. Un attaccante se osservando uno o più parametri "laterali" riuscisse a ricostruire una chiave crittografica segreta, potrebbe decriptare dati sensibili e privati. Per questi motivi, gli SCA rappresentano una grave minaccia per i dispositivi crittografici, in particolare smart card e dispositivi IoT, per i quali un utente malintenzionato potrebbe avere accesso a dati sensibili privati.
Gli attacchi comuni di tipo side-channel, come ad esempio gli attacchi alla potenza, monitorano il consumo di energia del dispositivo. Se consideriamo un dispositivo che sta effettuando una funzione di cifratura, il suo consumo energetico dipende dagli input della funzione crittografica. Per cifrare sequenze di bit differenti vengono dissipati valori di potenze diversi [20].

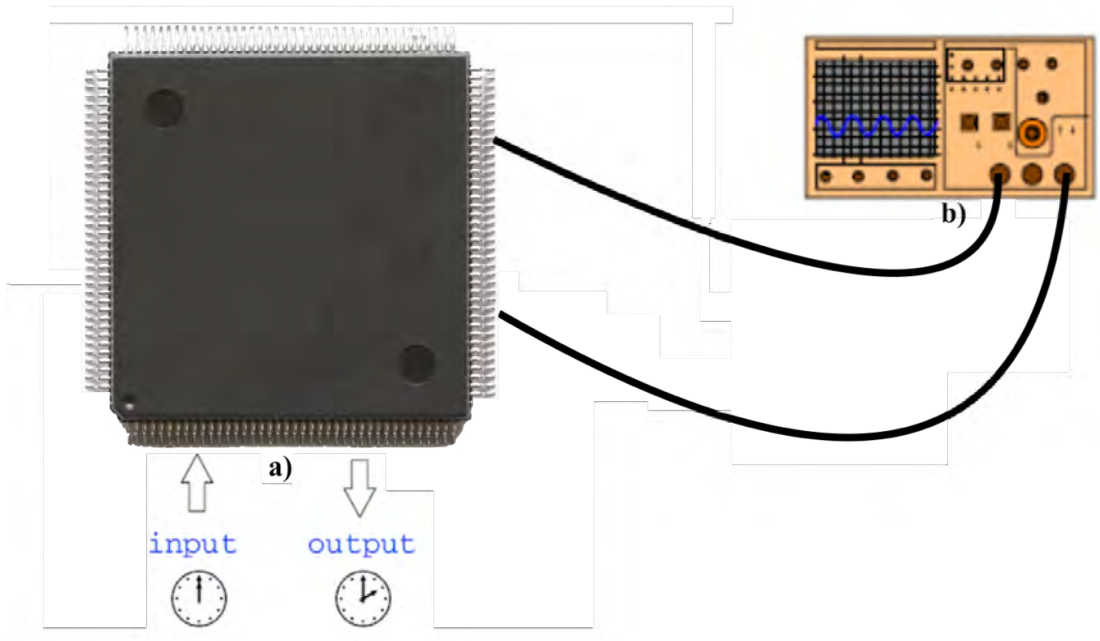

Figura 3 - *a) Chip sotto attacco, b) Oscilloscopio per analizzare le caratteristiche del circuito*

Un altro tipo di side-channel noto in letteratura è il *timing attack*. Ogni operazione eseguita in un dispositivo elettronico richiede una certa quantità di tempo per essere completata. Questo tempo può variare a seconda del tipo di operazione, dei dati di input, della tecnologia utilizzata per costruire il dispositivo e delle proprietà dell'ambiente in cui il dispositivo sta funzionando. Analizzando il tempo di esecuzione di ciascuna operazione in diverse configurazioni e schemi di input si possono ricavare informazioni cruciali [21][22].
Una possibile contromisura alle vulnerabilità a questo tipo di attacchi è la rimozione delle correlazioni tra gli input del circuito e le emissioni di tipo side-channel. Al variare dei dati in input al sistema possiamo pensare di mantenere costante sia la potenza dissipata dal chip [15], che i tempi di esecuzione delle istruzioni/operazioni [22]. Inoltre, pensando di partizionare il design dell'hardware, si potrebbero individuare due regioni diverse del circuito: una costituita da moduli che elaborano i dati cifrati ed un'altra che opera sui dati in chiaro.

5. Contromisure architetturali

Una nuova tendenza per garantire la sicurezza dell'hardware è l'inserzione nel circuito di moduli che implementano algoritmi probabilistici, servendosi di funzioni di hash. Questi possono essere aggiunti al circuito per rilevare l'eventuale presenza di trojan, o per segnalare attacchi di tipo side-channel [23][24][25]. Lo scopo di questi moduli è semplicemente quello di stimare alcuni parametri. La forza di questi approcci è il loro minimo overhead introdotto in termini di area e tempi per l'elaborazione.

Nei prossimi paragrafi vengono presentate due metodologie circuitali con le quali sarebbe possibile identificare con la prima HT un attacco di tipo *man in the middle* [28] e con la seconda un attacco di tipo side-channel.
Consideriamo, per esempio, il caso in cui un operatore malizioso, durante una delle fasi di produzione del chip, abbia manomesso il circuito. In particolare supponiamo abbia interposto un modulo hardware tra la memoria di un processore ed il core. Questa manomissione va a modificare le corrispondenze tra i dati e i relativi indirizzi di memoria in cui sono stati scritti precedentemente. In sede di scrittura della memoria si avranno determinate corrispondenze tra dati ed indirizzi; nel processo di lettura, con il payload del trojan attivo, la corrispondenza non sarà più la medesima. Per rilevare questo tipo di manomissioni è necessario, in primo luogo osservare a quali indirizzi della memoria vengono scritte le singole stringhe di dati ed in seguito controllare se vi è la medesima corrispondenza quando il core le legge. A questo proposito possono essere sfruttate le architetture basate sull'elaborazione di algoritmi probabilistici.

5.1. Checker di hardware trojan basato su filtro di Bloom

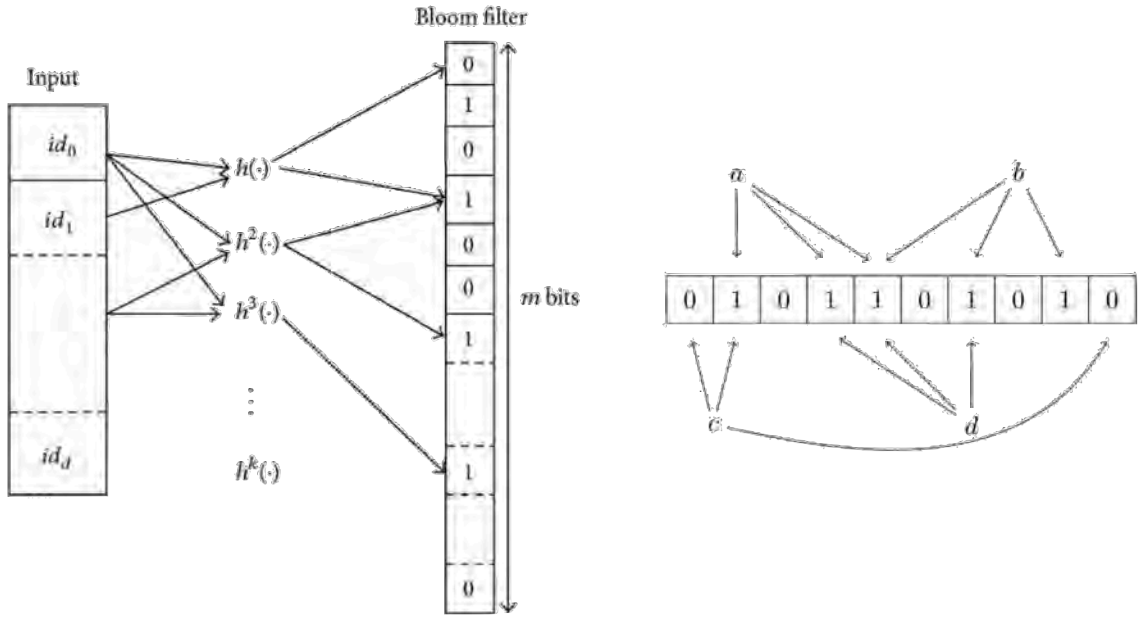

Figura 4 - *Processo di push a sinistra, processo di pull a destra (a e b risultano presenti nel set, c e d no)*

I filtri di Bloom sono strutture di dati probabilistiche utili per verificare se un elemento è presente in un determinato insieme di dati [26].
Questo tipo di struttura genera la presenza di falsi positivi, ma non consente la possibilità di falsi negativi. Se viene rilevato che un elemento non è nell'insieme, questo risultato è certamente vero, altrimenti abbiamo solo la possibilità che l'elemento sia realmente nel set. Pertanto gli elementi possono essere inseriti nel set, durante il processo di *push*, ma non possono essere rimossi. In secondo luogo, durante la fase di *pull* avviene il controllo dell'effettiva

presenza del dato nel set iniziale o meno. La probabilità di falsi positivi aumenta con il numero di inserimenti. Questi due processi sono illustrati nella figura 4.
Facciamo riferimento all'HT di tipo man in the middle sopracitato, in un contesto di scrittura e lettura di istruzioni di un determinato programma nella memoria istruzioni di un processore. Si può implementare un Filtro di Bloom che abbia come dataset in ingresso la concatenazione delle singole istruzioni e il loro relativo indirizzo di scrittura nella memoria (figure 5 e 6).

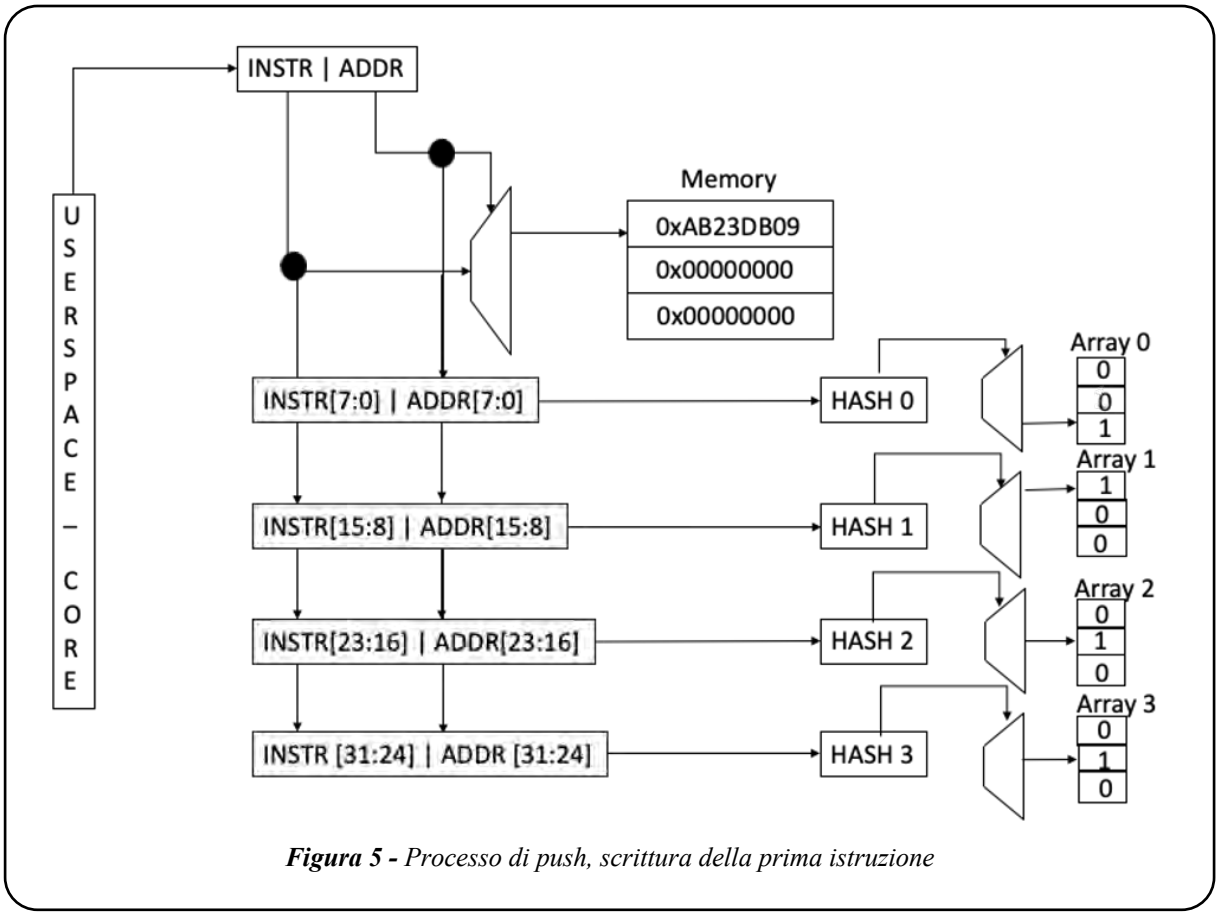

Figura 5 - *Processo di push, scrittura della prima istruzione*

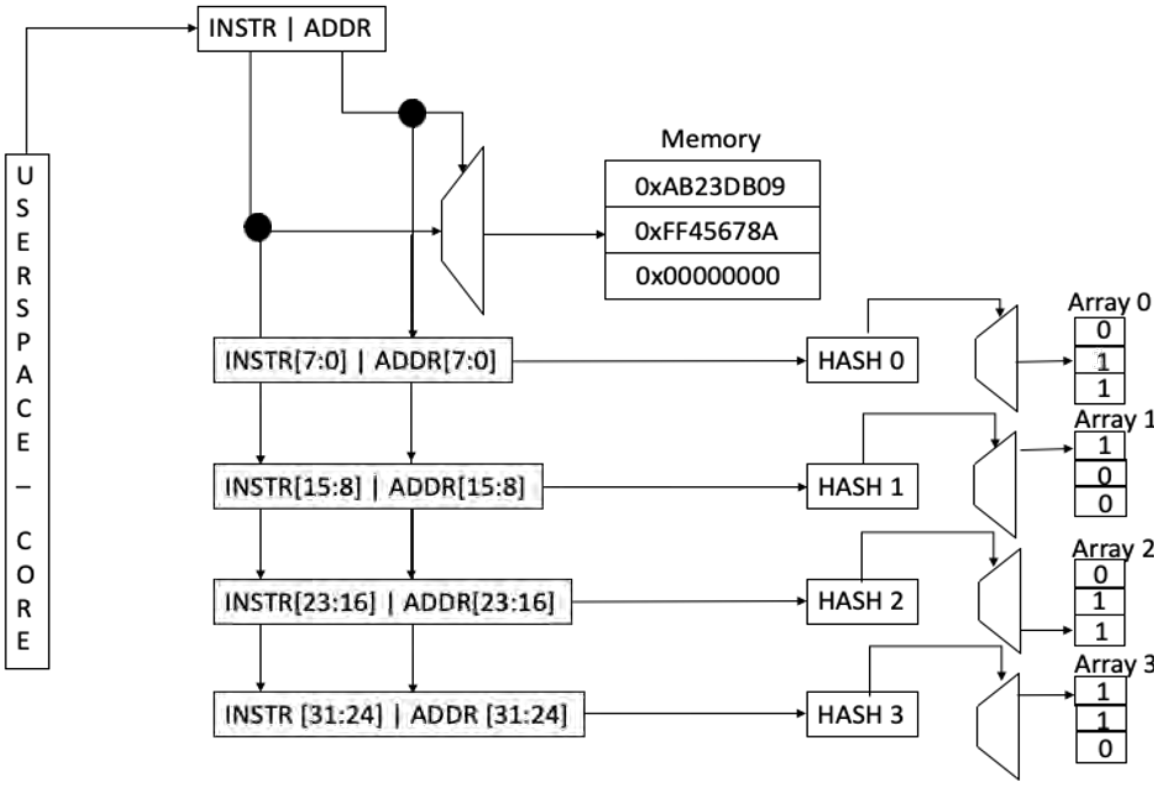

Figura 6 - *Processo di push, scrittura della seconda istruzione*

Più in dettaglio, consideriamo istruzioni ed indirizzi, provenienti dall'*userspace* o dal core, ciascuno a 32 bit. Dividiamo le singole concatenazioni [istruzione | indirizzo], in quattro segnali da 16 bit ciascuno, 8 bit del valore dell'indirizzo e 8 bit del valore dell'istruzione. Costituiamo il Filtro di Bloom con quattro vettori (inizializzati a 0) ed altrettante funzioni di hash che avranno in input le diverse concatenazioni.

Durante il processo di push, l'output della funzione di hash andrà ad indirizzare il relativo vettore e porrà un 1 in corrispondenza della locazione puntata; lascerà 0 nelle locazioni che non vengono indirizzate, ovvero:

$$Array_i[Address_j] = 1$$
$$Address_j = Hash_i(Instr[m:n]_j \mid AddrOfInstr[m:n]_j)$$

Set 1 di equazioni

$$BitArray_i[Address_j] = Array_i[Address_j]$$
$$Address_j = Hash_i(DataMemory[m:n]_j \mid AddrOfInstr[m:n]_j$$
$$AddressOfInstr = AddressOfDataMemory$$
$$Warning = \prod \overline{BitArray_i} = 0$$

Set 2 di equazioni

Una volta terminata l'intera scrittura delle istruzioni in memoria, in sede di esecuzione del programma, ha luogo la fase di pull del filtro di Bloom. In questo processo vi è una differente concatenazione: gli indirizzi continuano ad essere considerati quelli provenienti da userspace e/o core, ma le istruzioni provengono dall'output della memoria. In assenza di manomissioni verranno puntate le locazioni dei vettori dove vi è stato posto precedentemente il valore 1 (la corrispondenza coincide con quella in fase di scrittura, come notiamo nella figura 7 e nel set 2 di equazioni).
Nel caso in cui vi fosse un trojan, che ad esempio somma un valore costante all'indirizzo dal quale si vuole leggere, in output alla memoria sarà posta l'istruzione relativa all'indirizzo specificato più l'offset dato dal trojan, ovvero:

$$BitArray_i[Address_j + T] = Array_i[Address_j]$$
$$Address_j = Hash_i(DataMemory[m:n]_j \mid AddrOfInstr[m:n]_j$$
$$AddressOfInstr \neq AddressOfDataMemory$$
$$Warning = \prod \overline{BitArray_i} = 1$$

Set 3 di equazioni

In questo scenario sicuramente non vi sarà corrispondenza e nel filtro di Bloom verrà puntata almeno una locazione dove non è stato scritto 1 nel processo di push. Un segnale di warning che valga 1 quando viene puntata almeno una locazione degli array contenente uno 0, può essere implementato ponendo in ingresso ad una porta *NAND* bit presenti nei vettori (figure 7 e 8).
In [27] viene riportato un'altra implementazione, basata su un filtro di Bloom, per la rilevazione di errori nelle istruzioni.

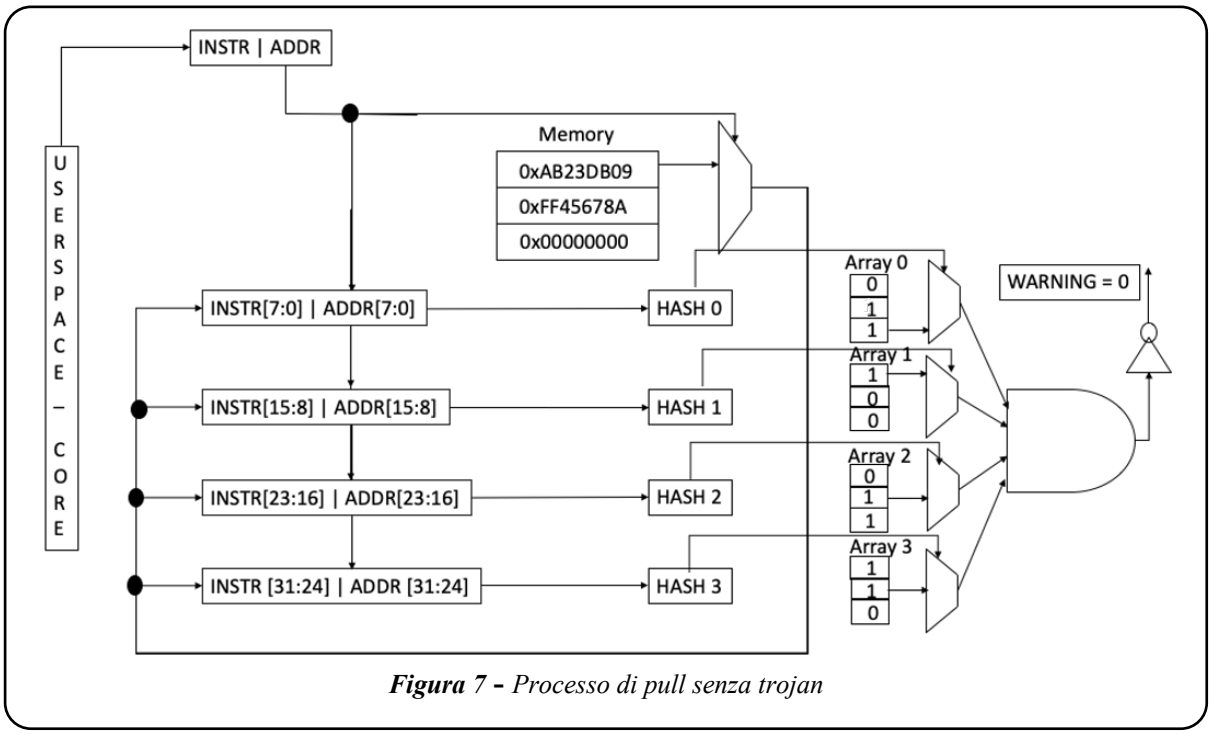

Figura 7 - *Processo di pull senza trojan*

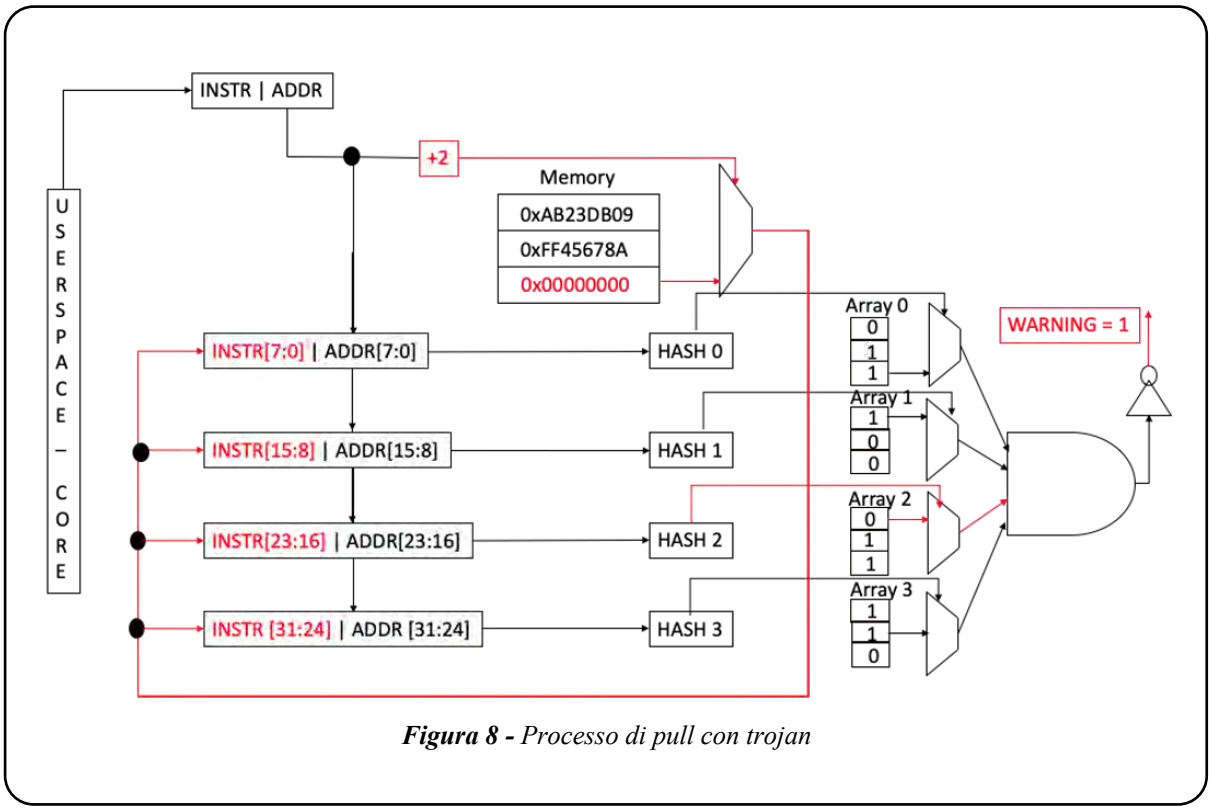

Figura 8 - *Processo di pull con trojan*

5.2. Checker di attacchi di tipo side-channel basato su Count-min sketch

La struttura *count-min sketch* consiste nell'elaborazione probabilistica di dati [29]. Viene adottata per contare il numero di volte che un elemento è presente in un set [30].
Gli elementi costitutivi del dataset vengono inseriti in una matrice. L'obiettivo di questa architettura è tenere traccia di un flusso di eventi e contare la frequenza dei differenti eventi appartenenti al medesimo flusso. Nel momento in cui si presenta un nuovo evento di tipo w, per ciascuna riga d della matrice, viene puntata la locazione corrispondente all'output della funzione di hash relativa, ovvero $K = Hash_d(w)$. Quindi viene incrementato di uno il valore della locazione K. Questo tipo di architetture può essere utile per rilevare precisi pattern di stream: ogni volta che viene presentato un dato in ingresso verranno incrementate determinate locazioni dello sketch. Inoltre viene registrato anche quante volte si è presentato quel particolare pattern.

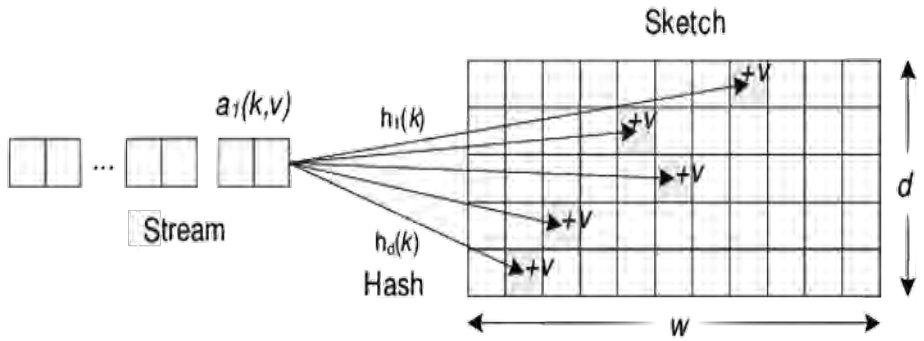

Figura 9 - *Processo di inserzione count-min sketch*

Inserendo un'architettura basata su count-min sketch in un processore si possono andare, ad esempio, a contare quante (e quali) istruzioni vengono eseguite. Consideriamo il caso in cui un attaccante abbia installato un software maligno nella memoria del mio core. In particolare facciamo riferimento ad attacchi dove, per diversi scopi, vengono eseguite molteplici volte le medesime istruzioni: Spectre [1] e Orchestration [31] effettuano accessi alla cache in *loops*; Battery Drain [32] esegue la medesima operazione (anche una *NOP* ad esempio), affinché il sistema non vada in *sleep mode* e di conseguenza dissipi potenza.
L'idea consiste nel disporre di una circuiteria che rilevi differenti pattern di istruzioni, quindi che sia programmabile. Il programmatore può specificare di quali opcode si vogliono contare le ricorrenze, settarne il valore massimo (*threshold*) ed impostare ogni quanto tempo resettare i valori dei contatori. Nella figura 10 vi è il *workflow* dell'architettura implementata (figura 11). In primis vengono resettati i valori dei contatori, dopo la programmazione del modulo (4) della figura 11. Durante l'esecuzione del programma, le istruzioni vengono passate al side-channel checker, che effettuerà differenti hash function per la ciascuna istruzione. Gli output di queste funzioni punteranno a determinati contatori che vengono incrementati istruzione dopo

istruzione. Una volta scaduto il *timeout*, se si verifica che i valori dei contatori eccedono il threshold precedentemente impostato ed inoltre vi è corrispondenza tra gli opcode definiti dal programmatore e quelli delle istruzioni eseguite, verrà attivato un segnale di warning, altrimenti si ripete il workflow inizializzando nuovamente il valore dei contatori.

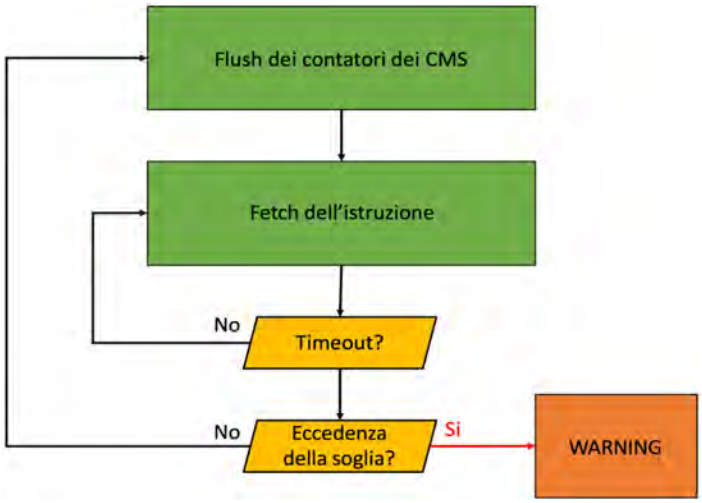

Figura 10 - *Workflow della funzione che implementa il side-channel checker*

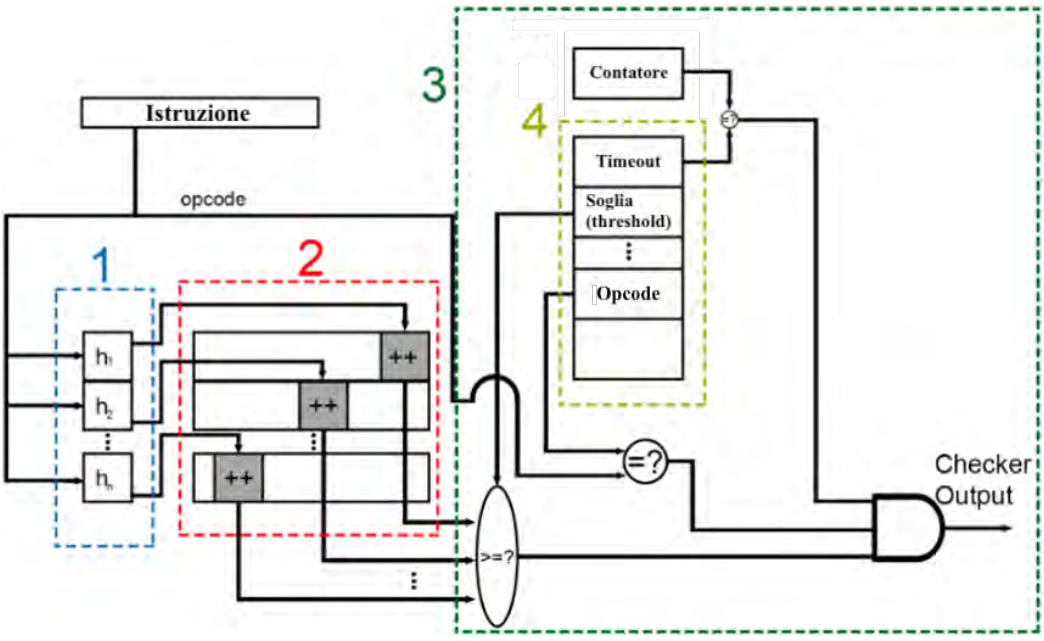

Figura 11 - *Architettura della circuiteria basata su count-min sketch. (1) Hash functions, (2) contatori, (3) attivazione del checker, (4) campi programmabili dall'utente*

5.3. Analisi delle implementazioni dei checker

Entrambe le circuiterie dei checker sono state integrate in *ibex* [33]: un prototipo di processore a 32 bit basato su un'architettura di tipo RISC-V, con due stage di pipeline e una memoria (istruzioni e dati) totale di 256Kbit. In particolare sono state posizionate delle istruzioni tra il core e la memoria. Le simulazioni sono state effettuate in un primo momento su Verilator [34], successivamente su Vivado [35]. Tramite quest'ultimo tool i checkers sono stati implementati su FPGA. Di seguito vengono riportati i numeri delle implementazioni:

Tabella 2 *risorse implementate*

	LUT	**Flip Flop**	**Celle BRAM**
Core	2519 (70%)	1590 (57.5%)	256 (96.5%)
Filtro di Bloom	91 (2.5%)	39 (1.5%)	6.5 (2.6%)
Count-min sketch	992 (27.5%)	936 (36.5%)	2.5 (0.9%)
Totale	3602 (100%)	2565 (100%)	265 (100%)

Sia l'architettura basata sul filtro di Bloom che quella basata sull'algoritmo di count-min sketch, sono indipendenti dalla piattaforma e possono essere impiegate tra il core e la memoria di processore, indipendentemente dagli stadi di pipeline, il numero di bit e le dimensioni della memoria.

6. Conclusioni

Con l'aumento esponenziale del volume dei dispositivi elettronici connessi ad Internet, garantire la sicurezza dei dati digitali è cruciale. L'hardware gioca un ruolo sempre più importante e fondamentale in questo scenario. Non si può dare per scontato che la circuiteria dove viene eseguito un algoritmo sia affidabile. Infatti, il circuito potrebbe essere stato manomesso e/o presentare molteplici vulnerabilità.

A questo proposito abbiamo proposto due architetture hardware da integrare in un processore, dove la prima (basata sui filtri di Bloom) rileva una possibile manomissione della circuiteria tra la memoria e core; la seconda (basata sull'algoritmo di count-min sketch) segnala l'eventuale fruizione di informazioni, non lecita, da parte di un utente malintenzionato.

Per essere certi che il chip prodotto svolga effettivamente la funzione desiderata possono essere integrati al suo interno moduli come quelli proposti.

Così come in una catena, la sicurezza di un sistema informatico dipende dalla sicurezza del suo componente più vulnerabile. Tali vulnerabilità spesso si nascondono dietro ai dettagli implementativi del circuito e dell'algoritmo in esecuzione e vanno accuratamente tenute in considerazione in fase progettuale con approcci di design for security.

Riferimenti bibliografici

[1] Kocher, J. Horn, A. Fogh, , D. Genkin, D. Gruss, W. Haas, M. Hamburg,M. Lipp, S. Mangard, T. Prescher, M. Schwarz, and Y. Yarom, "Spectre attacks: Exploiting speculative execution" in 40th IEEE Symposium on Security and Privacy (S&P'19), 2019.

[2] M. Lipp, M. Schwarz, D. Gruss, T. Prescher, W. Haas, A. Fogh,J. Horn, S. Mangard, P. Kocher, D. Genkin, Y. Yarom, and M. Hamburg,"Meltdown: Reading kernel memory from user space" in 27th USENIX Security Symposium (USENIX Security 18), 2018.

[3] L. Wang and S. K¨ose, "When hardware security moves to the edge and fog," in2018 IEEE 23rd International Conference on Digital Signal Processing (DSP), 2018, pp. 1–5.

[4] S. R. Chhetri, S. Faezi, N. Rashid, and M. A. Al Faruque, "Manu-facturing supply chain and product lifecycle security in the era of industry 4.0,"Journal of Hardware and Systems Security, vol. 2, no. 1,pp. 51–68, 2018.

[5] D. K. Oka, "Securing the automotive critical infrastructure," in Cyber-Physical Security. Springer, 2017, pp. 267–281.

[6] NIST-FIPS, "Announcing the advanced encryption standard (AES),"Federal Information Processing Standards Publication, vol. 197,no. 1-51, pp. 3–3, 2001.

[7] R. L. Rivest, A. Shamir, and L. Adleman, "A method for obtaining digital signatures and public-key cryptosystems,"Commun. ACM,vol. 21, no. 2, pp. 120–126, Feb. 1978. [Online]. Available:http://doi.acm.org/10.1145/359340.359342

[8] "sha-3 standard: Permutation-based hash and extendable output functions."

[9] M. Joye andet al., Fault analysis in cryptography Springer, 2012,vol. 147.

[10] R. Spreitzer, V. Moonsamy, T. Korak, and S. Mangard, "Systematic classification of side-channel attacks: A case study for mobile devices,"IEEE Communications Surveys Tutorials, vol. 20, no. 1, pp.465–488, 2018.

[11] F. Koeune, F.X. Standaert, A tutorial on physical security and side-channel attacks, in: Foundations of Security Analysis and Design III, 2005, pp. 78–108.

[12] P. Kocher, J. Jaffe, B. Jun, Differential power analysis, in: CRYPTO, 1999.

[13] F. Wang, Formal Verification of Timed Systems:A Survey and Perspective, Proceedings of the IEEE (2004) 1283–1305.

[14] A. Vijayakumar, V.C. Patil, D.E. Holcomb, C. Paar, S. Kundu, Physical design obfuscation of hardware: a comprehensive investigation of device and logic-level technique, IEEE Transactions on Information Forensics and Security (2017) 64–77.

[15] D. Zoni, L. Cremona and W. Fornaciari, "All-Digital Control-Theoretic Scheme to Optimize Energy Budget and Allocation in Multi-Cores," in IEEE Transactions on Computers, vol. 69, no. 5, pp. 706-721, 1 May 2020, doi: 10.1109/TC.2019.2963859.

[16] A. Nahiyan, M. Tehranipoor, Code coverage analysis for IP trust verification, in: Hardware IP Security and Trust, Springer, 2017, pp. 53–72.

[17] K. Xiao, D. Forte, Y. Jin, R. Karri, S. Bhunia, M. Tehranipoor, Hardware Trojans: lessons learned after one decade ofresearch, ACM Transactions on Design Automation of Electronic Systems 22 (2016) 6.

[18] A. P. Fournaris, L. Pocero Fraile, and O. Koufopavlou, "Exploiting hardware vulnerabilities to attack embedded system devices: a survey of potent microarchitectural attacks", Electronics, vol. 6,no. 3, p. 52, 2017.

[19] A. Barenghi, L. Breveglieri, I. Koren, D. Naccache, Fault Injection Attacks on Cryptographic Devices: Theory, Practice, and Countermeasures, Proceedings of the IEEE 100 (11) (2012) 3056–3076.

[20] C. Luo, Y. Fei, P. Luo, S. Mukherjee, and D. Kaeli, "Side-channel power analysis of a gpu AES implementation," in2015 33rd IEEE International Conference on Computer Design (ICCD).IEEE, 2015,pp. 281–288.

[21] P. Kocher, Timing Attacks on Implementations of Diffie–Hellman, RSA, DSS, and Other Systems, in: Advances in Cryptology CRYPTO96, Springer, 1996, pp. 104–113.

[22] Canvel B., Hiltgen A., Vaudenay S., Vuagnoux M. (2003) Password Interception in a SSL/TLS Channel. In: Boneh D. (eds) Advances in Cryptology - CRYPTO 2003. CRYPTO 2003. Lecture Notes in Computer Science, vol 2729. Springer, Berlin, Heidelberg. https://doi.org/10.1007/978-3-540-45146-4_34.

[23] Pedro Reviriego Vasallo, "Bloom Filters: Dependability and Security", Seminar at Tor Vergata, 16 November 2020.

[24] Reviriego Pedro, et al. "A method to protect Bloom filters from soft errors." 2015 IEEE International Symposium on Defect and Fault Tolerance in VLSI and Nanotechnology Systems (DFTS). IEEE, 2015.

[25] Reviriego Pedro, Jorge A. Martinez, and Marco Ottavi. "Soft Error Tolerant Count Min Sketches." IEEE Transactions on Computers, 2020.

[26] Bloom Filters — A Tutorial, Analysis, and Survey (Blustein & El-Maazawi, 2002)

[27] Atamaner, Mert & Ergin, Oguz & Ottavi, Marco & Reviriego, Pedro. (2017). Detecting errors in instructions with bloom filters. 1-4. 10.1109/DFT.2017.8244458.

[28] What is man-in-the-middle attack (MitM)? - Definition from WhatIs.com, su IoT Agenda. URL consultato il 2 dicembre 2020.

[29] Cormode, Graham (2009). "Count-min sketch". Encyclopedia of Database Systems. Springer. pp. 511–516.

[30] Cormode, Graham; S. Muthukrishnan (2005) "An Improved Data Stream Summary: The Count-Min Sketch and its Applications". J. Algorithms. 55: 29–38. doi:10.1016/j.jalgor.2003.12.001.

[31] M. R. Fadiheh, D. Stoffel, C. Barrett, S. Mitra, and W. Kunz.(2018, Dec.) Processor hardware security vulnerabilities and theirdetection by unique program execution checking. 1812.04975.pdf

[32] R. Smith, D. Palin, P. Ioulianou, V. Vassilakis, and S. Shahandashti,“Battery draining attacks against edge computing nodes in IoT networks,” 01 2020.

[33] https://github.com/lowRISC/ibex#ibex-risc-v-core, 18 December 2020

[34] https://www.veripool.org/wiki/verilator/Manual-verilator, 18 December 2020

[35] https://www.xilinx.com/products/design-tools/vivado.html, 18 December 2020

DVB-T2: Sperimentazione sulle potenziali interferenze LTE 700 MHz sugli impianti di ricezione televisiva

DVB-T2: Laboratory simulation on potential 700 MHz LTE interference on television reception systems

Gianmarco Fusco■*, Massimo Ferrante*■

■ *DGTCSI – ISCTI*

Sommario

Il continuo aumento del traffico dei dati trasmessi a banda larga senza fili e la sempre più crescente importanza della digitalizzazione sul piano economico, industriale e sociale, sono il traino per massicci investimenti nel potenziamento delle reti radiomobili in termini di affidabilità, capacità e velocità. L'indagine relaziona sui risultati ottenuti a seguito di una sperimentazione, svolta in modalità condotta, sugli effetti dei segnali del radiomobile LTE in banda 700 MHz sugli impianti TV riceventi i segnali del digitale terrestre di seconda generazione in banda 600 MHz.

Abstract

The incessant increase in wireless broadband transmitted data traffic and the growing importance of digitization in economic, industrial and social terms, are the driving force for massive investments in the upgrading, in terms of reliability, capacity and speed, of mobile radio networks. The research reports on the outcomes obtained as a result of a type of experimentation conducted on the effects of the LTE mobile radio signals in the 700 MHz band, on TV systems receiving the signals of the second generation digital terrestrial in the 600 MHz band.

1. Introduzione

L'Unione Europea, con una decisione del 2012 [1] del Parlamento europeo e del Consiglio, ha disposto di "cercare di assegnare tempestivamente uno spettro radio sufficiente e adeguato per sostenere gli obiettivi strategici dell'Unione e rispondere al meglio alla domanda di traffico di dati senza fili", quantificando la porzione di bande di frequenze da destinare a tale scopo in almeno 1200 MHz.

In una comunicazione del 6 maggio 2015 [2] la Commissione ha evidenziato l'importanza della banda dei 700 MHz che andrebbe assegnata per la fornitura di servizi di comunicazioni elettroniche a banda larga nelle zone rurali poiché porzione di spettro particolarmente adatto.

Ciò consentirà altresì lo sviluppo, la realizzazione e l'applicazione di nuovi servizi digitali come ad esempio i sistemi di reti elettriche dotate di sensori intelligenti, le telecomunicazioni in ambito sanitario, la guida automobilistica controllata via radio senza pilota, l'automazione industriale.

I Regolamenti radio dell'Unione Internazionale delle Telecomunicazioni, adottati dalla Conferenza mondiale delle radiocomunicazioni del 2015 (WRC-2015), hanno previsto per la Regione 1 (in cui si trova l'Italia) l'assegnazione della banda di frequenze dei 700 MHz ai servizi di trasmissione radiomobili. La CEPT ha identificato con ECC Decision (15)01, approvata il 6 marzo 2015 [3], due bande di 30 MHz all'interno della banda 700 da dedicare all'uplink ed al downlink delle reti di comunicazioni mobili/fisso.

Tale porzione di spettro attualmente è utilizzata a livello nazionale in modo massivo dai servizi di radiodiffusione televisiva terrestre. Il Parlamento Europeo e il Consiglio hanno previsto, con una decisione di maggio 2017 [4], il termine del 2020 per la liberazione della banda 700 MHz con la flessibilità di due anni per gli Stati membri che adducano giustificate ragioni tra le quali la necessità e la complessità di assicurare la migrazione tecnica di un'ampia fetta di popolazione verso standard di trasmissione avanzati.

Con la Legge di Bilancio 2018 [5], in Italia, è stato indicato che entro il 1° luglio 2022 si proceda alla migrazione dei programmi trasmessi attraverso multiplexer televisivi attualmente presenti in banda 700 MHz verso frequenze inferiori. La nuova attribuzione della banda 700 MHz ai servizi radiomobili potrà avere impatto sul corretto funzionamento degli impianti di ricezione televisiva che sono attualmente predisposti per ricevere in parte sino al canale 60 (frequenza centrale 786 MHz) ed in parte ancora sino al canale 69 (frequenza centrale 858 MHz) a seconda che sia stato dato seguito o meno ad un loro adeguamento, attraverso l'installazione di filtri appropriati [6] conseguente all'assegnazione della banda 800 MHz ai servizi radiomobili di quarta generazione (LTE).

Il Ministero dello sviluppo economico con proprio decreto datato 8 agosto 2018 [7], come richiesto dalla decisione UE 2017/899 [4], ha stabilito tra l'altro la road map per la liberazione della banda 700 MHz a favore dei servizi 5G con l'indicazione di scadenze intermedie e finali per il rilascio. Il medesimo decreto ha fissato che "[…] in coincidenza con l'avvio delle attività del periodo transitorio stesso nell'Area 1 […], è disposta sull'intero territorio nazionale la dismissione della codifica MPEG-2 in favore della codifica MPEG-4 su standard DVB-T"

Con ulteriore decreto, datato 19 giugno 2019 [10], il Ministero dello Sviluppo Economico ha aggiornando la roadmap, prevedendo, all'art. 6 comma 3, che "Al termine delle operazioni di transizione delle reti alla struttura dei multiplex definita dal PNAF, è disposta l'attivazione dello standard DVB-T2 a livello nazionale, nel periodo tra il 21 giugno 2022 e il 30 giugno 2022".

La sperimentazione di seguito illustrata è finalizzata alla verifica della coesistenza del servizio radiomobile LTE, che è stato ritenuto essere, tra i servizi attualmente disponibili ai fini di questo test, quello che più si avvicina a simulare il segnale che si prevede sarà offerto in banda 700 MHz, e del servizio di radiodiffusione che continuerà ad essere assegnatario della banda

adiacente inferiore ancora per diversi anni (figura 1) trasmesso in DVB-T2, tecnica che si ritiene che verrà utilizzata in modo preponderante, se non esclusivo, subito dopo la definitiva liberazione della banda considerata.

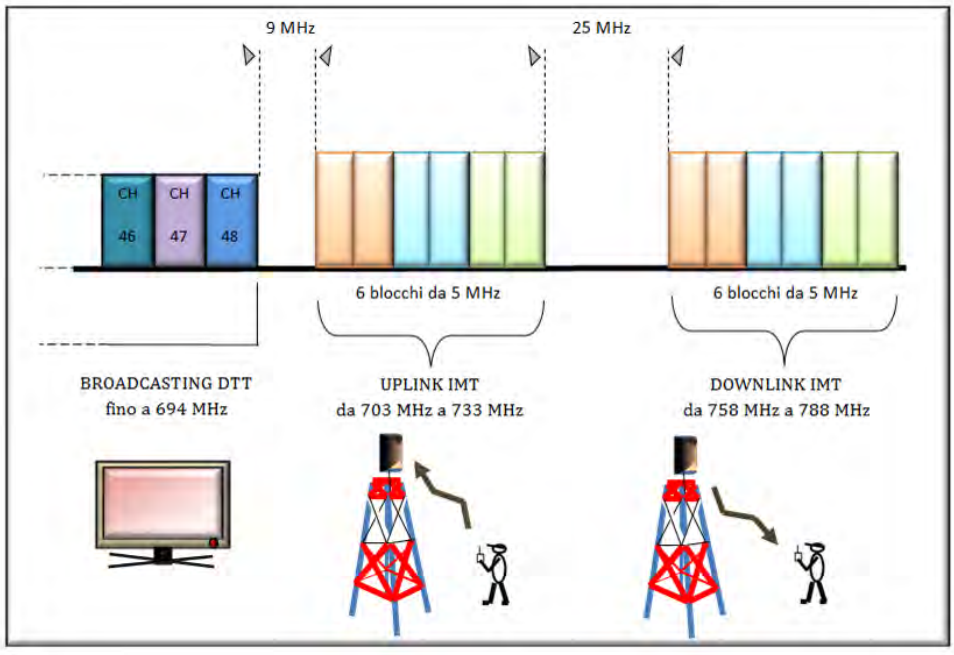

Figura 1 - *Situazione spettrale in banda UHF (radiodiffusione televisiva e radiomobile)*

Le verifiche e le misurazioni sono state effettuate in modo condotto attraverso l'utilizzo di un banco di prove predisposto presso i laboratori della Direzione generale per le tecnologie delle comunicazioni e la sicurezza informatica - Istituto superiore delle comunicazioni e delle tecnologie dell'informazione (di seguito DGTCSI - ISCTI) del Ministero dello sviluppo economico.

2. Scenario interferenziale e banco di simulazione Utilizzo

Con il prossimo utilizzo della banda 700 MHz da parte dei servizi di comunicazione elettronica a banda larga si potrebbe presentare, in Italia, una problematica interferenziale all'ingresso di un impianto ricevente il segnale digitale terrestre del broadcasting televisivo. I segnali, che permetteranno la propagazione dei due servizi, radiomobile in banda 700 MHz (in downlink ed in uplink) e radiotelevisivo dalla banda VHF fino a frequenze prossime alla banda 700 MHz, si troveranno ad essere ricevuti dall'antenna di un impianto tv che è realizzato per la ricezione della terza banda VHF e la quarta e quinta banda UHF fino alla frequenza di 790 MHz, nel caso migliore, e fino alla frequenza di 862 MHz in quello peggiore.

La sperimentazione di seguito illustrata ha preso in considerazione l'eventualità delle possibili interferenze che si possono verificare su tali impianti mentre ricevono segnali televisivi trasmessi in tecnica di modulazione DVB-T2 nella banda 600 MHz. Lo studio ha riguardato le interferenze provocate da segnali LTE, precipuamente in trasmissione uplink (da terminale d'utente a stazione radio base) e che occupano, alternativamente o simultaneamente, la parte iniziale della banda 700 MHz (da 703 MHz a 733 MHz). E' stato in seguito dato un piccolo sguardo anche alla possibile interferenza da trasmissioni LTE in downlink (da 758 MHz a 788 MHz). Nel laboratorio di radiodiffusione sonora e televisiva della DGTCSI - ISCTI è stato predisposto appositamente un banco di simulazione per la generazione dei due segnali in questione (Figura 2). Tali segnali, miscelati, vengono presentati via cavo all'ingresso d'antenna del ricevitore televisivo (DUT).

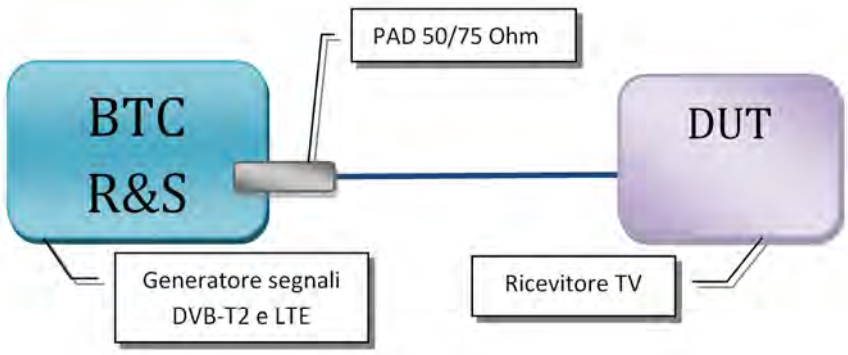

Figura 2 - *Banco di simulazione del laboratorio Radiodiffusione - DGTCSI - ISCTI*

L'analisi ha riguardato la determinazione dei livelli interferenziali del segnale LTE in *uplink* ed in *downlink* che hanno generato *macroblocking* (artefatti) nelle immagini video riprodotte sugli schermi televisivi. La rilevazione della misura è stata effettuata al verificarsi del *macroblocking* (Figura 3) seguendo il criterio indicato nella norma tecnica armonizzata ETSI EN 303 340 V1.1.2 (2016-09) ovvero la prima ripetizione di degradazione dell'immagine occorsa all'interno di un periodo d'osservazione di 15 secondi - *onset* of *picture degradation* [8]. Le prove eseguite hanno prodotto altresì l'individuazione del rapporto di protezione, definito come il valore minimo del rapporto tra il segnale voluto, in questo caso il segnale televisivo, ed il segnale indesiderato del servizio radiomobile in corrispondenza della soglia di degradamento su indicata. Il valore viene misurato all'ingresso del dispositivo sotto prova. Nel presente documento è stato utilizzato l'inverso di tale rapporto per una migliore gestione grafica dei risultati.

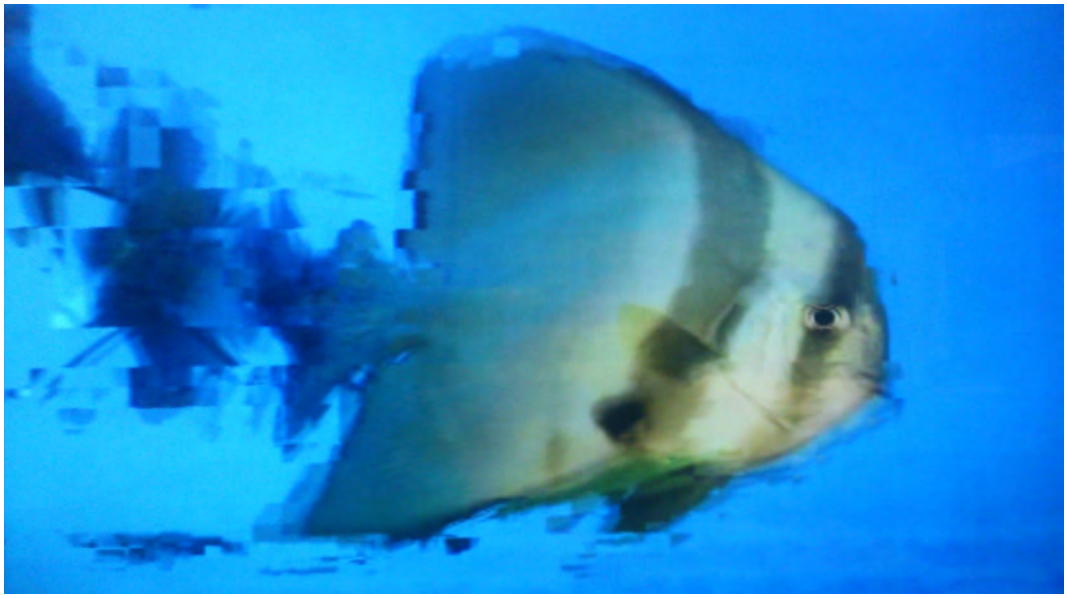

Figura 3 - *Esempio di macroblocking su schermo televisivo*

Per quanto riguarda gli aspetti della trasmissione in *uplink* del segnale potenzialmente interferente, è stata presa in considerazione la forma d'onda indicata dall'ETSI in allegato alla norma armonizzata EN 303 340 e denominata "short_UE-Video-Stream_V2". Essa ha una larghezza di banda di 10 MHz ed è rappresentativa del traffico del terminale che si viene a generare in una reale trasmissione di streaming video, con un segnale trasportato da una rete mobile LTE di banda 800 MHz e trasmesso dai moderni *smartphones* 4G [8]. Il segnale è stato centrato, per la sperimentazione, alle frequenze di 708 MHz, 718 MHz e 728 MHz.

Di seguito, in Figura 4, viene mostrato un esempio di spettro del segnale LTE in trasmissione *uplink* ottenuto monitorando la forma d'onda su un analizzatore di spettro impostato secondo la norma armonizzata [8].

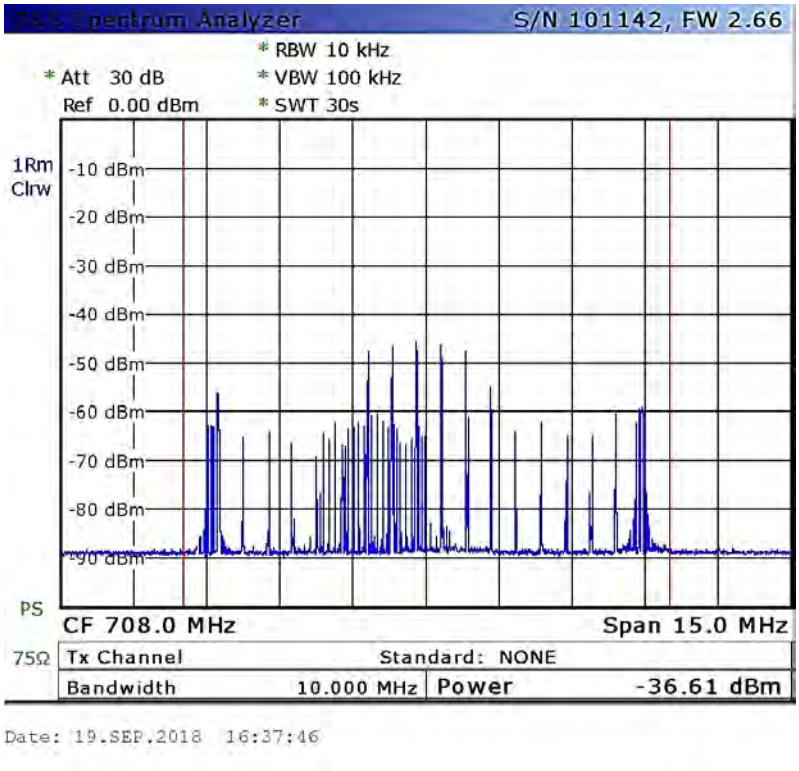

Figura 4 - *Spettro del segnale LTE Uplink (ETSI EN 303 340)*

Anche nel caso di studio di interferenza da LTE *downlink* sono stati presi segnali campione indicati dalla norma armonizzata europea [8], e si tratta di quelli denominati "LTE_BS-100PC_synth" nel caso di traffico pari al 100% e "LTE_BS_idle_V3_synth" nel caso di condizione di quasi *idle*, di larghezza di banda pari a 10 MHz. Il segnale è stato centrato alle frequenze di 763 MHz, 773 MHz e 783 MHz.

In Figura 5 vengono mostrati due esempi di spettro del segnale LTE in trasmissione downlink indicativi dei casi di traffico 100% e quasi idle utilizzando le sintesi su menzionate.

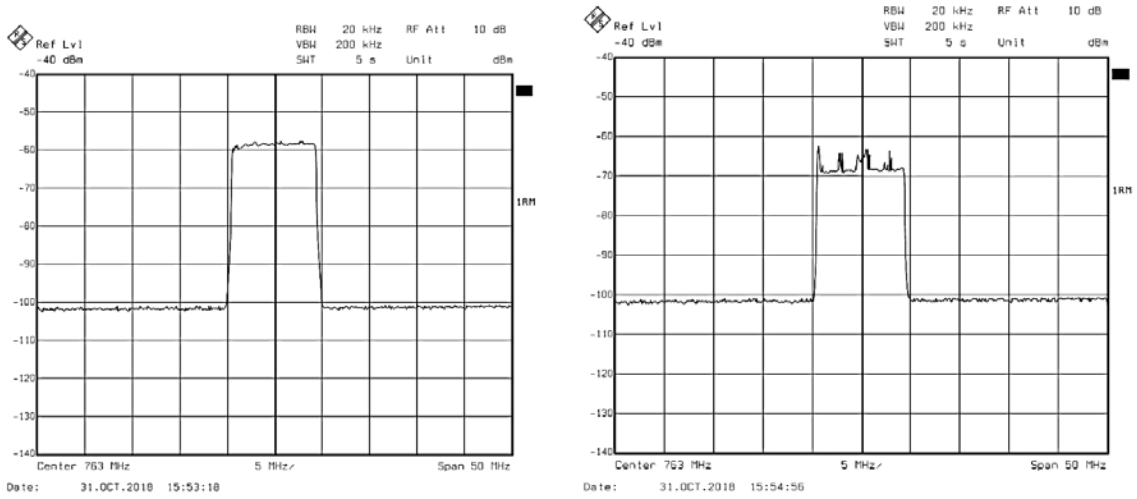

Figura 5 - *Spettro dei segnali LTE downlink rispettivamente traffico 100% e near Idle (ETSI EN 303 340)*

Il segnale voluto, quello di broadcasting televisivo, viene prodotto in tecnica DVB-T2 in banda UHF canalizzata a 8 MHz, tenendo in considerazione principalmente la configurazione prevista dalla norma tecnica armonizzata [8] per la verifica della conformità al requisito essenziale 3.2 della direttiva europea 2014/53/EU (RE-D) dei ricevitori del digitale terrestre televisivo. In Tabella 1 sono riportati i parametri di maggior interesse e di più immediata interpretazione:

Tabella 1. Impostazione principali parametri DVB-T2

PARAMETRI	VALORI
Larghezza di banda	7,61 MHz; 7,77 MHz
FFT	8k; 32k_ext
Modulazione	64 QAM e 256 QAM con rotazione
Code Rate	2/3; 3/4
Guard Interval	1/16

Il livello del segnale DVB-T2 all'ingresso del ricevitore è stato impostato alternativamente a -63 dBm e a -70 dBm, ritenendo quest'ultima con buona approssimazione la potenza minima che si debba manifestare alla presa d'utente di un televisore digitale [9] per poter visualizzare correttamente sul video quanto ricevuto. I canali vittima dell'interferenza, di larghezza 8 MHz, sono centrati alle frequenze che vanno da 618 MHz (ch. 39) a 690 MHz (ch. 48).

In Figura 6 viene illustrato un esempio di immagine spettrale e di costellazione per una modulazione 256 QAM ruotata di un segnale DVB-T2 di 8 MHz di banda.

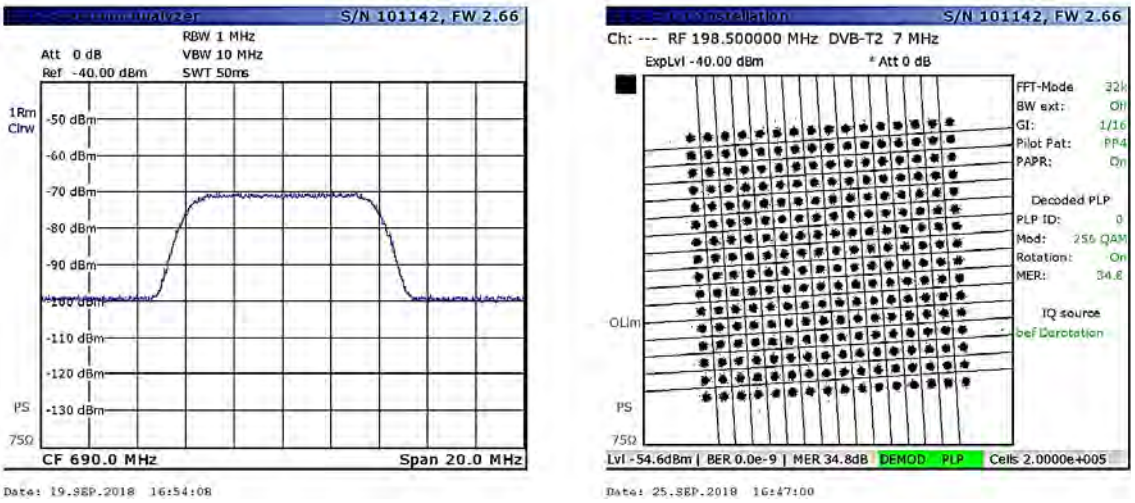

Figura 6 - *Spettro e Costellazione segnale DVB-T2, modulazione 256 QAM ruotata*

Successivamente sono state effettuate alcune misurazioni anche in presenza di un terminale di testa che solitamente è presente a valle di un'antenna di tipo condominiale ricevente il segnale televisivo. È stato impostato all'ingresso del terminale un segnale utile del livello di circa -75 dBm, ritenuto come caso emblematico di valore minimo previsto [9], e del livello di -55 dBm. Per lo scopo è stata utilizzata una variante del banco di simulazione come indicato in Figura 7. La variante ha previsto tra l'altro l'inserimento di un attenuatore variabile al fine di produrre all'ingresso RF del televisore un livello costante di -50 dBm.

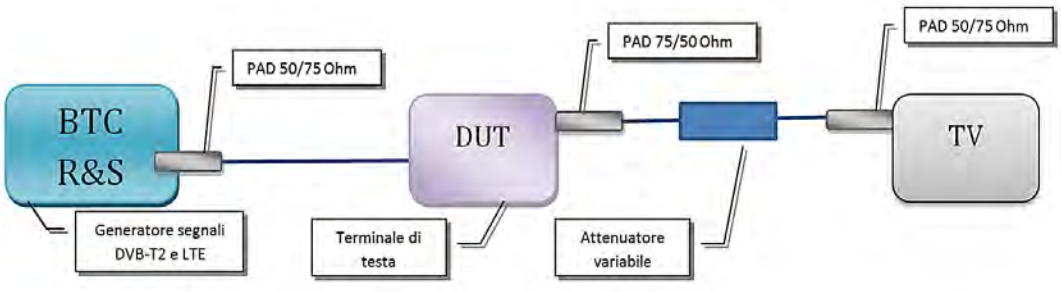

Figura 7 - *Banco di simulazione modificato in presenza di un terminale di testa*

Il terminale di testa utilizzato come device sotto prova è stato impostato con il massimo guadagno di circa 37 dB e con quello minimo di circa 17 dB e risulta avere una risposta in

frequenza pressoché piatta nella banda di interesse con una variazione massima di circa 2 dB, come mostrato in Figura 8.

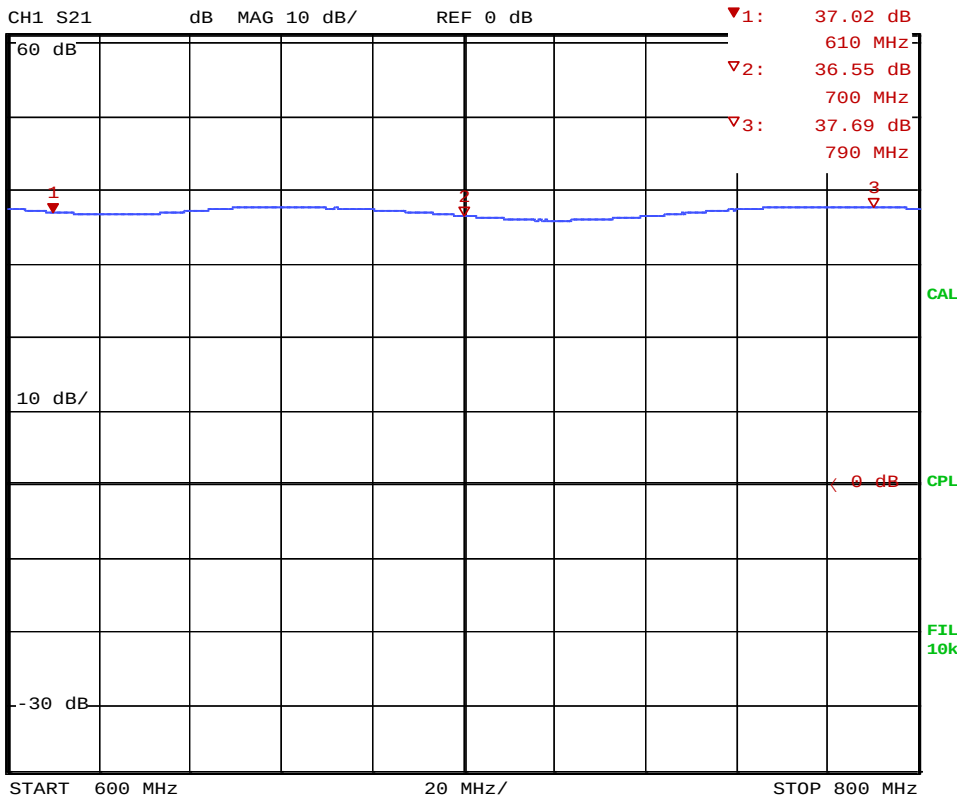

Figura 8 - *Risposta in frequenza (in banda UHF) di un tipico terminale di testa impostato a guadagno massimo*

3. Risultati delle prove di laboratorio

Le prove effettuate hanno prodotto una serie di dati che sono stati rappresentati graficamente principalmente in termini di rapporto di protezione espresso in decibel, ossia rapporto tra segnale interferente (LTE in uplink e/o downlink in banda 700 MHz) e segnale utile (DVB-T2 in banda adiacente, a partire dal canale centrato alla frequenza di 690 MHz) individuato al momento della degradazione dell'immagine rilevata secondo il criterio precedentemente descritto. I grafici sintetizzano misure effettuate simulando semplici impianti TV, senza e con terminale di testa, rilevando i dati necessari, livello del segnale DVB-T2 definito con la lettera "C" e livello del segnale interferente definito con la lettera "I", all'ingresso RF del ricevitore televisivo. I primi sei grafici mostrano l'andamento del rapporto I/C all'ingresso di due ricevitori TV (senza terminale di testa) immaginando di avere un livello di segnale utile pari a -63 dBm per i primi tre e di -70 dBm per il secondo gruppo. Le misure sono state effettuate utilizzando un segnale DVB-T2 caratterizzato da un code rate di 2/3, un guard interval di 1/16

ed una modulazione 256 QAM ruotata. Il segnale interferente è LTE in Uplink come indicato in precedenza.

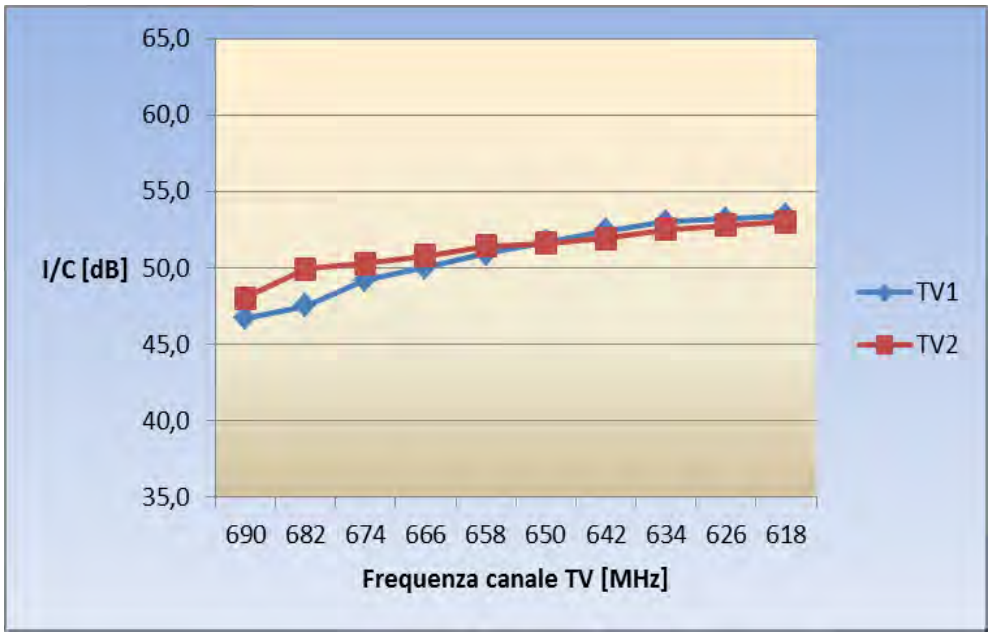

Figura 9 - *(cfr. TV1-TV2), I/C con LTE UL centrato a 708 MHz (10 MHz), DVB-T2 a -63 dBm*

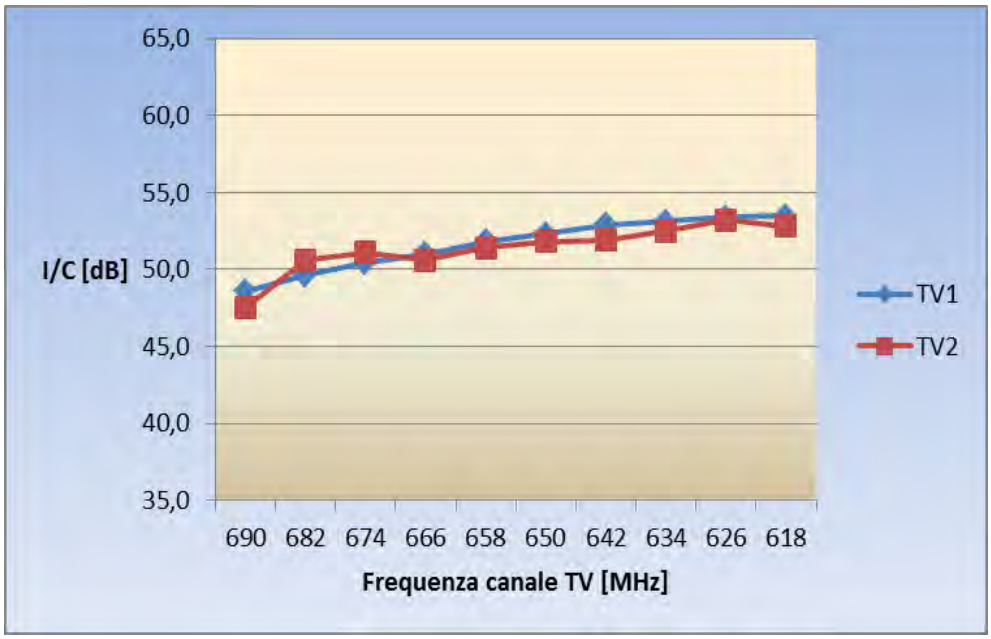

Figura 10 - *(cfr. TV1-TV2), I/C con LTE UL centrato a 718 MHz (10 MHz), DVB-T2 a -63 dBm*

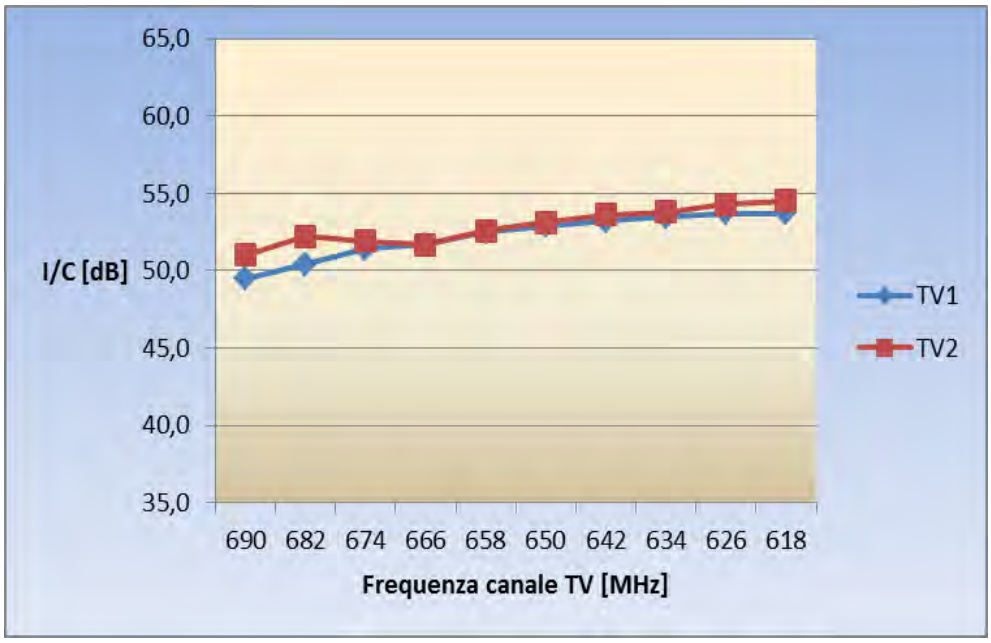

Figura 11 - *(cfr. TV1-TV2), I/C con LTE UL centrato a 728 MHz (10 MHz), DVB-T2 a -63 dBm*

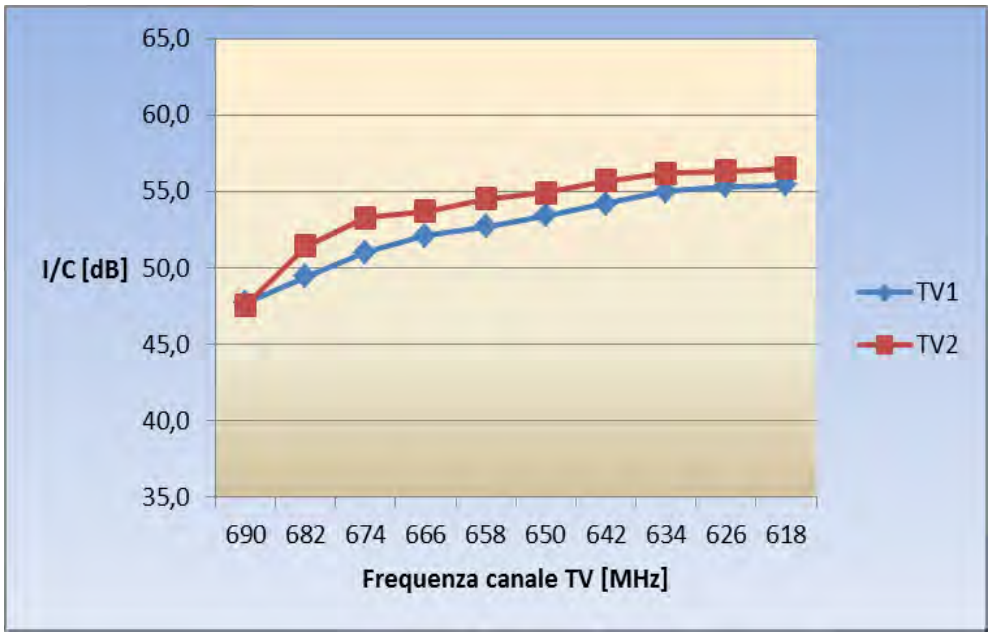

Figura 12 - *(cfr. TV1-TV2), I/C con LTE UL centrato a 708 MHz (10 MHz), DVB-T2 a -70 dBm*

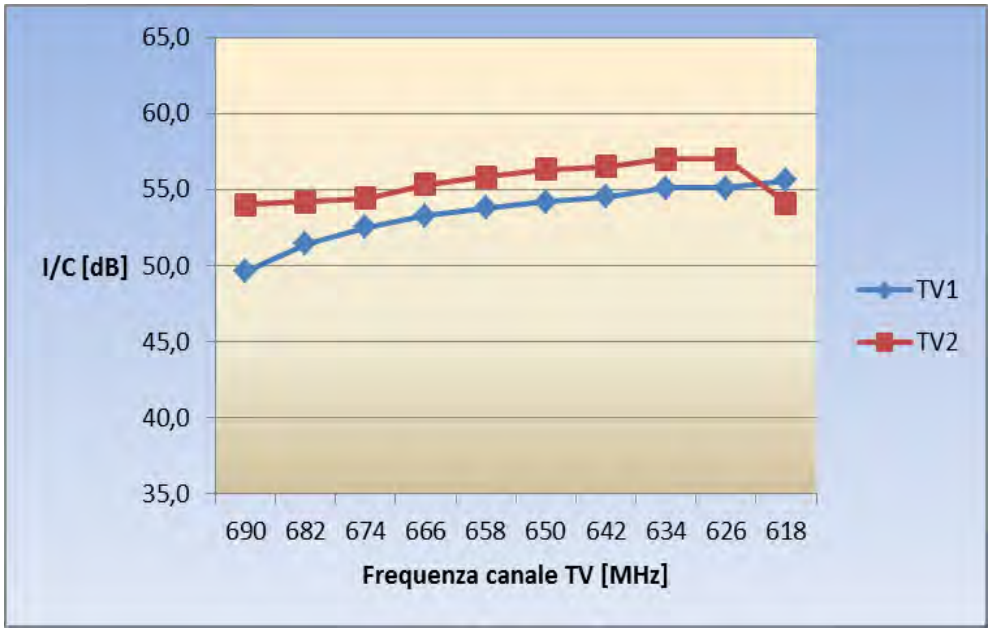

Figura 13 - *(cfr. TV1-TV2), I/C con LTE UL centrato a 718 MHz (10 MHz), DVB-T2 a -70 dBm*

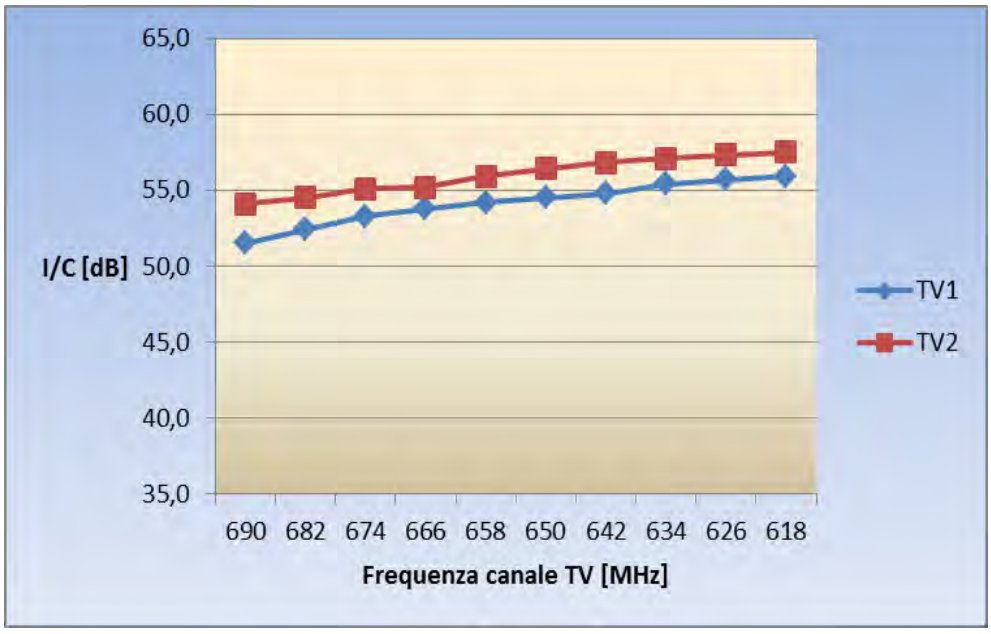

Figura 14 - *(cfr. TV1-TV2), I/C con LTE UL centrato a 728 MHz (10 MHz), DVB-T2 a -70 dBm*

I seguenti sei grafici mettono a confronto i rapporti di protezione (I/C) ricavati variando il code rate (2/3 e 3/4) e la modulazione (256 QAM e 64 QAM) del segnale utile in tecnica DVB-T2. La misura viene sempre effettuata in assenza di terminale di testa ed all'ingresso RF di un

ricevitore TV. Il segnale interferente è ancora di tipo LTE in Uplink con le caratteristiche precedentemente descritte.

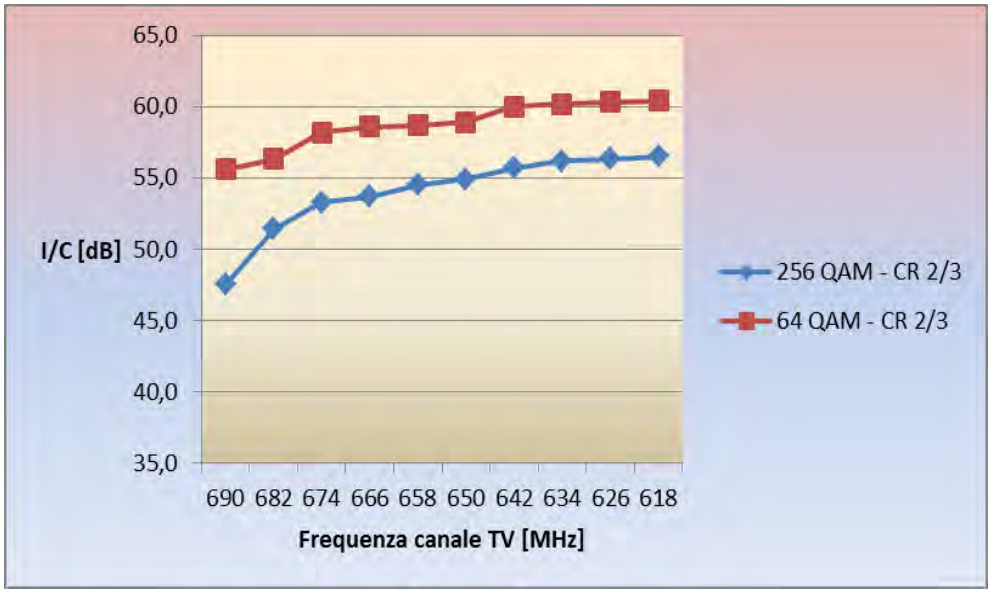

Figura 15 - *(cfr. modulazione), I/C con LTE UL centrato a 708 MHz (10 MHz), DVB-T2 a -70 dBm*

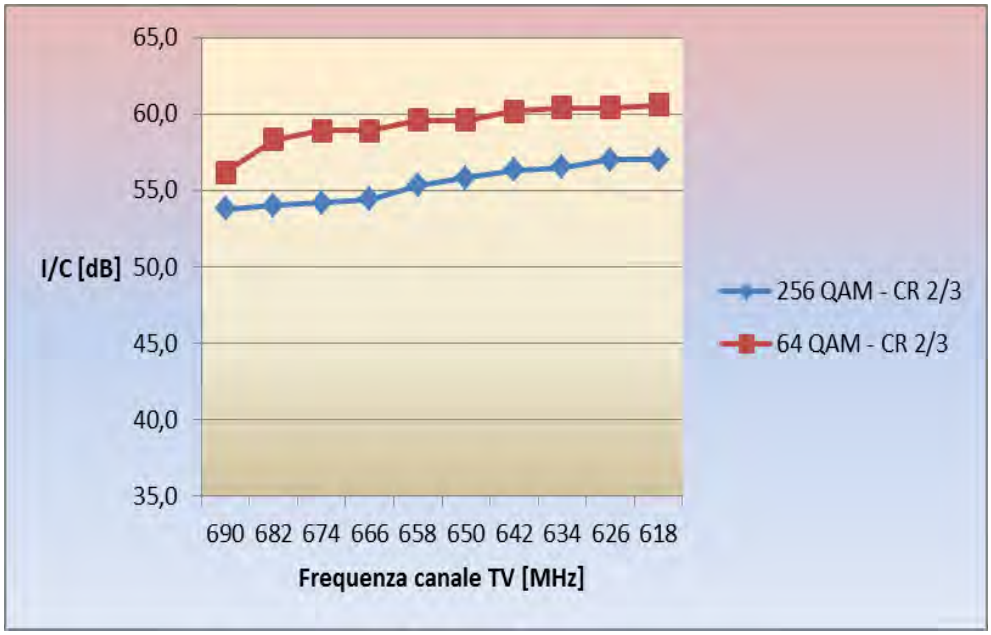

Figura 16 - *(cfr. modulazione), I/C con LTE UL centrato a 718 MHz (10 MHz), DVB-T2 a -70 dBm*

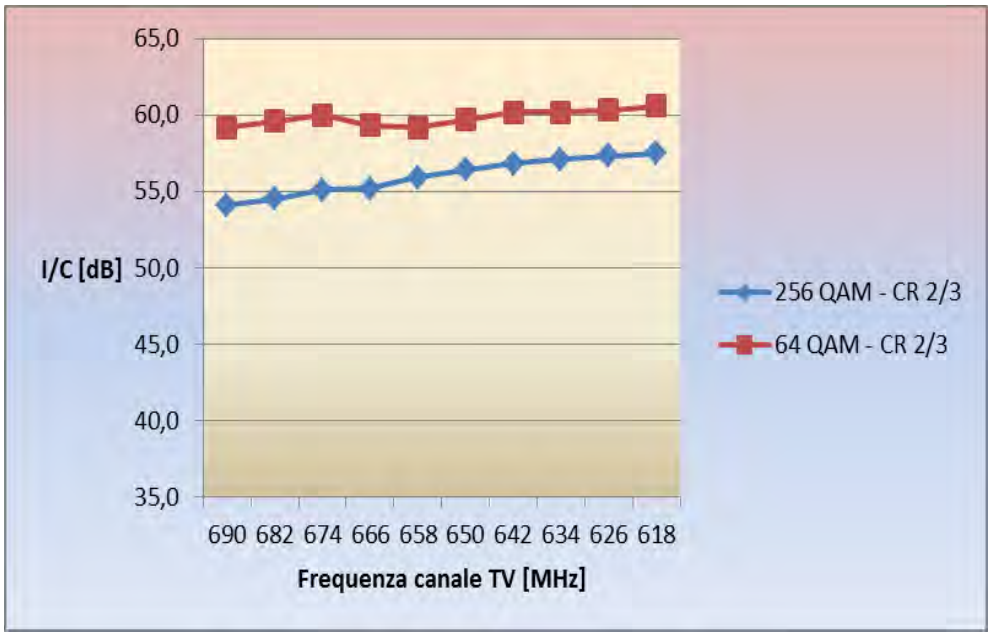

Figura 17 - *(cfr. modulazione), I/C con LTE UL centrato a 728 MHz (10 MHz), DVB-T2 a -70 dBm*

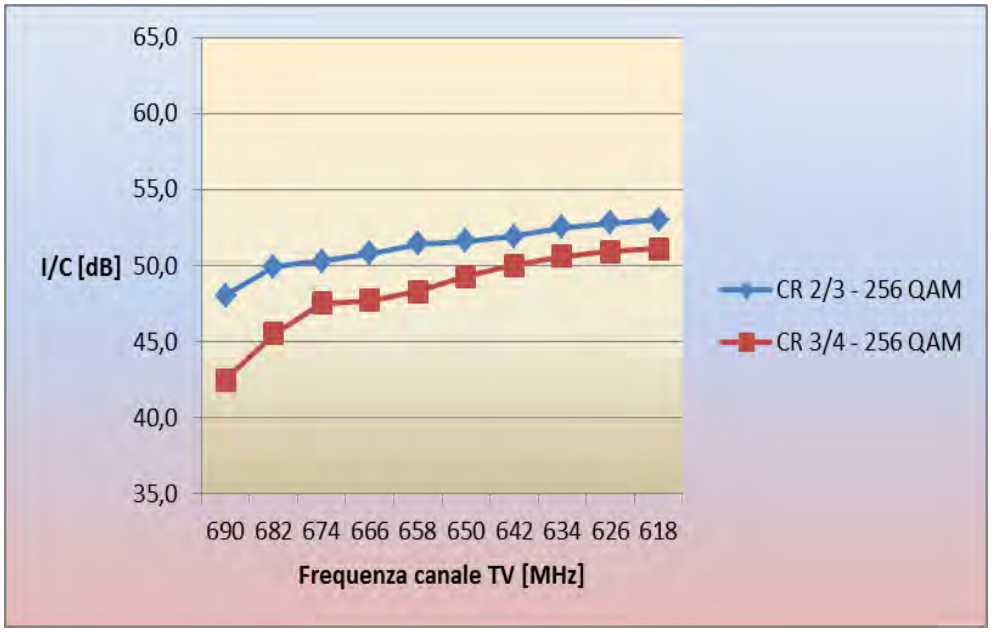

Figura 18 - *(cfr. Code rate), I/C con LTE UL centrato a 708 MHz (10 MHz), DVB-T2 a -63 dBm*

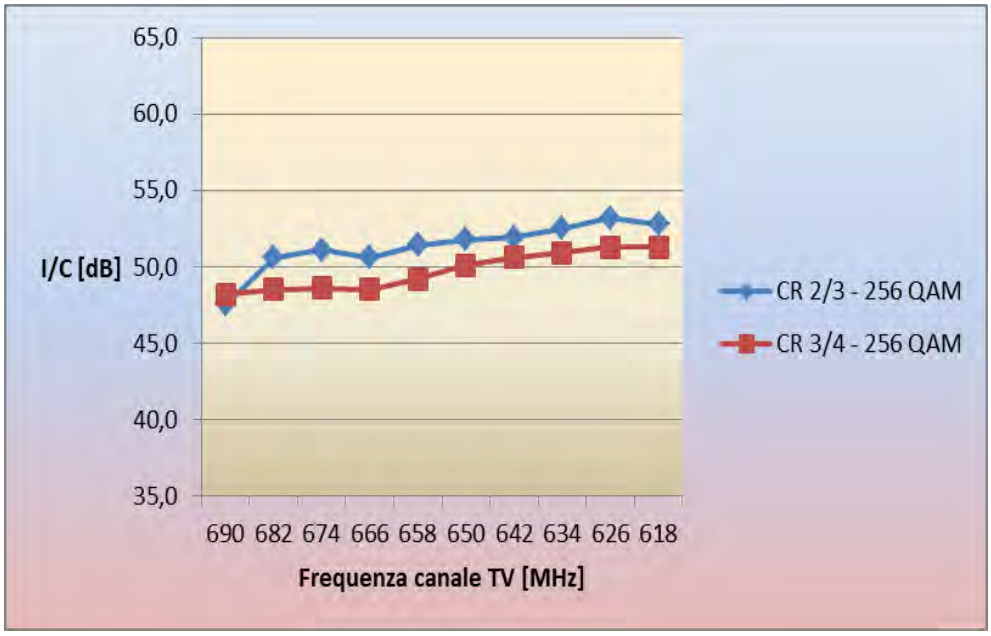

Figura 19 - *(cfr. Code rate), I/C con LTE UL centrato a 718 MHz (10 MHz), DVB-T2 a -63 dBm*

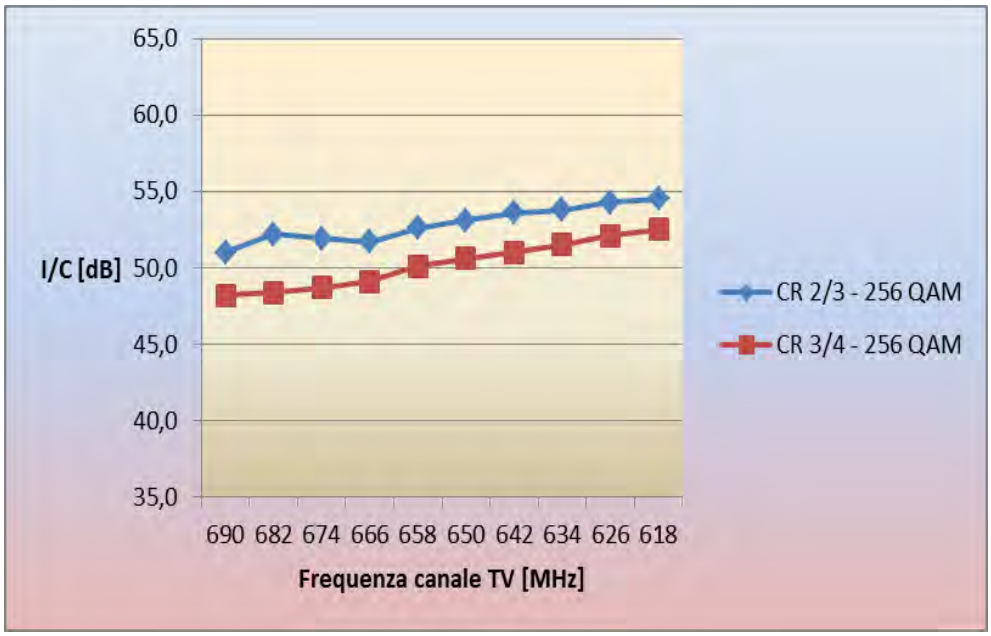

Figura 20 - *(cfr. Code rate), I/C con LTE UL centrato a 728 MHz (10 MHz), DVB-T2 a -63 dBm*

Il seguente grafico mette a confronto i rapporti di protezione in presenza di segnali indesiderati di radiomobile LTE in *downlink* o in *uplink*, presenti singolarmente e posizionati nelle

frequenze ad essi attribuite. La misurazione è avvenuta in assenza di terminale di testa e con un livello di DVB-T2 di -70 dBm.

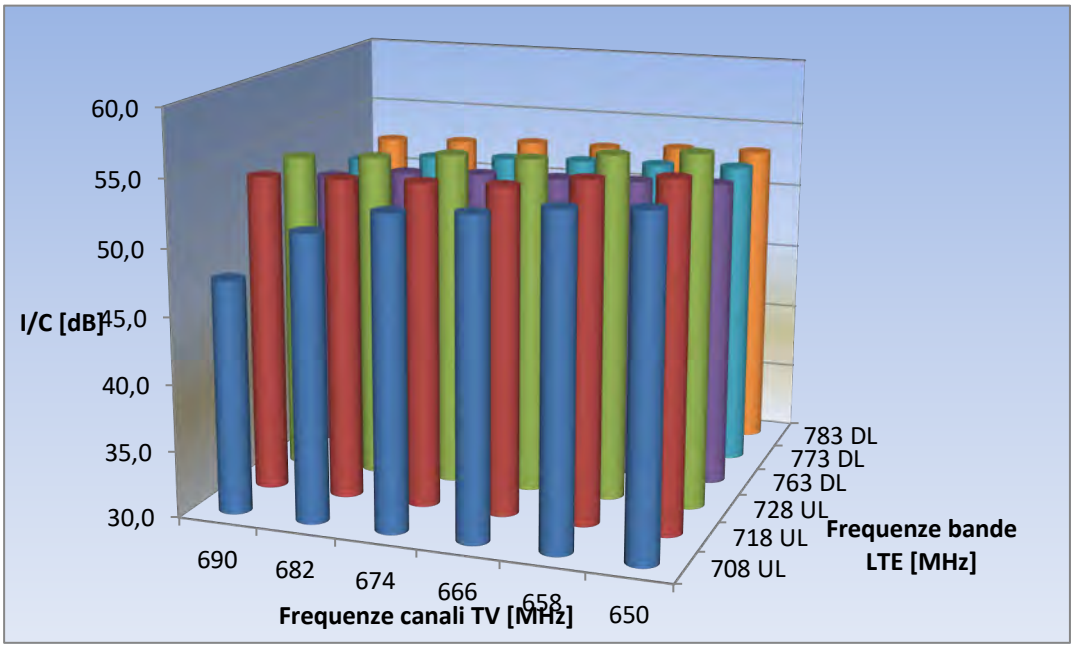

Figura 21 - *cfr. andamento rapporto di protezione I/C con LTE in DL o in UL*

I seguenti tracciati mettono a confronto la degradazione provocata dalla singola presenza dei segnali LTE Uplink a 10 MHz centrati nelle frequenze di 708 MHz, 718 MHz e 728 MHz e la degradazione provocata dalla copresenza dei tre segnali 3x10 MHz, quest'ultimi a pari livello di potenza. La rappresentazione grafica avviene attraverso il rapporto I/C misurato all'ingresso del terminale di testa di un impianto TV impostato a guadagno massimo (≃ 37 dB) e con un livello di segnale utile (DVB-T2, Code Rate 2/3, Guard Interval 1/16, Modulazione 256 QAM ruotata) pari sia a -75 dBm che a -55 dBm. Attraverso la parte terminale del banco, composta da un attenuatore variabile e due matching pad 50/75 ohm, è stato fissato a -50 dBm il segnale utile all'ingresso RF del televisore.

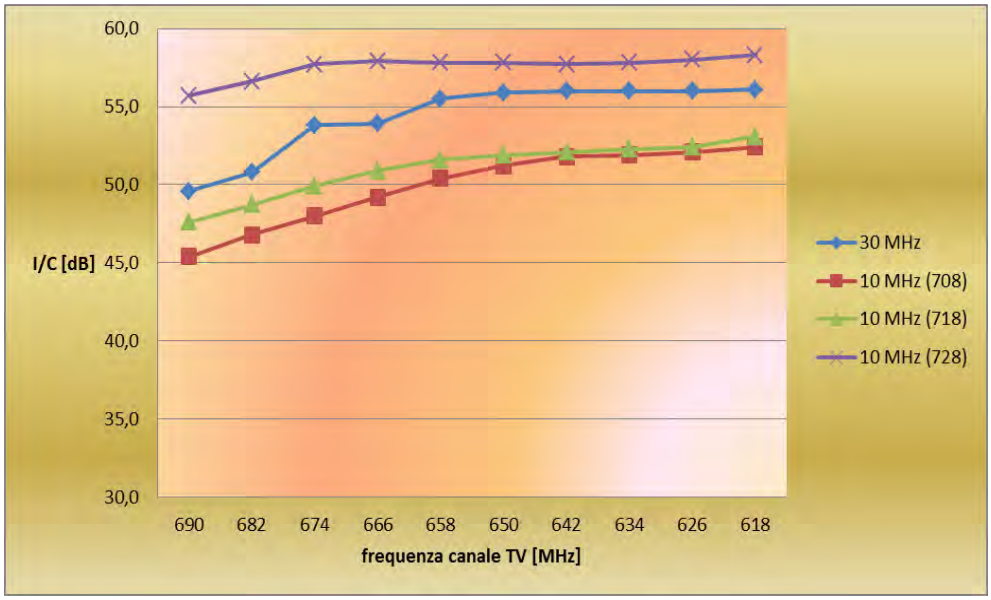

Figura 22 - *(cfr LTE Uplink 10 MHz, 30 MHz) Andamento I/C, DVB-T2 -75 dBm*

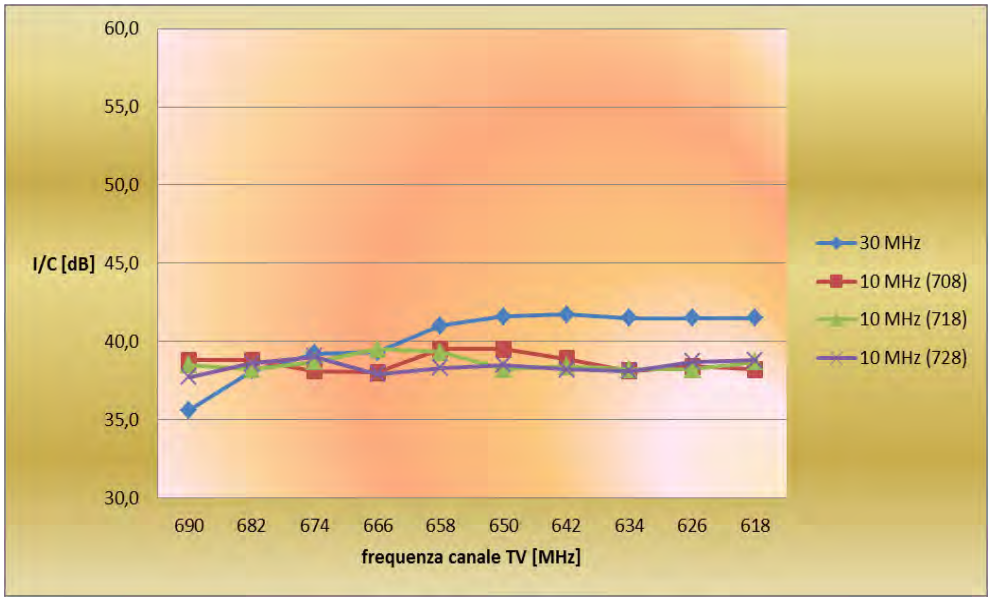

Figura 23 - *(cfr LTE Uplink 10 MHz, 30 MHz) Andamento I/C, DVB-T2 -55 dBm*

I prossimi quattro grafici mostrano l'andamento del rapporto di protezione misurato all'ingresso di un amplificatore di testa impostato con guadagno massimo, in presenza di segnale

indesiderato in configurazione di LTE Downlink (con traffico al 100% e in Idle) centrato alle frequenze di 763 MHz, 773 MHz e 783 MHz e larghezza di banda di 10 MHz. I primi due grafici si riferiscono a misure con livello di potenza del segnale utile di -75 dBm, i due successivi con livello di -55 dBm.

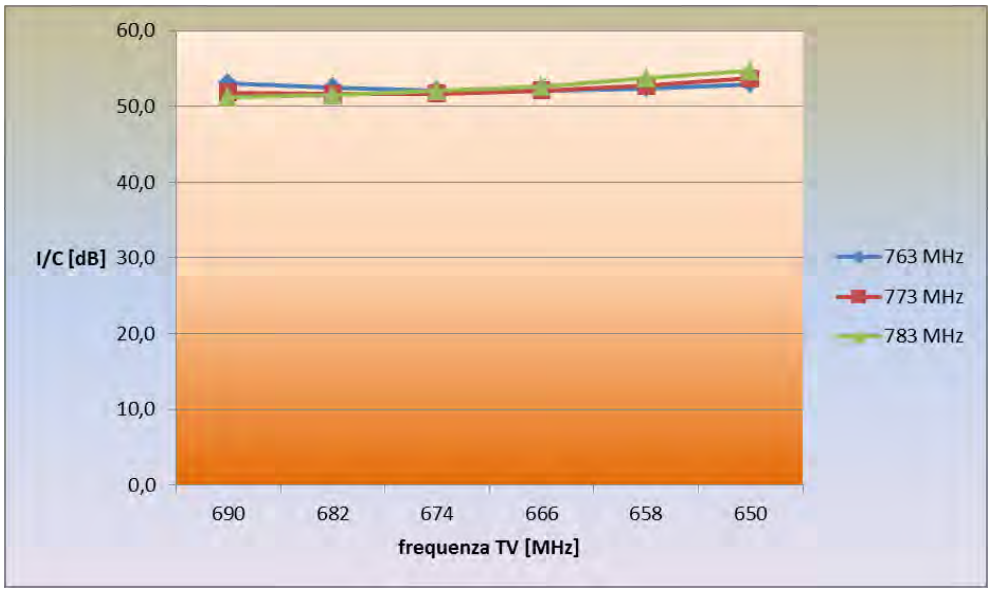

Figura 24 - *I/C con LTE DL "100%", DVB-T2 a -75 dBm*

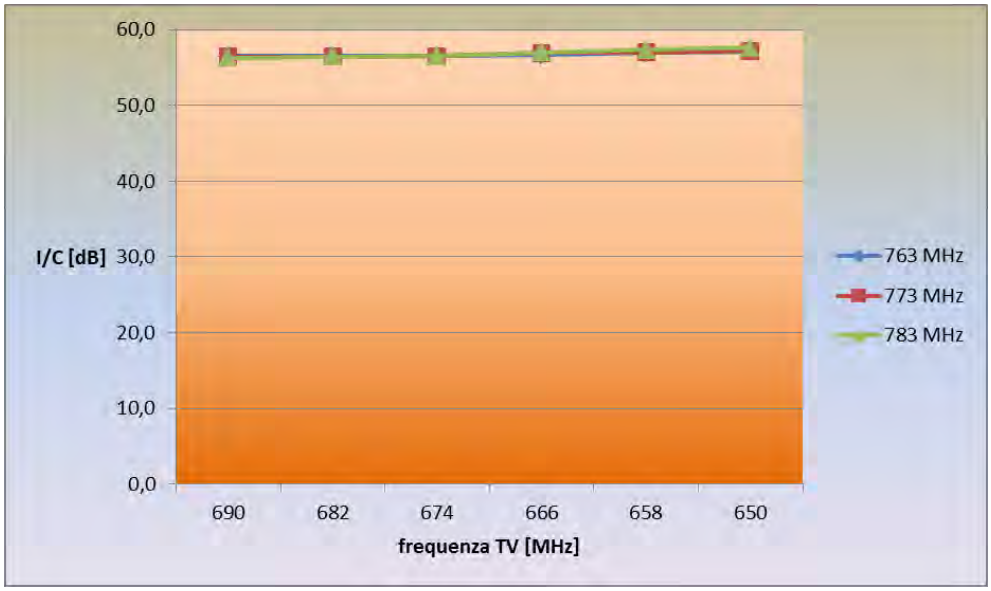

Figura 25 - *I/C con LTE DL "near IDLE", DVB-T2 a -75 dBm*

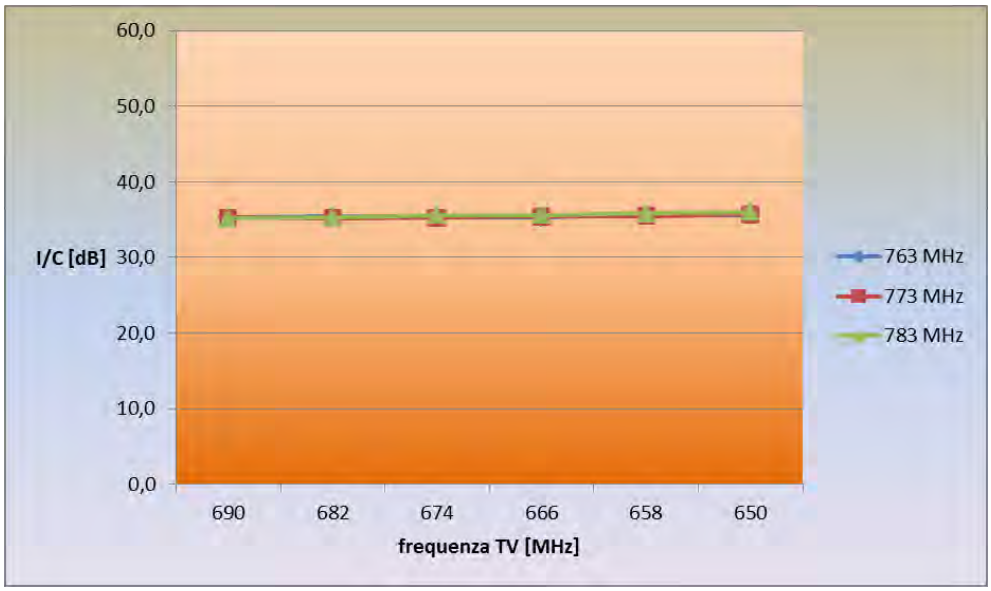

Figura 26 - *I/C con LTE DL "100%", DVB-T2 a -55 dBm*

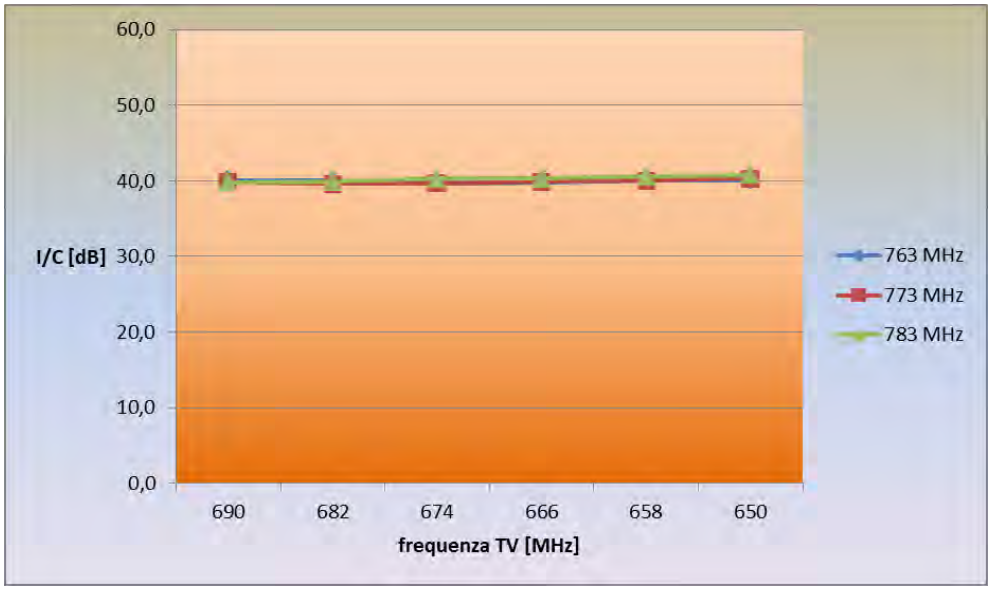

Figura 27 - *I/C con LTE DL "near IDLE", DVB-T2 a -55 dBm*

Gli ultimi due grafici sintetizzano l'andamento del livello di potenza del segnale LTE in configurazione di downlink e traffico al 100%, centrato a 763 MHz, in funzione del livello di potenza del segnale LTE in uplink, centrato alla frequenza di 708 MHz, entrambi a larghezza

di banda di 10 MHz e misurati all'ingresso del terminale di testa al momento del verificarsi della degradazione dell'immagine sul display televisivo. Il livello del segnale DVB-T2 (trasmesso sul canale 48, frequenza centrale 690 MHz) è fissato a -55 dBm all'ingresso del terminale di testa ed i due grafici si riferiscono rispettivamente ad impostazione di guadagno minimo (≃ 17 dB) e di guadagno massimo (≃ 37 dB) del terminale di testa medesimo.

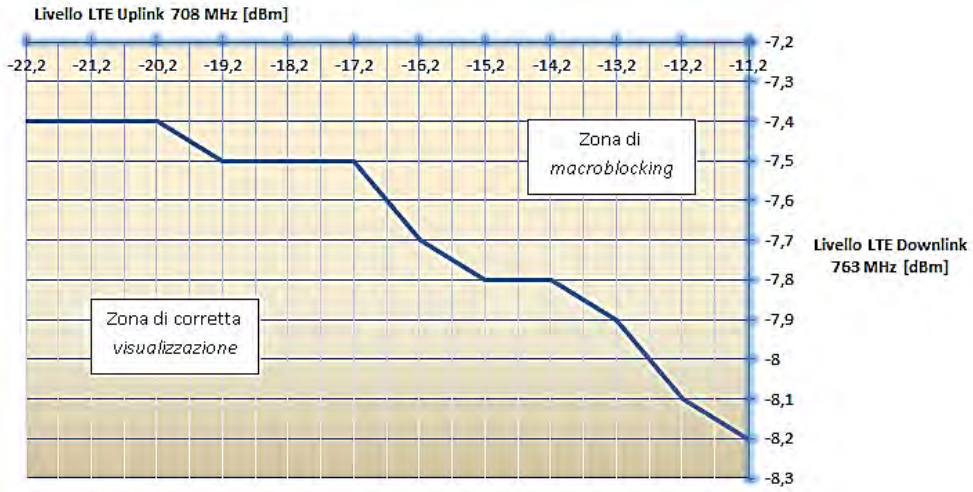

Figura 28 - *Andamento alla soglia di degradazione con guadagno minimo del terminale di testa*

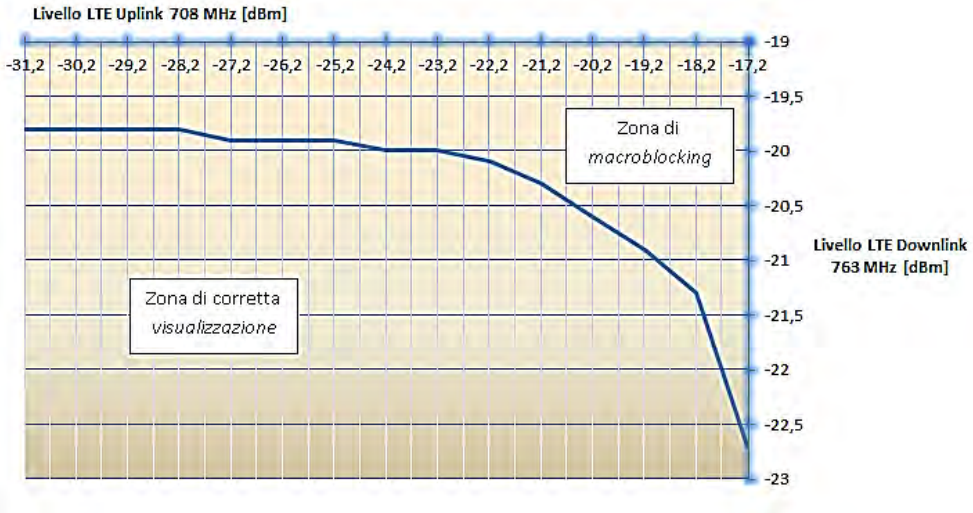

Figura 29 - *Andamento alla soglia di degradazione con guadagno massimo del terminale di testa*

Immaginando uno scenario interferenziale come illustrato in Figura 30, assumendo quindi assenza di ostacoli tra lato trasmissione e lato ricezione, mantenendo valida la condizione di trasmissione in spazio libero ed ipotizzando una perdita per cross polarizzazione tra antenna TV e antenne uplink e downlink LTE rispettivamente di 14 dB massima (0 dB nel caso di perdita minima) e di 3 dB, grazie ai dati raccolti, è possibile calcolare approssimativamente la coppia di valori distanza minima da antenna TV - potenza massima EIRP, che deve essere rispettata da una stazione radio base e/o un terminale d'utente LTE (smartphone) affinché non si producano macroblocking sul monitor televisivo.

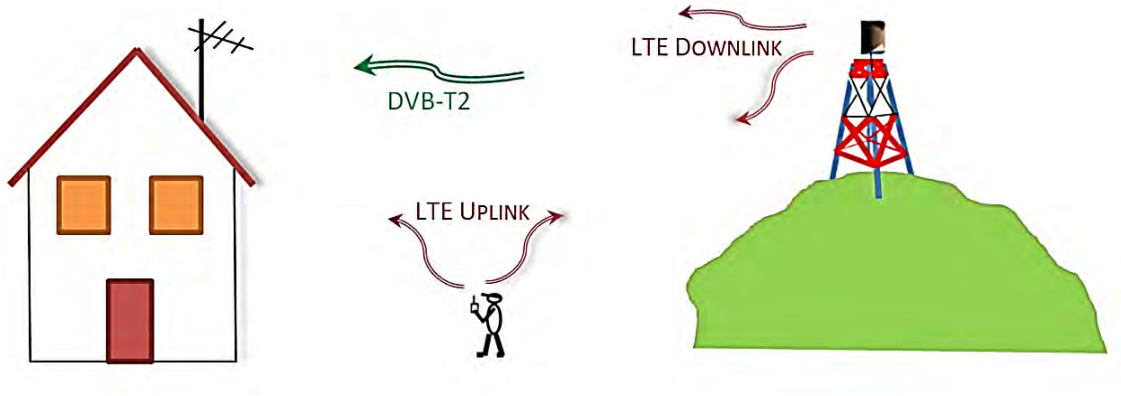

Figura 30 - *Scenario: interferenze LTE Downlink e Uplink su antenna TV*

Si definiscono quindi i seguenti parametri necessari per identificare la relazione che permetta il calcolo su indicato:

- EIRP [dBm]: Potenza equivalente irradiata isotropicamente dalle antenne LTE nella direzione verso l'antenna TV;
- d [m]: Distanza tra antenna trasmittente LTE e antenna ricevente TV;
- f [MHz]: Frequenza di lavoro LTE;
- I [dBm]: Livello del segnale interferente LTE all'ingresso del dispositivo sotto test per un I/C in corrispondenza di macroblocking sul ricevitore;
- Gr [dBi]: Guadagno antenna ricevente in relazione all'antenna isotropa alla frequenza f e nella direzione verso l'antenna LTE;
- Ap [dB]: Perdita per disadattamento di polarizzazione;
- Ac [dB]: Attenuazione del cavo dell'impianto TV.

La relazione che ne deriva a seguito delle ipotesi e dei parametri considerati è la seguente:

EIRP[dBm] – 20log(d[m]) = I[dBm] + 20log(f [MHz]) + Ap[dB] + Ac[dB] + Gr[dBi] – 27,6

Scenario 1 (segnale televisivo scarso e assenza di amplificatore TV)

1.a) Smartphone LTE che trasmette videostreaming alla frequenza di 708 MHz, in prossimità di abitazione con impianto TV, non dotato di terminale di testa, sintonizzato sul canale 48 (690 MHz) e ricevente un segnale DVB-T2 (256 QAM, Code rate 2/3, Guard interval 1/16), e antenna TV con guadagno 9 dBi e attenuazione cavo tv di 3 dB.

Degradazione all'ingresso del TV: I/C = 47,3 dB; (Figura 12)

C = -70 dBm; I = -22,7 dBm

- per Ap= 0 dB

LTE Uplink EIRP [dBm]	d [m]
23	1.6
21	1,3
19	1
17	0,8

- per Ap= 14 dB

LTE Uplink EIRP [dBm]	d [m]
23	0,3
21	0,3
19	0,2
17	0,2

1.b) Stazione Radio Base LTE che trasmette a pieno carico (traffico 100%) alla frequenza di 763 MHz, in prossimità di abitazione con impianto TV, non dotato di terminale di testa, sintonizzato sul canale 48 (690 MHz) e ricevente un segnale DVB-T2 (Code rate 2/3, Guard interval 1/16), e antenna TV con guadagno 9 dBi e attenuazione cavo tv di 3 dB.

Degradazione all'ingresso del TV: I/C = 51,5 dB; (Figura 21)

C = -70 dBm; I = -18,5 dBm

- per Ap= 3 dB

LTE Downlink EIRP [dBm]	d [m]
60	47
57	33
54	24
51	17

Scenario 2 (segnale televisivo di livello basso e presenza di amplificatore TV con guadagno massimo)

2.a) Smartphone LTE che trasmette videostreaming alla frequenza di 708 MHz, in prossimità di abitazione con impianto TV, dotato di terminale di testa, sintonizzato sul canale 48 (690 MHz) e ricevente un segnale DVB-T2 (256 QAM, Code rate 2/3, Guard interval 1/16), e antenna TV con guadagno 9 dBi e attenuazione cavo tv di 3 dB.

Degradazione all'ingresso del terminale di testa: I/C = 45,4 dB; (Figura 22)

C = -75 dBm; I = -29,6 dBm

- per Ap= 0 dB

LTE Uplink EIRP [dBm]	d [m]
23	3,6
21	2,9
19	2,3
17	1,8

- per Ap= 14 dB

LTE Uplink EIRP [dBm]	d [m]
23	0,7
21	0,6
19	0,5
17	0,4

2.b) Stazione Radio Base LTE che trasmette a pieno carico (traffico 100%) alla frequenza di 763 MHz, in prossimità di abitazione con impianto TV, dotato di terminale di testa, sintonizzato

sul canale 48 (690 MHz) e ricevente un segnale DVB-T2 (Code rate 2/3, Guard interval 1/16), e antenna TV con guadagno 9 dBi e attenuazione cavo tv di 3 dB.

Degradazione all'ingresso del terminale di testa: I/C = 53,1 dB; (Figura 24)

C = -75 dBm; I = -21,9 dBm

- per Ap= 3 dB

LTE Downlink EIRP [dBm]	d [m]
60	70
57	49
54	35
51	25

Scenario 3 (segnale televisivo di livello medio e presenza di amplificatore TV con guadagno massimo)

3.a) Smartphone LTE che trasmette videostreaming alla frequenza di 708 MHz, in prossimità di abitazione con impianto TV, dotato di terminale di testa, sintonizzato sul canale 48 (690 MHz) e ricevente un segnale DVB-T2 (256 QAM, Code rate 2/3, Guard interval 1/16), e antenna TV con guadagno 9 dBi e attenuazione cavo tv di 3 dB.

Degradazione all'ingresso del terminale di testa: I/C = 38,8 dB; (Figura 23)

C = -55 dBm; I = -16,2 dBm

- per Ap= 0 dB

LTE Uplink EIRP [dBm]	d [m]
23	0,8
21	0,6
19	0,5
17	0,4

- per Ap= 14 dB

LTE Uplink EIRP [dBm]	d [m]
23	0,2
21	0,1
19	0,1
17	0,1

3.b) Stazione Radio Base LTE che trasmette a pieno carico (traffico 100%) alla frequenza di 763 MHz, in prossimità di abitazione con impianto TV, dotato di terminale di testa, sintonizzato sul canale 48 (690 MHz) e ricevente un segnale DVB-T2 (Code rate 2/3, Guard interval 1/16), e antenna TV con guadagno 9 dBi e attenuazione cavo tv di 3 dB.

Degradazione all'ingresso del terminale di testa: I/C = 35,3 dB; (Figura 26)

C = -55 dBm; I = -19,7 dBm

- per Ap= 3 dB

LTE Downlink EIRP [dBm]	d [m]
60	54
57	38
54	27
51	19

3.c) Smartphone LTE che trasmette videostreaming alla frequenza di 708 MHz e, contemporaneamente, Stazione Radio Base LTE che trasmette a pieno carico (traffico 100%) alla frequenza di 763 MHz, in prossimità di abitazione con impianto TV, dotato di terminale di testa, sintonizzato sul canale 48 (690 MHz) e ricevente un segnale DVB-T2 (Code rate 2/3, Guard interval 1/16), e antenna TV con guadagno 9 dBi e attenuazione cavo tv di 3 dB.

Degradazione all'ingresso del terminale di testa (Figura 29) – un esempio

C = -55 dBm; IUL = -29,2 dBm; IDL = -19,8 dBm

- per Ap= 0 dB

LTE Uplink EIRP [dBm]	d [m]
23	3,5
21	2,8
19	2,2
17	1,7

- per Ap= 14 dB

LTE Uplink EIRP [dBm]	d [m]
23	0,7
21	0,5
19	0,4
17	0,3

- per Ap= 3 dB

LTE Downlink EIRP [dBm]	d [m]
60	55
57	39
54	27
51	19

4. Conclusioni

In questo documento sono state riportate le misurazioni eseguite, in modalità condotta, su un banco di sperimentazione presso il laboratorio Radiodiffusione sonora e televisiva dell'Istituto Superiore C.T.I. del Ministero dello sviluppo economico. Le prove sono state effettuate al fine di indagare sulla coesistenza tra i segnali del servizio radiomobile LTE trasmessi in banda 700 MHz in uplink (nell'intervallo di frequenze che va da 703 MHz a 733 MHz) e/o in downlink (nell'intervallo di frequenze che va da 758 MHz a 788 MHz) ed i segnali in tecnica DVB-T2 in banda 600 MHz (fino al canale 48, frequenza centrale 690 MHz, ultimo canale disponibile in Italia dal 1° luglio 2022 per le trasmissioni televisive del digitale terrestre). Per sondare l'interferenza provocata sui ricevitori tv sono stati utilizzati come segnali indesiderati le forme d'onda rappresentative del servizio LTE indicate dalla norma armonizzata ETSI EN 303 340 V1.1.2 (2016/09). I dati dei test di laboratorio sono stati analizzati per valutare le

eventuali situazioni interferenziali scaturite dai suindicati segnali radiomobile all'ingresso di un tipico impianto di ricezione televisiva presente attualmente in Italia, con e senza terminale di testa. I risultati dei test hanno mostrato un andamento interferenziale essenzialmente atteso:

- L'effetto interferenziale LTE, qualora il segnale televisivo sia di livello di potenza minimo, è presente tanto per le trasmissioni in Uplink quanto per le trasmissioni in Downlink, seppur di valore piuttosto trascurabile.
- Tale effetto generalmente decresce con l'incremento della separazione in frequenza tra il segnale utile DVB-T2 e quello indesiderato LTE.
- Le distanze e le potenze dei trasmettitori LTE (smartphone e stazioni radio base) tali che non si procuri degradazione sul display televisivo sono agevolmente rispettabili.
- Una modulazione più robusta del segnale utile mostra una migliore resistenza alla presenza di segnali interferenziali LTE.
- L'aumento di symbol rate a parità di modulazione del segnale utile mostra una maggiore sensibilità alla presenza di interferenza LTE in particolar modo per il canale televisivo più vicino ai segnali indesiderati.

Gli autori ringraziano il Dirigente, Ing. Giuseppe Pierri e i sigg. Roberto Dal Molin e Maurizio Fasciolo della Divisione IV della DGTCSI - ISCTI per la disponibilità alla realizzazione della sperimentazione.

Riferimenti bibliografici

[1] DECISIONE N. 243/2012/UE DEL PARLAMENTO EUROPEO E DEL CONSIGLIO del 14 marzo 2012 che istituisce un programma pluriennale relativo alla politica in materia di spettro radio

[2] COMUNICAZIONE DELLA COMMISSIONE AL PARLAMENTO EUROPEO, AL CONSIGLIO, AL COMITATO ECONOMICO E SOCIALE EUROPEO E AL COMITATO DELLE REGIONI - Strategia per il mercato unico digitale in Europa (6 maggio 2015)

[3] ECC Decision (15)01 "Harmonised technical conditions for mobile/fixed communications networks (MFCN) in the band 694-790 MHz including a paired frequency arrangement (Frequency Division Duplex 2x30 MHz) and an optional unpaired frequency arrangement (Supplemental Downlink)", CEPT, 6 marzo 2015

[4] DECISIONE (UE) 2017/899 DEL PARLAMENTO EUROPEO E DEL CONSIGLIO del 17 maggio 2017 relativa all'uso della banda di frequenza 470-790 MHz nell'Unione

[5] Legge 27 dicembre 2017, n. 205 - Bilancio di previsione dello Stato per l'anno finanziario 2018 e bilancio pluriennale per il triennio 2018-2020

[6] E. Restuccia, G. Fusco, M. Ferrante, "Laboratory simulation on the coexistence of TV broadcasting service with broadband wireless access LTE in the 800 MHz band", La Comunicazione Magazine, 2014

[7] Decreto Ministero dello sviluppo economico 8 agosto 2018 relativo alla road map per la liberazione della banda 700 MHz

[8] ETSI EN 303 340 V1.1.2, "Digital Terrestrial TV Broadcast Receivers; Harmonised Standard covering the essential requirements of article 3.2 of Directive 2014/53/EU", Settembre 2016

[9] GUIDA CEI 100-7, "Guida per l'applicazione delle Norme sugli impianti per segnali televisivi, sonori e servizi interattivi", 2016, edizione quinta

[10] Decreto Ministero dello Sviluppo Economico del 19 giugno 2019 recante "Nuovo calendario nazionale rilascio banda 700 MHz"