



Ministero delle Imprese  
e del Made in Italy

Dipartimento per il Digitale, la Connettività e le Nuove Tecnologie

# LA COMUNICAZIONE

Note, Recensioni e Notizie

Pubblicazione del Dipartimento per il Digitale,  
la Connettività e le Nuove Tecnologie

Anno **2025**  
Volume **VXX**

COMUNICAZIONI ELETTRONICHE - SERVIZI POSTALI - TELEVISIONE E TECNOLOGIE DELL'INFORMAZIONE  
RADIO - SICUREZZA INFORMATICA - QUALITÀ DEI SERVIZI - COORDINAMENTO FREQUENZE  
PIANIFICAZIONE E GESTIONE SPETTRO RADIO - SCUOLA SUPERIORE DI SPECIALIZZAZIONE TLC  
SORVEGLIANZA MERCATO APPARECCHIATURE RADIO - INTEROPERABILITÀ NUMERAZIONE STANDARDIZZAZIONE  
RICERCA IN TLC E ICT - AUTORITA' DI SETTORE NIS - POLITICHE NUOVE TECNOLOGIE ABILITANTI



#### In copertina

L'immagine usata per la copertina è del fotografo U.Lucas Dubé-Cantin pubblicata con licenza ad uso gratuito sul sito [www.pexels.com](http://www.pexels.com)



**Ministero delle Imprese  
e del Made in Italy**

## LA COMUNICAZIONE

Note Recensioni e Notizie  
Anno 2025 Vol. LXX

Pubblicazione del  
**Dipartimento per il digitale, la connettività  
e le nuove tecnologie**

Capo Dipartimento

**Dott.ssa Eva Spina**

Hanno collaborato in questo numero:

*Redazione e Pubblicazione sul web*

**Corrado Pisano**

*Organizzazione, 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.

**La Comunicazione - Note, Recensioni & Notizie** è la rivista "storica" dal **1952** di informazione e divulgazione scientifica edita dal **Dipartimento per il digitale, la connettività e le nuove tecnologie**, 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

---

Dott.ssa Eva Spina      Introduzione del Capo Dipartimento      5

## Dipartimento per il digitale, la connettività e le Nuove Tecnologie

---

---

Marcello **Folli** ♦  
Manuel **Faccioli** ♦  
Claudia **Carciofi** ♦  
Valeria **Petrini** ♦

**Studio e applicazione del metodo FDP per la protezione dei collegamenti Fissi: analisi dell'interferenza tempo e spazio variante**

*Study and application of the FDP method for the protection of Fixed Service links: analysis of temporal and spatial interference variation*

**7**

♦ Fondazione Ugo Bordoni

---

Giancarlo **Butti** ♦

**La gestione della supply chain ICT nel Regolamento 2022/2554 (DORA)**

*ICT supply chain management in Regulation 2022/2554 (DORA)*

**29**

♦ Isaca Milano

---

Marina **Lotti** ♦  
Andrea **Garzia** ♦  
Claudia **Carciofi** ♦  
Simona **Valbonesi** ♦

**Studio sperimentale e numerico della perdita di penetrazione veicolare in scenari V2X**

*Experimental and numerical study of vehicle penetration loss in V2X scenarios*

**42**

♦ Fondazione Ugo Bordoni

---

# Sommario

---

Massimo <b>Celidonio</b> ♦	<b>Stato dell'arte sull'attività di regolamentazione del servizio di connettività diretta da satellite a terminali utente IMT (DC-MSS-IMT)</b>	<b>68</b>
	<i>State of the art on the regulatory activity of the direct satellite connectivity service to IMT user terminals (DC-MSS-IMT)</i>	

♦ Fondazione Ugo Bordoni

---

Valeria <b>Petrini</b> ♦ Claudia <b>Carciofi</b> ♦ Manuel <b>Faccioli</b> ♦ Andrea <b>Garzia</b> ♦	<b>Analisi delle opportunità di condivisione della banda di frequenza 27.5-29.5 GHz tra sistemi terrestri e sistemi satellitari</b>	<b>90</b>
	<i>Analysis of the spectrum sharing opportunities of the frequency band 27.5-29.5 GHz between terrestrial and satellite systems</i>	

♦ Fondazione Ugo Bordoni

---

Fabrizio <b>Cirilli</b> ♦ Massimiliano <b>Perrone</b> ♦ Luca <b>Tufarelli</b> □, Maria Lilia <b>La Porta</b> □,	<b>Gli standard ISO a supporto dell'AI ACT</b>	<b>108</b>
	<i>ISO standards supporting AI ACT</i>	

♦ PDCA Srl  
□ Avvocato - Studio Ristuccia & Tufarelli

---

## **Introduzione del Capo Dipartimento**

Il nuovo numero della rivista *“La Comunicazione – Note, Recensioni e Notizie”* intende mettere a disposizione contributi di alto profilo informativo, pensati per supportare la comprensione e la gestione delle sfide connesse alla continua evoluzione del panorama tecnologico e regolatorio.

L'edizione propone analisi e approfondimenti su temi di particolare interesse, tra cui gli standard per l'intelligenza artificiale, le comunicazioni satellitari in condivisione con quelle terrestri nonché le soluzioni di connettività diretta tra satellite e terminali IMT. Vengono inoltre esaminati argomenti di stretta attualità, quali la governance della supply chain ICT nel contesto del Regolamento DORA applicabile alle entità finanziarie, le problematiche di interferenza radio nei collegamenti fissi e le criticità legate all'attenuazione o alla perdita del segnale all'interno dei veicoli.

I contributi, redatti da specialisti del settore, offrono un inquadramento tecnico rigoroso delle tematiche trattate e al contempo stimolano una riflessione sulle ricadute operative e strategiche delle innovazioni in atto. Attraverso questa iniziativa editoriale, la rivista mira a promuovere il dialogo tra professionisti, comunità scientifica e istituzioni, favorendo l'aggiornamento costante e la diffusione del sapere.

In uno scenario segnato da trasformazioni tecnologiche rapide e profonde, affrontare le sfide della digitalizzazione, della sostenibilità e della competizione a livello globale richiede competenze avanzate e una visione strategica orientata al lungo periodo. In tale contesto, *“La Comunicazione”* si propone come strumento di orientamento in un quadro complesso, contribuendo a chiarire le opportunità derivanti dalle tecnologie emergenti, dalle politiche pubbliche e dai processi normativi in evoluzione.

Un'informazione qualificata e un percorso di formazione continua rappresentano leve fondamentali per convertire le criticità in occasioni di sviluppo e innovazione. La rivista si configura quindi come un valido supporto non solo per i professionisti del MIMIT, ma anche

per tutti gli operatori interessati a partecipare attivamente alla crescita del settore tecnologico e delle comunicazioni.

Desidero infine esprimere un sincero ringraziamento agli autori, ai ricercatori e a quanti, con professionalità e impegno, contribuiscono alla realizzazione di questa pubblicazione, garantendo contenuti affidabili, aggiornati e di qualità. Il loro contributo è determinante per consolidare il ruolo della rivista quale riferimento autorevole nel panorama dell'informazione tecnica e professionale.

**Dott.ssa Eva Spina**

Capo Dipartimento per il digitale,

la connettività e le nuove tecnologie

## **Studio e applicazione del metodo FDP per la protezione dei collegamenti Fissi: analisi dell'interferenza tempo e spazio variante**

### ***Study and application of the FDP method for the protection of Fixed Service links: analysis of temporal and spatial interference variation***

Marcello Folli ♦, Manuel Faccioli ♦, Claudia Carciofi ♦, Valeria Petrini ♦

♦ Fondazione Ugo Bordoni, Rome (Italy)

#### **Sommario**

Nell'ambito delle attività della CEPT, e in particolare del gruppo SE19 relativo ai sistemi fissi, nel settembre 2025 è stato finalizzato il Report ECC CEPT 367 [1] il quale introduce la Fractional Degradation in Performance (FDP) come criterio operativo per quantificare la frazione aggiuntiva di tempo in cui un collegamento Fixed Service (FS) non soddisfa i propri obiettivi di prestazione a causa di interferenze variabili nel tempo.

L'identificazione di appropriati criteri di protezione per i servizi fissi in funzione delle caratteristiche della sorgente interferente è un aspetto rilevante soprattutto nel contesto nazionale dove sono presenti numerosi sistemi fissi in diverse bande di frequenza.

Nel presente articolo viene illustrata e implementata in un simulatore sviluppato dalla Fondazione Ugo Bordoni (FUB) la metodologia FDP che si basa sulla combinazione tra la funzione di densità di probabilità (pdf) dell'interferenza, la distribuzione del fading del segnale voluto al ricevitore ed il margine di fading a disposizione del collegamento definito come Flat Fade Margin (FFM) o, in presenza di controllo automatico di potenza, come Net Fade Margin (NFM).

I risultati ottenuti tramite simulazioni sono stati confrontati con i medesimi test con cui è stato validato il tool CEPT di riferimento, SEAMCAT, affinché possa poi essere utilizzato anche per scenari realistici. Il metodo FDP di protezione dei sistemi FS è stato inoltre confrontato con il metodo tradizionalmente utilizzato per la coesistenza basato sul criterio I/N.

Si evidenzia che il metodo FDP presenta alcune aree di incertezza che richiedono ulteriori approfondimenti scientifici per tener conto degli effetti di interferenze impulsive di tipo burst,

dell'impatto dell'Adaptive Coding and Modulato (ACM) e delle tecniche di diversità nella mitigazione del degrado di prestazioni.

### **Abstract**

Within the framework of CEPT activities, and in particular those of the SE19 group related to fixed systems, the ECC CEPT Report 367 [1] was finalized in September 2025. This report introduces the Fractional Degradation in Performance (FDP) as an operational criterion to quantify the additional fraction of time during which a Fixed Service (FS) link fails to meet its performance objectives due to time-varying interference.

The identification of the appropriate protection criteria for fixed services considering the characteristics of the interference source is a relevant aspect especially at national level where numerous fixed systems are present in different frequency bands.

This article presents and implements, the FDP methodology, which is based on the combination of the probability density function (pdf) of the interference, the fading distribution of the wanted signal at the receiver, and the available fading margin of the link defined as the Flat Fade Margin (FFM) or, in the presence of automatic power control, as the Net Fade Margin (NFM).

The results obtained through simulations have been compared and validated against the same test cases used to validate the CEPT reference tool, SEAMCAT, so that the methodology can later be applied to realistic scenarios. Furthermore, the FDP protection method for FS systems has been compared with the traditionally used coexistence method based on the I/N criterion. It is noted that the FDP method presents certain areas of uncertainty that require further scientific investigation, particularly to account for the effects of impulsive or burst-type interference, the impact of Adaptive Coding and Modulation (ACM), and the role of diversity techniques in mitigating performance degradation.

### **Keyword**

Sistemi Fissi, Fractional Degradation in Performance, Metodo I/N.

## **1 - Introduzione**

Negli ultimi anni, la coesistenza dei collegamenti FS con un numero crescente e sempre più eterogeneo di sorgenti di interferenza ha richiesto approfondimenti scientifici sulla applicabilità di criteri di protezione basati esclusivamente su misure stazionarie o su soglie di potenza. In un recente report CEPT [2], è stata analizzata la coesistenza tra sistemi fissi e Radio Local Area Networks (RLAN) considerando diverse metodologie di protezione dei sistemi fissi per valutarne gli effetti sia nel caso di sistemi Low-Power Indoor (LPI) che nel caso di sistemi Very Low Power (VLP). L'evoluzione delle reti radio (densificazione delle celle, diffusione di servizi a bassa latenza, uso crescente di bande millimetriche e tecniche di condivisione dinamica) e l'introduzione di tecniche adattive sui link fissi (ATPC, ACM), inoltre, hanno aumentato la complessità del fenomeno interferenziale perciò non è più sufficiente conoscere il livello di interferenza, ma diventa cruciale descriverne la variabilità temporale e spaziale oltre che il suo effetto sul tempo di non disponibilità del servizio.

Per rispondere a questa esigenza, il gruppo CEPT SE19 ha sviluppato il Report ECC 367 ("Generic methodology for the protection of the Fixed Service to complement the criteria in Recommendation ITU-R F.758-8") che propone il concetto operativo di FDP per la protezione dei sistemi FS da sorgenti interferenti variabili nel tempo e nello spazio (es. WLAN, IMT). Questo criterio permette di passare da una valutazione puntuale a una valutazione probabilistica-temporale che integra la statistica di fading del segnale desiderato del link fisso e la distribuzione temporale/spaziale dell'interferenza. Tale approccio è particolarmente utile quando le sorgenti interferenti presentano caratteristiche non stazionarie quali, ad esempio, la mobilità. Poiché il criterio FDP è stato introdotto solo di recente, la letteratura tecnica sull'argomento è ancora limitata e gli studi disponibili sono pochi. Ciò rende particolarmente significativo ogni contributo che affronti il tema con un approccio quantitativo e basato su dati reali. In questo contesto, uno dei pochi riferimenti attualmente disponibili è il contributo presentato dalla Francia in ambito ECC PT1, che offre una delle prime valutazioni site-specific dell'impatto delle reti IMT sui collegamenti FS nella banda 6425–7125 MHz. Lo studio si

distingue per l'impiego di deployment reali FS e IMT, per l'utilizzo di modelli di propagazione consolidati e per un'estesa simulazione Monte Carlo, configurandosi come un contributo tecnico rilevante in un settore di ricerca ancora nelle sue fasi iniziali [3]. Tali considerazioni forniscono il contesto entro cui si inserisce anche il presente lavoro.

Nelle sezioni successive, infatti, saranno descritte la metodologia generale per il calcolo del metodo FDP e le modalità di implementazione simulativa del metodo. Saranno inoltre presentati i risultati ottenuti dal simulatore sviluppato da FUB e la validazione dei risultati con il tool di riferimento CEPT (Seamcat). Infine, saranno illustrati i principali limiti del metodo FDP che richiedono ulteriori approfondimenti scientifici e ulteriori verifiche simulate e sperimentali.

## **2 – Definizioni Essenziali e Metodologia**

Nel valutare la protezione dei collegamenti FS è necessario partire dagli obiettivi che questi link devono garantire per il corretto funzionamento: gli Error Performance Objectives (EPO) e gli Availability Performance Objectives (APO) i quali definiscono rispettivamente i requisiti di progetto e le soglie attese a livello regolatorio, spesso misurate tramite indicatori temporali come gli Errored Seconds (ES) o i Severely Errored Seconds (SES). Queste metriche collegano direttamente il livello di qualità del canale a grandezze osservabili nel tempo in quanto si verificano ogni qual volta il rapporto  $\Delta C/N$  supera il margine di fading (Figura 1). Per questo motivo la valutazione della degradazione dovuta all'interferenza viene espressa in termini probabilistici-temporali.

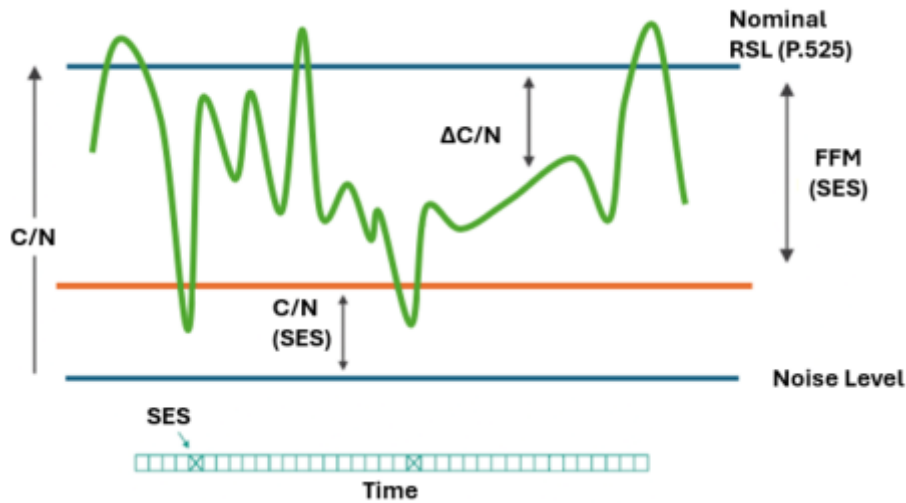


Figura 1 - Definizioni fondamentali metodo FDP

La metodologia FDP delineata in [1] si fonda sul concetto che la degradazione di prestazioni di un collegamento FS in presenza di interferenza debba essere misurata non solo come condizione istantanea, ma come variazione della probabilità di fuori servizio (outage probability) su un orizzonte temporale definito. Per questo motivo, la procedura richiede la conoscenza di tre parametri tecnici fondamentali:

- Margine di Fading;
- distribuzione del fading del segnale voluto al ricevitore del Fixed Service (Raccomandazione ITU-R P.530 [9]);
- funzione di densità di probabilità del segnale di interferenza al ricevitore FS.

In termini formali, la FDP è definita come:

$$FDP = (P_{O,i}/P_{O,0}) - 1 \quad (1)$$

Dove  $P_{O,0}$  è la probabilità di outage in assenza di interferenza mentre  $P_{O,i}$  la probabilità di outage in presenza di interferenza.

Come si può facilmente intuire, un punto operativo cruciale nella valutazione del metodo è la costruzione della distribuzione dell'interferenza normalizzata al rumore, cioè la pdf di I/N. Derivarla richiede una modellazione realistica dei fenomeni fisici e deve catturare non solo il livello medio degli interferenti ma anche la loro variabilità spaziale e temporale. Tipicamente,

nell'ambito dei lavori che si stanno svolgendo a livello CEPT si raccomanda di produrre le distribuzioni I/N mediante l'impiego di simulazioni Monte-Carlo, adattando la modalità di simulazione al grado di conoscenza delle posizioni e del comportamento degli interferenti.

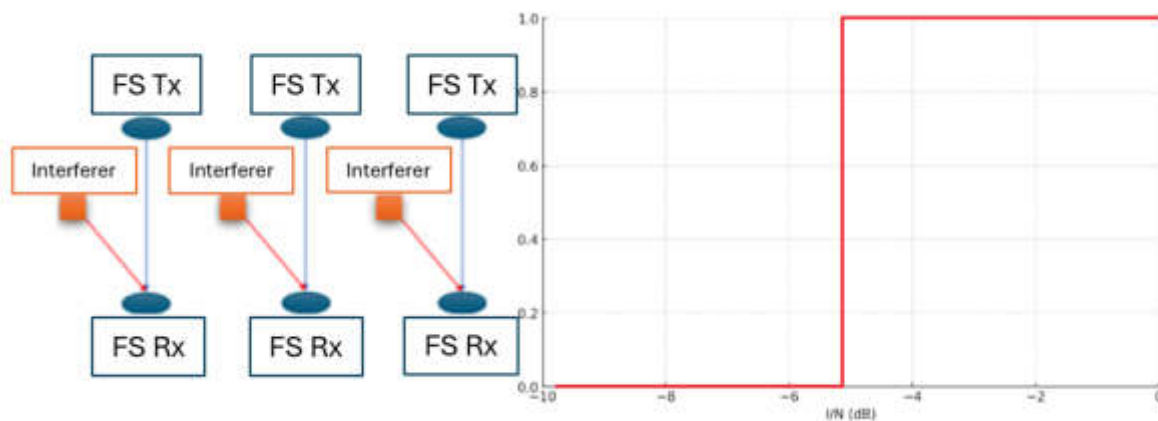


Figura 2 Esempio di distribuzione I/N in cui la posizione dell'interferente è fissa e conosciuta

Se le posizioni degli interferenti fissi sono note, la simulazione si applica direttamente alla topologia reale e produce un singolo valore di FDP per questa configurazione (Figura 2).

Quando, invece, la posizione degli interferenti fissi è casuale, si generano molteplici configurazioni spaziali (space-only Monte-Carlo) in modo da esplorare l'insieme delle topologie possibili e ricavare la distribuzione corrispondente (Figura 3).**Errore. L'origine riferimento non è stata trovata.**

M. Folli, M. Faccioli, C. Carciofi, V. Petrini

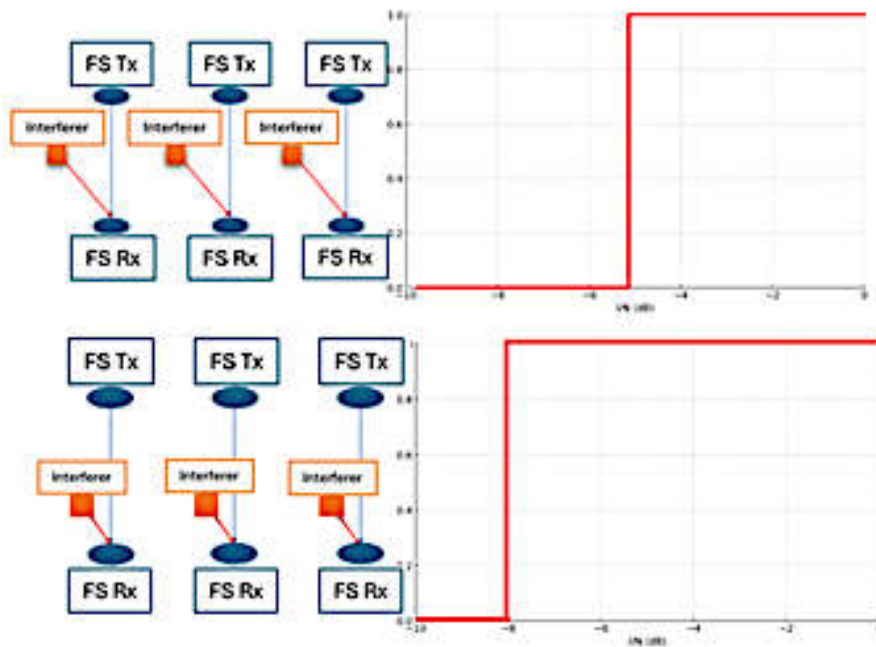


Figura 3 Esempio di distribuzione I/N in cui la posizione dell'interferente è fissa e casuale (con distribuzione statistica conosciuta)

In generale, la scelta dell'approccio utilizzato per la modellazione dipende dalla natura della sorgente interferente: la prevalenza di dispositivi mobili richiede modelli congiunti (space-time Monte-Carlo) mentre sorgenti di interferenti fissi ma non perfettamente localizzati possono essere efficacemente trattate con metodi space-only.

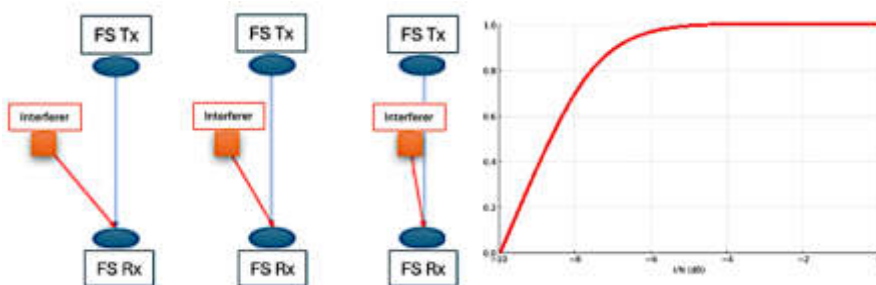


Figura 4 Esempio di distribuzione I/N in cui l'interferente è in movimento e con posizioni conosciute

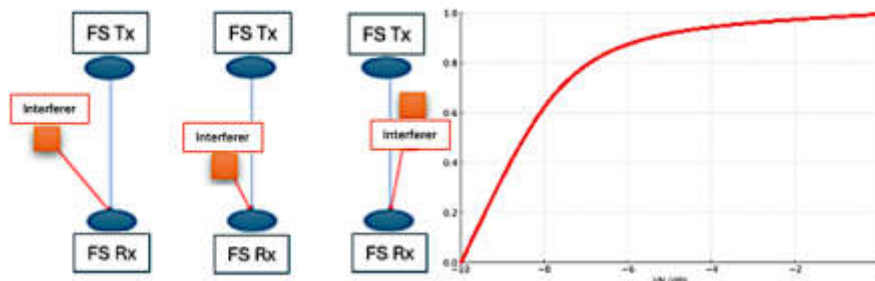


Figura 5 Esempio di distribuzione I/N in cui l'interferente è in movimento e con posizioni casuali (con distribuzione statistica conosciuta)

Su queste basi, la probabilità di outage in presenza di interferenza viene definita dal seguente integrale congiunto:

$$P_{O,i} = \int_{z=0}^{+\infty} pdf_z(z) Prob(f \geq FM - 10 \log(1 + z)) dz \quad (2)$$

Dove:

- $z$  è la variabile casuale che rappresenta il rapporto interferenza/rumore I/N in forma lineare;
- $pdf_z(z)$  è la pdf di I/N;
- $Prob(f \geq FM - 10 \log(1 + z))$  è la probabilità di superamento del margine di fading per il segnale desiderato, determinata a partire dalla distribuzione di fading (ITU-R P.530);
- Il termine  $10 \log(1 + z)$  rappresenta la penalizzazione, in dB, introdotta dall'interferenza rispetto al rumore termico.

L'FDP, inoltre, può essere ulteriormente scomposto in due contributi distinti: una componente short-term ( $FDP_{ST}$ ), che rappresenta la degradazione dovuta a picchi di interferenza che superano direttamente il fade margin, ed una componente long-term ( $FDP_{LT}$ ), che descrive le situazioni in cui la combinazione tra fading del segnale e interferenza determina complessivamente il superamento del margine disponibile. Questa distinzione è cruciale per interpretare i risultati: eventi di brevissima durata ma alta ampiezza (burst, transitori dovuti a interferenti molto vicini) impattano prevalentemente su  $FDP_{ST}$ , mentre interferenze

persistenti e di bassa intensità “accumulano” il loro effetto nell' $FDP_{LT}$ . L'equazione (1), perciò, si può riscrivere come:

$$FDP = FDP_{LT} + FDP_{ST} = \frac{P_{O,iLT} - P_{O,0}}{P_{O,0}} + \frac{P_{O,iST} - P_{O,0}}{P_{O,0}} \quad (3)$$

In cui:

$$FDP_{LT} = \frac{\int_{z=0}^{z < (i/n)_{st}} pdf_z(z) Prob(f \geq FM - 10 \log(1 + z)) dz - (1 - \gamma) \times EPO}{EPO} =$$

$$\frac{\int_{z=0}^{z < (i/n)_{st}} pdf_z(z) Prob(f \geq FM - 10 \log(1 + z)) dz}{EPO} - (1 - \gamma) \quad (4)$$

$$FDP_{ST} = \frac{\int_{z=(i/n)_{st}}^{+\infty} pdf_z(z) Prob(f \geq FM - 10 \log(1 + z)) dz - \gamma \times EPO}{EPO} =$$

$$\frac{\int_{z=(i/n)_{st}}^{+\infty} pdf_z(z) Prob(f \geq FM - 10 \log(1 + z)) dz}{EPO} - \gamma \quad (5)$$

Dove:

- $P_{O,0} = Prob(f \geq FM) = EPO$
- $\gamma = Prob(z \geq (i/n)_{st})$

Particolare attenzione va rivolta alle tecnologie adattive che influenzano in modo diretto la disponibilità del fade margin del collegamento. L'ATPC riduce la potenza trasmessa in condizioni favorevoli, diminuendo la riserva disponibile per contrastare eventuali picchi di interferenza. Per questo motivo, nelle valutazioni pratiche, il margine nominale Flat Fade Margin deve essere sostituito con il Net Fade Margin.

$$NFM = FFM - ATPC_{RANGE} \quad (6)$$

Risulta quindi necessario modellare in modo esplicito la soglia e la dinamica di attivazione dell'ATPC modificando opportunamente le equazioni di calcolo contenute nell'eq. 3:

M. Folli, M. Faccioli, C. Carciofi, V. Petrini

$$P_{O,iATPCLT} = \int_0^{(i/n)_{st}} pdf_z(z) Prob(f > FM - 10 \log(1 + z)) dz + \gamma \times P_{o,0}$$

(7)

$$P_{O,iATPCST} = Prob(f \leq ATPC \text{ Range}) Prob(10 \log(1 + z) \geq NFM) + Prob(10 \log(1 + z) > NFM) Prob(f > ATPC \text{ range}) + (1 - \gamma) \times P_{o,0} = Prob(10 \log(1 + z) \geq NFM) + (1 - \gamma) \times P_{o,0}$$

(8)

Parallelamente, l'Adaptive Coding and Modulation (ACM) interrompe la relazione lineare tra SNR e qualità del collegamento: le variazioni di schema di modulazione e codifica (MCS) introducono curve non lineari throughput-vs-SNR e BER-vs-SNR, per cui un identico decremento di SNR può generare perdite di capacità molto diverse a seconda del profilo ACM in uso (Figura 6). Di conseguenza, le simulazioni devono includere le curve MCS-specifiche del sistema e definire con chiarezza la modulazione di riferimento o la soglia operativa utilizzata per il calcolo della probabilità di outage, in modo da rappresentare correttamente il comportamento dinamico del collegamento.

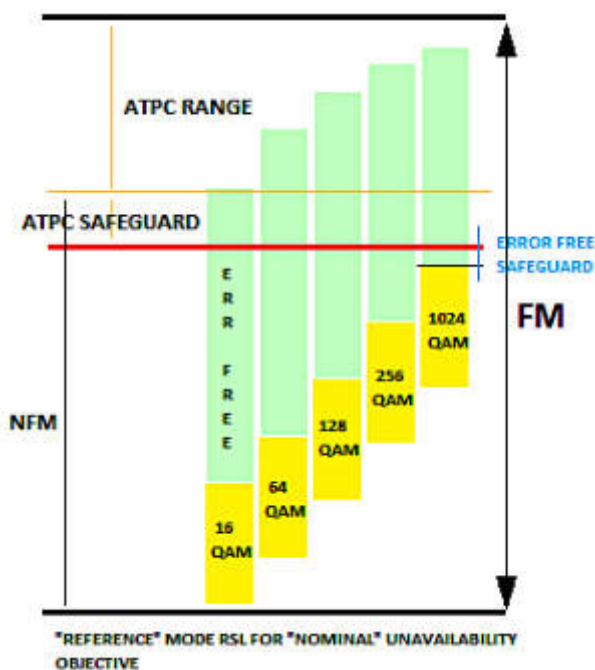


Figura 6 Modalità di funzionamento mista (ACM + ATPC)

In sintesi, ATPC e ACM non sono aspetti tecnici trascurabili ma variabili che influenzano sia la stima di  $P_{O,i}$  che il termine dominante tra  $FDP_{ST}$  e  $FDP_{LT}$ .

### **3 – Criteri di protezione Raccomandati**

I criteri di protezione raccomandati in [1] richiedono che l'FDP dovrebbe rimanere al di sotto di soglie prestabilite indicativamente  $\leq 10\%$  per interferenze da servizi co-primari e  $\leq 1\%$  per interferenze non co-primarie.

Secondo la raccomandazione ITU-R F.1494 [4], in scenari tipicamente dominati dal multipath la quota long-term tende a prevalere (es. ordine di grandezza  $90\% FDP_{LT} / 10\% FDP_{ST}$ ), mentre in scenari dove l'effetto della pioggia è dominante la raccomandazione ITU-R F.1495 [5] definisce che la componente short-term sia quella dominante (es.  $80\% FDP_{ST} / 20\% FDP_{LT}$ ). Queste percentuali vanno usate esclusivamente come valori semplificativi nelle analisi Monte-Carlo e non come valori assoluti in quanto le variabili di input influenzano i risultati finali.

È importante far notare che alcuni aspetti tecnici richiedono attenzione per l'utilizzo del metodo teorico FDP. In primo luogo, le emissioni a burst possono produrre effetti non lineari difficili da catturare con modelli di interferenza stazionari: la durata dell'impulso, il duty-cycle e la frequenza di ripetizione influenzano fortemente l'effetto sul ricevitore e la valutazione di outage. In secondo luogo, l'uso di diversità spaziale modifica la statistica del fading e la sensibilità ai picchi interferenti, perciò le ipotesi di fading semplice possono non essere valide in presenza di configurazioni complesse di diversità. Il terzo fattore critico è il comportamento reale della catena ricevente: ricevitori differenti reagiscono in modo diverso a impulsi brevi o a interferenze a duty-cycle basso, con impatti concreti su ES/SES che i modelli idealizzati non prevedono.

In aggiunta, la possibile correlazione statistica del fading tra il percorso voluto e il percorso interferente tipicamente rilevante in condizioni meteorologiche avverse può invalidare l'assunzione di indipendenza usata in molte derivazioni analitiche. Per questi motivi in [1] viene suggerito di accompagnare le analisi teoriche con campagne di misura e test di

laboratorio che caratterizzino profili temporali di burst, risposta dinamica dei ricevitori, effetti della diversità e le statistiche congiunte di fading. Questi elementi andrebbero considerati come priorità per temi di ricerca e studi sperimentali futuri, perché solo la combinazione di modellazione avanzata e validazione sperimentale può garantire stime di FDP robuste e applicabili in contesti operativi reali.

#### 4 –Risultati metodo FDP: validazione implementativa e confronto con metodo I/N

Come accennato in precedenza, l'implementazione del metodo FDP all'interno degli strumenti simulativi della Fondazione ha previsto una fase di validazione, durante la quale ogni valore intermedio è stato verificato utilizzando i dati pubblicamente accessibili sui siti web dell'ECC-CEPT.

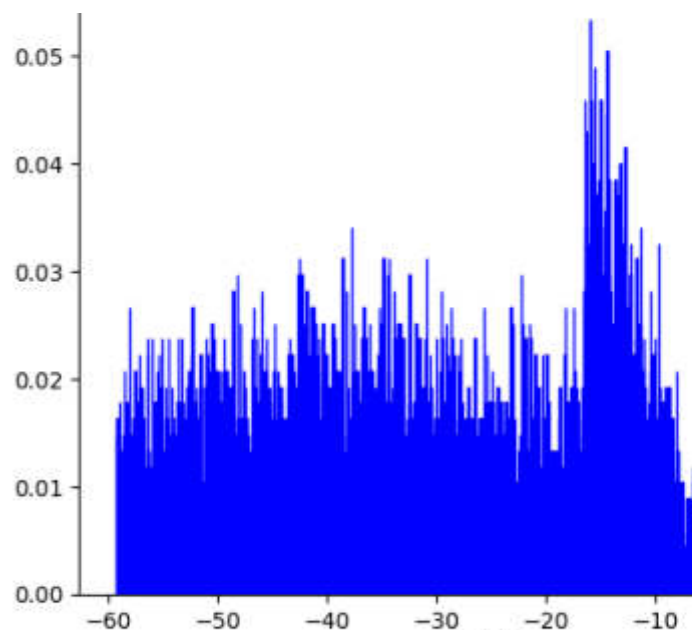


Figura 7 PDF del vettore I/N scelto per eseguire l'analisi

Tali dati consentono infatti un'analisi completa del collegamento FS, descrivendone in modo esaustivo tutte le caratteristiche. Prendendo come riferimento il primo test presentato in [6],

i cui parametri di input sono elencati in Tabella 1 a cui si aggiunge il vettore I/N, è possibile calcolare la probabilità di disservizio sia in assenza che in presenza di interferenza.

Tabella 1 Parametri di input del metodo FDP

Inputs		
Longitudine	15.5	deg
Latitudine	45	deg
he	20	m
hr	20	m
ht	0	m
Frequenza	6	GHz
Distanza	30	km
Margine di Fading	10	dB
Rumore di fondo	-94	dBm

In generale, la metodologia implementata si basa sull'applicazione del modello ITU-R P.530 per la stima della probabilità di fading nei collegamenti radio integrandola con l'analisi statistica del rapporto interferenza/rumore (I/N). L'obiettivo è quantificare la probabilità complessiva di degrado delle prestazioni del collegamento, tenendo conto sia del fading che degli effetti di interferenza. Per ogni valore possibile del rapporto I/N, ricavato dalla distribuzione statistica del rumore interferente (Figura 7), viene stimato il corrispondente livello di peggioramento della qualità del link. Questo permette di valutare come varia la probabilità di degrado al crescere dell'interferenza distinguendo la componente a lungo termine (LT) e la componente a breve termine (ST). La separazione tra le due regioni avviene individuando la soglia di I/N al di sopra della quale l'interferenza provoca un degrado significativo del margine di fading, oppure, in presenza di controllo automatico di potenza, quando l'escursione di potenza disponibile viene esaurita. Una volta definite le due regioni, le probabilità associate vengono calcolate mediante integrazione numerica. I risultati finali forniscono la probabilità totale di degrado (FDP) e le sue componenti a lungo e breve termine, espresse in percentuale rispetto alla probabilità di fading pura (vedi Tabella 2).

Tabella 2 Risultati estesi test di validazione

FDP	18.8733
FDP_LT	18.8733
FDP_ST	0
p0	8.8122
P00 (%)	0.6423
POI (%)	0.7635
POI_LT	0.0076
POI_ST	0.0064
Gamma	0
IN_ST	9.5424

Per verificare la correttezza dell'implementazione sviluppata, è stata condotta una ulteriore, e generale, validazione diretta dei risultati calcolati rispetto a quelli forniti dal SEAMCAT Technical Group (STG) [6], [7] dell'ECC/CEPT. La tabella di confronto (Tabella 3) riporta, per ciascun caso di test, i valori di FDP totale,  $FDP_{LT}$  e  $FDP_{ST}$  ottenuti con l'algoritmo implementato (FUB) e con il riferimento ufficiale (ECO).

Tabella 3 Validazione implementativa - No ATPC

Test	Metriche	Risultati ECO [%]	Risultati FUB [%]	Differenza assoluta	Test	Metriche	Risultati ECO [%]	Risultati FUB [%]	Differenza assoluta
S1_case1	FDP	12.4963	12.49630921	9.21327E-06	S6_case1	FDP	80.633	80.63343435	0.000434347
S1_case1	FDP_LT	4.6318	4.6318327	3.26995E-05	S6_case1	FDP_LT	62.459	62.45923771	0.000237714
S1_case1	FDP_ST	7.8644	7.864476514	7.65137E-05	S6_case1	FDP_ST	18.174	18.17419663	0.000196633
S1_case2	FDP	12.6165	12.61653071	3.07068E-05	S6_case2	FDP	79.452647	79.45264712	1.1525E-07
S1_case2	FDP_LT	4.479	4.479500747	0.000500747	S6_case2	FDP_LT	79.452647	79.45264712	1.1525E-07
S1_case2	FDP_ST	8.137	8.13702996	2.996E-05	S6_case2	FDP_ST	0	0	0
S2	FDP	16.406	16.199043	-0.206956996	S7	FDP	45.2461	45.24618343	8.34281E-05
S2	FDP_LT	16.406	16.199043	-0.206956996	S7	FDP_LT	31.89332	31.89332458	4.58065E-06
S2	FDP_ST	0	0	0	S7	FDP_ST	13.3528	13.35285885	5.88474E-05
S3	FDP	17.7248	17.72482586	2.58622E-05	S8	FDP	180.01736	180.0173637	3.67285E-06
S3	FDP_LT	17.7248	17.72482586	2.58622E-05	S8	FDP_LT	101.9188	101.9188425	4.25496E-05
S3	FDP_ST	0	0	0	S8	FDP_ST	78.09852	78.09852112	1.12326E-06
S4	FDP	249.58241	249.5534526	-0.028957445	S9	FDP	11.9544	11.95443513	3.51256E-05
S4	FDP_LT	249.58241	249.5534526	-0.028957445	S9	FDP_LT	11.9544	11.95443513	3.51256E-05
S4	FDP_ST	0	0	0	S9	FDP_ST	0	0	0
S5	FDP	18.87333	18.87333874	8.73682E-06	S11	FDP	7.665	7.665006819	6.81901E-06
S5	FDP_LT	18.87333	18.87333874	8.73682E-06	S11	FDP_LT	5.6307	5.630707975	7.9748E-06
S5	FDP_ST	0	0	0	S11	FDP_ST	2.0343	2.034298844	-1.15579E-06

L'analisi copre sia scenari a interferenza prevalentemente long-term (in cui  $FDP_{ST}$  risulta nulla o marginale), sia casi a maggiore componente short-term, come nei test S1. In tutti i casi, la concordanza fra FDP totale e le sue componenti mostra che la catena di calcolo è stata riprodotta correttamente e che le differenze numeriche rientrano pienamente nella precisione attesa.

Tabella 4 Validazione implementativa - ATPC

Test	Metriche	Risultati ECO [%]	Risultati FUB [%]	Differenza assoluta
S5	FDP	40.652	40.65226589	0.000265892
S5	FDP_LT	0.7265	0.726537533	3.75332E-05
S5	FDP_ST	39.9257	39.92572836	2.83588E-05
S6	FDP	29.9225	29.92255123	5.12295E-05
S6	FDP_LT	8.874	8.874085059	8.50589E-05
S6	FDP_ST	21.0486	21.04846617	-0.000133829

In Tabella 4, sono mostrati i risultati dell'analisi in cui il collegamento FS impiega l'ATPC, con conseguente sostituzione del Flat Fade Margin con il Net Fade Margin nel calcolo. Anche in questi scenari, i risultati ottenuti con l'implementazione FUB mostrano un'ottima corrispondenza con i valori di riferimento CEPT, con differenze assolute dell'ordine di  $10^{-5}$ .

Dal confronto emerge che l'introduzione dell'ATPC modifica la distribuzione tra le componenti short-term e long-term del livello di degradazione del segnale: la riduzione del margine effettivo disponibile incrementa la sensibilità ai picchi interferenti, comportando una quota  $FDP_{ST}$  significativamente superiore rispetto alla  $FDP_{LT}$ . Questo comportamento è coerente con quanto previsto in [1], secondo cui l'ATPC, pur migliorando l'efficienza energetica del link in condizioni normali, può ridurre temporaneamente la resilienza ai transitori di interferenza quando la potenza trasmessa è al minimo.

In entrambi i casi analizzati, la perfetta coerenza numerica tra implementazioni conferma che l'algoritmo gestisce correttamente la dinamica dell'ATPC e il passaggio dal margine nominale (FFM) a quello effettivo (NFM). L'accuratezza del modello consente quindi di estendere con

affidabilità la metodologia FDP anche a collegamenti adattivi, mantenendo la compatibilità con i risultati di riferimento CEPT.

In termini operativi, questi risultati dimostrano che l'approccio implementato consente di replicare fedelmente la metodologia FDP definita in [1], garantendo consistenza con i benchmark ufficiali CEPT. Tale validazione costituisce quindi una base affidabile per applicare l'algoritmo a studi di compatibilità nazionali o a campagne di simulazione su scenari reali.

Infine, sono stati prodotti confronti con il metodo tradizionalmente utilizzato per le analisi di coesistenza, in cui un link fisso è considerato protetto se, e solamente se, il valore di I/N corrispondente risulta inferiore a  $-10$  dB. Tale soglia, definita dal criterio di protezione I/N riportato nella Raccomandazione ITU-R F.758-6 [8], garantisce che il degrado del rapporto segnale/rumore complessivo del sistema risulti accettabile per la salvaguardia delle prestazioni di un link fisso. A tal fine è stata sviluppata una procedura che, a partire da un insieme di valori di I/N, calcolati attraverso la procedura Minimum Coupling Loss (MCL), genera, mediante un approccio in stile Monte Carlo, un vettore di lunghezza estesa. Per l'esecuzione dell'analisi è stato scelto casualmente un intervallo di distanze  $[d_{random}, d_{random} + 1 \text{ km}]$  entro il quale, per ciascuna direzione radiale rispetto al servizio fisso, sono stati simulati gli interferenti orientando, al fine di rappresentare la condizione di interferenza più sfavorevole possibile, le antenne verso il sistema FS.

Una volta calcolati i valori relativi al worst case, il vettore è stato esteso generando, in modo casuale, nuovi puntamenti per ciascun interferente, simulando così il servizio dei dispositivi mobili e la conseguente degradazione dell'interferenza verso il sistema FS. L'analisi complessiva ha considerato diverse configurazioni di link, differenziate in base ai parametri di margine di fading, larghezza di banda e coordinate spaziali dei sistemi ricevente (Rx) e trasmittente (Tx).

A titolo esemplificativo di seguito sono riportati i risultati di quattro casi di test sviluppati utilizzando dati di sistemi FS realmente esistenti.

Tabella 5 Confronto 1 FDP - I/N: Valori FDP

FDP (%)	21.94566
FDP_LT (%)	11.9056
FDP_ST (%)	10.04006
IN_ST (dB)	31.99726
FM (dB)	32
Metodo I/N superamento soglia protezione (%)	5

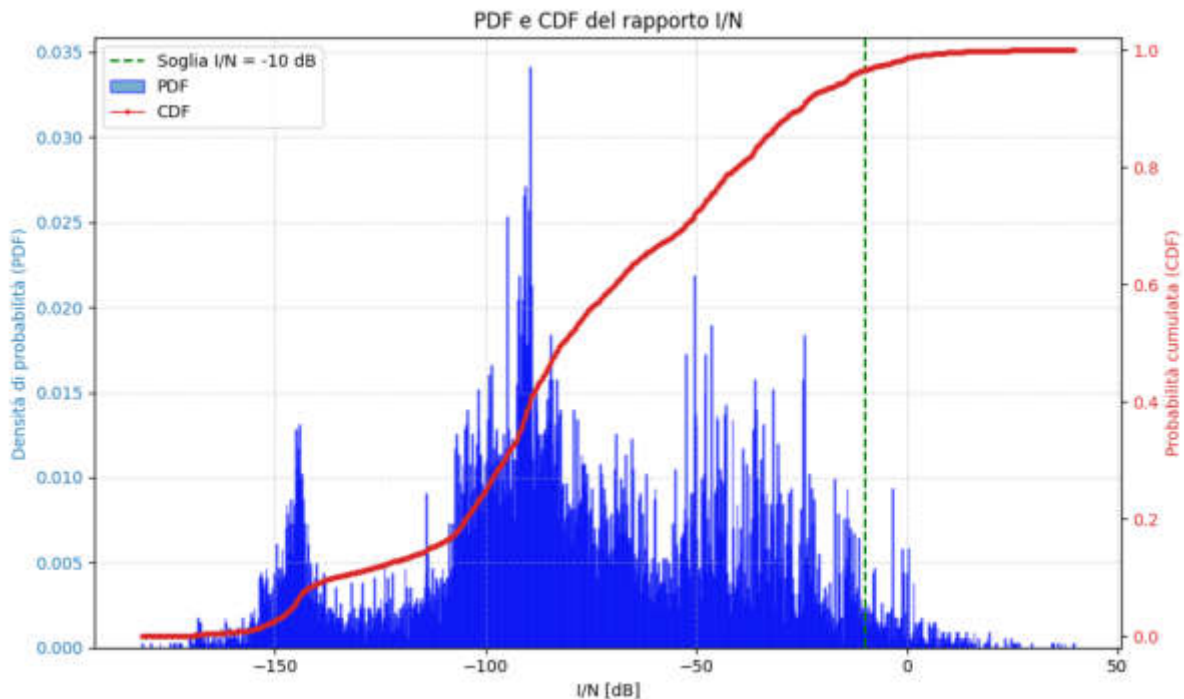


Figura 8 PDF e CDF di I/N - confronto 1

Nel primo scenario analizzato (Tabella 5), sia il metodo FDP che, nel 5% dei casi, il criterio I/N evidenziano il mancato rispetto della protezione del sistema fisso. Come prevedibile dalla distribuzione (Figura 8), la componente dominante risulta essere quella long-term in quanto il valore di soglia  $\left(\frac{I}{N}\right)_{ST}$  è piuttosto elevato e consente la protezione rispetto alle interferenze

M. Folli, M. Faccioli, C. Carciofi, V. Petrini

short term. Nel caso successivo, invece, si osserva il rispetto di entrambi i criteri; in particolare, ricordando il significato fisico delle equazioni (4) e (5), il valore associato al margine di fading (Tabella 6) consente di mitigare gli effetti dell'interferenza la cui distribuzione è mostrata in Figura 9. Nel terzo scenario, in cui si è simulato un sistema fisso dotato di ATPC (Tabella 7 e Figura 10), risulta soddisfatto il solo criterio I/N.

Tabella 6 Confronto 2 FDP - I/N: Valori FDP

FDP (%)	0.000001
FDP_LT (%)	0.000001
FDP_ST (%)	0
IN_ST (dB)	31.99726
FM (dB)	32
Metodo I/N superamento soglia protezione (%)	0

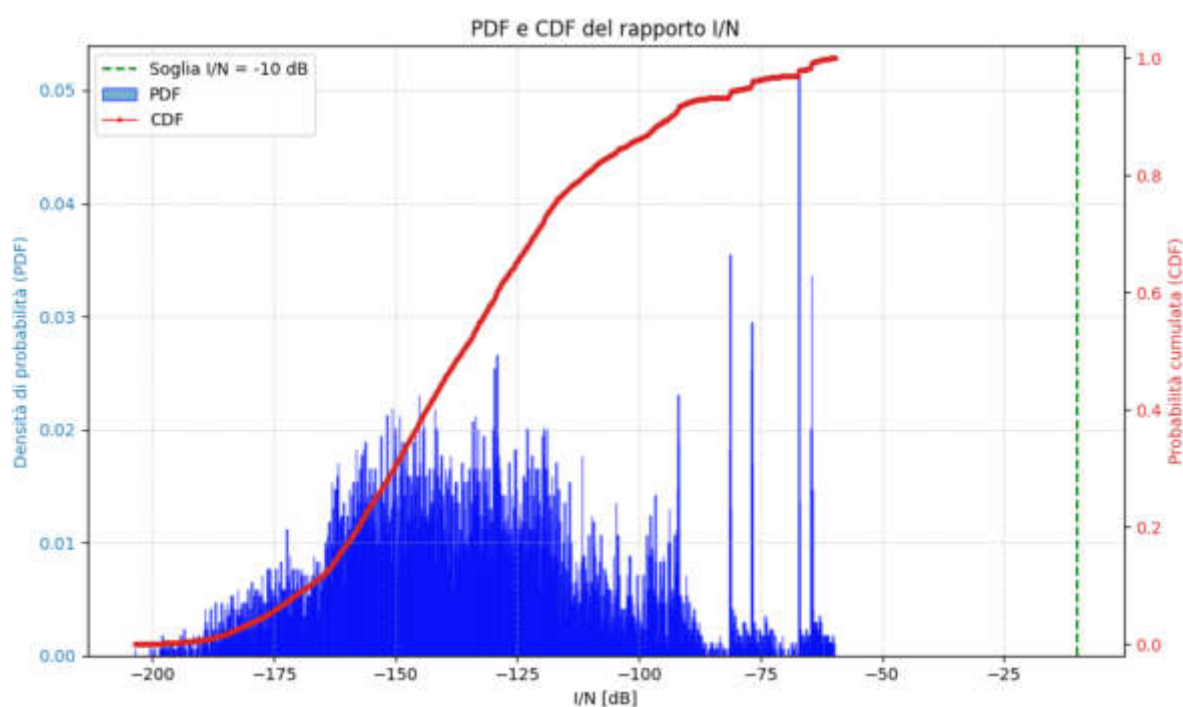


Figura 9 PDF e CDF di I/N - confronto 2

Come evidenziato in precedenza, l'impiego di tale tecnologia comporta una riduzione del margine di fading effettivamente disponibile; di conseguenza, risulta facilmente comprensibile il motivo per cui soltanto il criterio I/N risulti rispettato.

Infine nel quarto, ed ultimo, caso il criterio I/N non è rispettato nell'1% dei casi mentre per l'FDP vale la stessa motivazione dedotta per il secondo caso di test.

Tabella 7 Confronto 3 FDP - I/N: Valori FDP

FDP (%)	1266.43
FDP_LT (%)	0.004396
FDP_ST (%)	1266.426
IN_ST (dB)	-5.86825
ATPC Range (dB)	36
FM (dB)	37
IN_ST (dB)	-5.86825
Metodo I/N superamento soglia protezione (%)	0

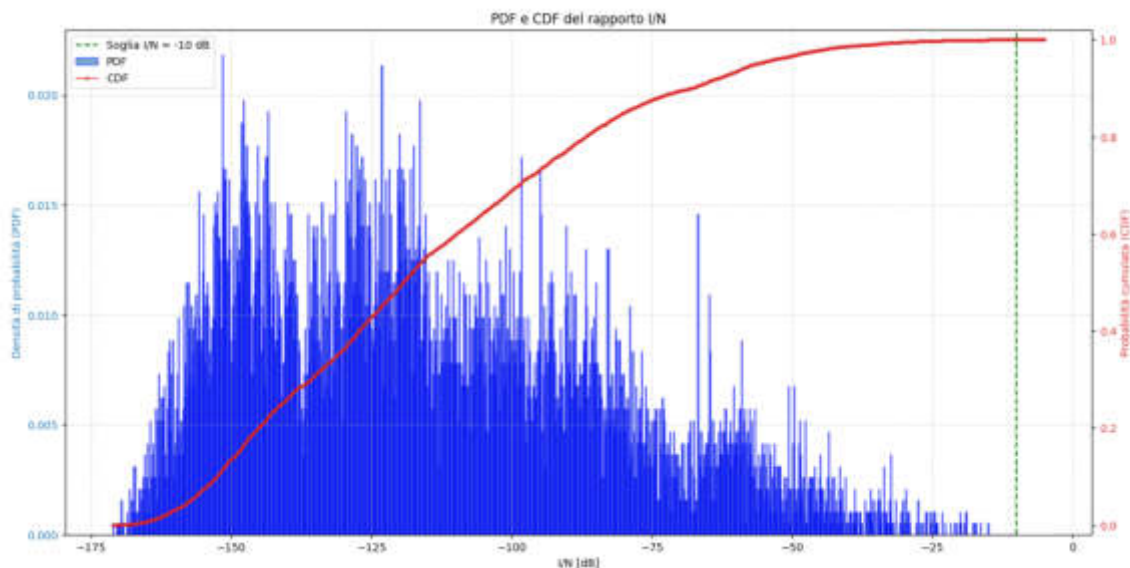


Figura 10 PDF e CDF di I/N - confronto 3

Tabella 8 Confronto 4 FDP - I/N: Valori FDP

FDP (%)	0.224396
FDP_LT (%)	0.224396
FDP_ST (%)	0
IN_ST (dB)	31.99726
FM (dB)	32
Metodo I/N superamento soglia protezione (%)	1

M. Folli, M. Faccioli, C. Carciofi, V. Petrini

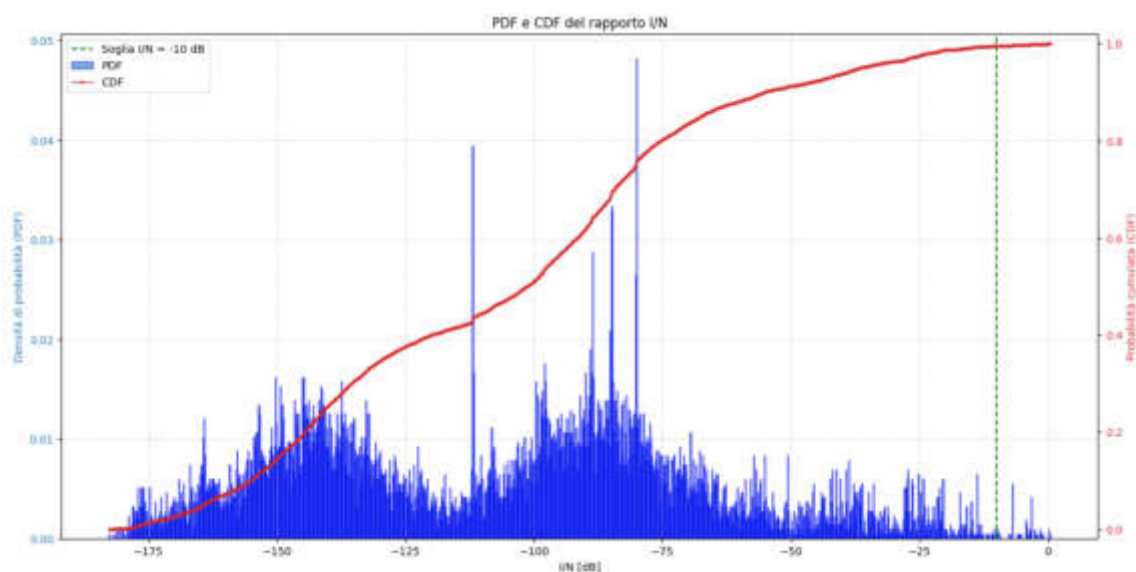


Figura 11 PDF e CDF di I/N - confronto 4

## 5 – Conclusioni

Il lavoro presentato ha descritto l'implementazione simulativa sviluppata da FUB, la validazione tramite confronto con tool CEPT e l'impatto sulla protezione dei sistemi fissi del nuovo metodo Fractional Degradation in Performance (FDP) recentemente approvato in ambito CEPT come criterio alternativo al tradizionale I/N per la protezione dei collegamenti del Fixed Service (FS) in presenza di interferenze tempo e spazio varianti. In ambito CEPT, inoltre, diverse amministrazioni hanno recentemente risposto ad un questionario [10] relativo a questa tecnologia, consentendo di ottenere una descrizione statistica più accurata dei sistemi utilizzati nei vari paesi. Queste informazioni, in futuro, potranno essere utilizzate per integrare i risultati di questo studio e confermare che il metodo FDP, grazie alla sua natura probabilistica e temporale, consente di tener conto dell'effetto dell'interferenza sia "long term" che "short term" permettendo una descrizione più realistica del comportamento dei collegamenti fissi in ambienti interferenziali complessi, superando i limiti delle valutazioni statiche del metodo I/N basate esclusivamente su soglie di potenza. Ciò è particolarmente rilevante in scenari caratterizzati da interferenze non stazionarie, come quelle generate da servizi mobili IMT o da sorgenti con duty-cycle variabile RLAN/WLAN. Sono stati considerati

diversi scenari interferenziali realistici mostrando un confronto dei risultati tra il metodo FDP e I/N in termini di rispetto del criterio di protezione per i sistemi FS stabilito in ambito CEPT e ITU per le due metodologie.

Si evidenzia che l'applicazione operativa del metodo FDP presenta alcune criticità che richiedono ulteriori approfondimenti scientifici tra cui sono di particolare rilevanza la modellazione accurata delle interferenze a burst e l'influenza delle tecniche adattative e di diversità.

## **7 – Bibliografia**

[1] ECC CEPT, Draft Report 367 "General methodology for derivation of protection of Fixed Service links to complement the criteria in Recommendation ITU-R F.758-8", 2025

[2] ECC CEPT, Report 364 "Sharing and compatibility studies related to Wireless Access Systems including Radio Local Area Networks (WAS/RLAN) in the frequency band 6425-7125 MHz", 2025

[3] ECC CEPT Project Team 1, Meeting Document PT1(25)147\_France: "PT1\_58: Site-specific FS Study", 2025

[4] ITU-R, Recommendation ITU-R F.1494 "Interference criteria to protect the fixed service from time varying aggregate interference from other services sharing the 10.7-12.75 GHz band on a co-primary basis", 2000

[5] ITU-R, Recommendation ITU-R F.1495-2 "Interference criteria to protect the fixed service from time varying aggregate interference from other radiocommunication services sharing the 17.7-19.3 GHz band on a co-primary basis", 2012

[6] SEAMCAT Technical Group, Meeting Document STG(25)012A03 "Tests eEPP FDP Without ATPC", 2025

[7] SEAMCAT Technical Group, Meeting Document STG(25)012A04 "Tests eEPP FDP With ATPC", 2025

**[8]** ITU-R, Recommendation ITU-R 758-6 “System parameters and considerations in the development of criteria for sharing or compatibility between digital fixed wireless systems in the fixed service and systems in other services and other sources of interference”, 2015

**[9]** ITU-R, Recommendation ITU-R 530-19 “Propagation data and prediction methods required for the design of terrestrial line-of-sights systems”, 2005

**[10]** ECC CEPT, Report 365 “Fixed Links in CEPT; Technical characteristics and statistical review”, 2025

## **La gestione della supply chain ICT nel Regolamento 2022/2554 (DORA)**

### ***ICT supply chain management in Regulation 2022/2554 (DORA)***

Giancarlo Butti ♦

♦ Comitato scientifico del CLUSIT - Milano

#### **Sommario**

Uno dei pillar del Regolamento DORA (Digital Operational Resilience Act), entrato in vigore nel gennaio 2023 e pienamente operativo dal gennaio 2025, riguarda la gestione dell'intero ciclo di vita del rapporto fra le entità finanziarie (termine con cui nella normativa sono identificate 20 diverse tipologie di enti, quali banche, assicurazioni, SGR...) ed i fornitori ICT.

A tale tema, il regolamento dedica sia una specifica parte del testo normativo, sia ulteriori regolamenti aggiuntivi, fornendo un livello di dettaglio difficilmente riscontrabile in altre normative.

Per questo motivo, al di là dell'ambito di applicazione specifico, costituito dalla entità finanziarie e dai loro fornitori ICT, la normativa DORA può costituire una buona pratica di riferimento per qualunque altro settore.

#### **Abstract**

*One of the pillars of the DORA (Digital Operational Resilience Act) Regulation, which came into force in January 2023 and is fully operational from January 2025, concerns the management of the entire life cycle of the relationship between financial entities (a term used in the regulation to identify 20 different types of entities, such as banks, insurance companies, asset management companies...) and ICT suppliers.*

*The regulation dedicates both a specific part of the regulatory text and further additional regulations to this topic, providing a level of detail that is difficult to find in other regulations.*

*For this reason, beyond the specific scope of application, consisting of financial entities and their ICT suppliers, the DORA regulation can constitute a good reference practice for any other sector.*

## **Keyword**

Supply chain, risk, exit strategy, business continuity

## **1 - Introduzione**

Il **Regolamento (UE) 2022/2554** (Regolamento (UE) 2022/2554 del Parlamento europeo e del Consiglio del 14 dicembre 2022 relativo alla resilienza operativa digitale per il settore finanziario e che modifica i regolamenti (CE) n. 1060/2009, (UE) n. 648/2012, (UE) n. 600/2014, (UE) n. 909/2014 e (UE) 2016/1011), noto come **Digital Operational Resilience Act (DORA)**, entrato in vigore il 16 gennaio 2023 e applicabile dal 17 gennaio 2025, stabilisce un quadro normativo rigoroso e armonizzato per la gestione dei rischi tecnologici e informatici (ICT) nel settore finanziario europeo.

Abbiamo già parlato di questo regolamento nel precedente numero della rivista ed anche il tema della supply chain è stato da me affrontato nel numero 67 di questa rivista nel 2023.

Nel precedente articolo si è già accennato al fatto che DORA, fra i propri obiettivi di presidio del rischio ICT, ricomprende anche la gestione della catena di fornitura in ambito ICT, ma sono stati approfonditi essenzialmente i vincoli contrattuali che la normativa ha previsto per regolamentare i rapporti fra cliente e fornitore.

In realtà DORA regola l'intero ciclo di vita del rapporto fra una entità finanziaria ed i suoi fornitori ICT ed in particolare stabilisce che le entità finanziarie devono effettuare una serie di azioni specifiche nell'ambito di tali soggetti, soprattutto quando tali servizi supportano funzioni essenziali o importanti, termine con cui nella normativa si intendono (Art. 3.22):

*una funzione la cui interruzione comprometterebbe sostanzialmente i risultati finanziari di un'entità finanziaria o ancora la solidità o la continuità dei suoi servizi e delle sue attività, o la cui esecuzione interrotta, carente o insufficiente comprometterebbe sostanzialmente il costante adempimento, da parte dell'entità finanziaria, delle condizioni e degli obblighi*

*inerenti alla sua autorizzazione o di altri obblighi previsti dalla normativa applicabile in materia di servizi finanziari.*

In tale contesto il principio fondamentale stabilito dal Regolamento (UE) 2022/2554 è che le entità finanziarie che stipulano accordi contrattuali per l'utilizzo di servizi ICT rimangono sempre pienamente responsabili del rispetto di tutti gli obblighi normativi e delle responsabilità nei confronti dei clienti.

La gestione dei rischi informatici derivanti da terzi deve essere una componente integrante del quadro generale per la gestione dei rischi informatici dell'entità finanziaria e in tale contesto, l'applicazione del regolamento DORA è guidata dal principio di proporzionalità. Le entità finanziarie devono tenere conto delle loro dimensioni, del loro profilo di rischio complessivo e della natura, della portata e della complessità dei loro servizi e delle loro operazioni.

I requisiti includono l'obbligo di adottare e riesaminare periodicamente una strategia per i rischi informatici derivanti da terzi.

Tale strategia deve includere una politica specifica per l'utilizzo di servizi ICT che supportano funzioni essenziali o importanti.

Le azioni principali includono una serie di azioni volte a definire:

- la governance ed la strategia per la gestione dei fornitori ICT
- il mantenimento del registro delle informazioni, nel quale sono elencati tutti i fornitori ICT ed i subfornitori rilevanti nell'ambito della gestione dei processi FEI
- la valutazione pre-contrattuale (valutazione del rischio) e la due diligence
- la gestione dei contratti
- il monitoraggio continuo e la gestione del mancato rispetto, ad esempio, degli SLA concordati da parte del fornitore
- la risoluzione del contratto e le strategie di uscita.

Una attenzione particolare viene riservata alla gestione dei subfornitori, che fanno parte anch'essi del presidio della entità finanziaria.

## 2- L'inquadramento normativo

La normativa DORA ha un'architettura molto complessa e comprende:

- il regolamento DORA
- la direttiva DORA
- una serie di regolamenti delegati
- una serie di regolamenti esecutivi
- alcune linee guida.

In particolare, per quanto attiene la gestione della catena di fornitura, la normativa DORA comprende:

- per tutti i fornitori ICT:
  - il regolamento DORA, agli artt. 28, 29, 30
  - il regolamento di esecuzione (UE) 2024/2956, che regola la gestione del registro dei fornitori e subfornitori
- per i fornitori ICT a supporto di funzioni essenziali e importanti, in aggiunta a quanto sopra:
  - il regolamento delegato (UE) 2024/1773 della Commissione, che regola il rapporto con i fornitori
  - il regolamento delegato (UE) 2025/532 della Commissione, che regola il rapporto con i subfornitori.

Complessivamente, il numero di pagine di cui è composto il quadro normativo che regola il rapporto fra entità finanziarie e fornitori, è di oltre 100, a testimonianza del livello di analiticità di questa normativa, che non trova eguali (a mia conoscenza) in altri settori.

È per tale motivo che DORA può costituire una buona pratica per una corretta e completa gestione del rapporto cliente/fornitore in ogni settore.

Inoltre DORA si intreccia con altre normative, emesse da enti regolatori che sovrintendono specifiche entità finanziarie, collettivamente definite **ESA** (European Supervisory Authorities), quali ad esempio le banche (**EBA**).

In particolare sono presenti i seguenti documenti:

- **EBA** (European Banking Authority) - **Orientamenti in materia di esternalizzazione**
- **EIOPA** (European Insurance and Occupational Pensions Authority) - **Orientamenti in materia di esternalizzazione a fornitori di servizi cloud**
- **ESMA** (European Securities and Markets Authority) - **Orientamenti in materia di esternalizzazione a fornitori di servizi cloud.**

La sovrapposizione con DORA è parziale, e questo costringe le entità finanziarie ad una attenta individuazione di quale normativa regola il singolo rapporto.

DORA infatti regola solo il rapporto con i fornitori ICT, mentre ad esempio EBA, nelle sue linee guida, regola le esternalizzazioni di qualunque tipo di fornitura, ma non, ad esempio, una semplice fornitura.

Non vi sono problemi, viceversa, nel caso in cui ci siano sovrapposizioni fra le normative, in quanto DORA è un regolamento europeo, mentre le linee guida delle varie ESA, non hanno un carattere prescrittivo.

Inoltre, la gestione dei fornitori è influenzata anche dalla presenza di altre normative, che possono applicarsi direttamente a questi ultimi, e che possono avere impatti nella regolamentazione del rapporto, agevolando il rispetto dei requisiti contrattuali previsti dalla normativa DORA.

In particolare, molti dei fornitori ICT delle entità finanziarie sono soggetti alla direttiva NIS2 (*Direttiva (UE) 2022/2555 del Parlamento europeo e del Consiglio del 14 dicembre 2022 relativa a misure per un livello comune elevato di cibersecurity nell'Unione, recante modifica del regolamento (UE) n. 910/2014 e della direttiva (UE) 2018/1972 e che abroga la direttiva (UE) 2016/1148 (direttiva NIS 2)*), normativa gemella del regolamento DORA (basti pensare che il regolamento DORA riporta il numero 2022/2554, mentre la direttiva NIS2 il numero 2022/2555), è che può essere considerata una versione semplificata di DORA, ma che richiede analoghi requisiti di sicurezza (DORA viene considerato una *lex specialis* rispetto alla NIS2, e cioè una versione settoriale di quest'ultima, una valutazione che personalmente non

condivido, per la presenza di alcune differenze sostanziali relativamente al perimetro al quale si applicano i requisiti di sicurezza).

Altra normativa di rilievo, già pienamente operativa, è il **Data ACT (REGOLAMENTO (UE) 2023/2854 DEL PARLAMENTO EUROPEO E DEL CONSIGLIO del 13 dicembre 2023 riguardante norme armonizzate sull'accesso equo ai dati e sul loro utilizzo e che modifica il regolamento (UE) 2017/2394 e la direttiva (UE) 2020/1828 (regolamento sui dati)**, che fra le altre cose impone, ai fornitori di un «servizio di trattamento dei dati» (identificabili, ad esempio, con i cloud provider), la portabilità e interoperabilità dei servizi offerti (Capi VI e VIII del Data Act). Se un fornitore è soggetto alla NIS2, sarà obbligato, da questa normativa (Artt.20, 21, 23) della NIS2), ad adottare gli stessi requisiti di sicurezza che l'entità finanziaria può imporre solo contrattualmente. Questo si traduce in una garanzia notevole per l'entità finanziaria che, grazie alla NIS2, ha una leva per imporre le proprie condizioni, molto più rilevante rispetto ad un generico vincolo contrattuale.

Analogamente l'obbligo per i fornitori cloud di garantire la portabilità ed interoperabilità dei servizi offerte, semplifica enormemente per le entità finanziarie la messa a punto di soluzioni di exit strategy e dei relativi exit plan, in quanto sarà il fornitore stesso, per obbligo normativo, a dover garantire questo processo.

Come vedremo più avanti, nell'apposito paragrafo dedicato al punto di vista dei fornitori, queste normative non favoriscono solo le entità finanziarie, ma anche i fornitori possono avvantaggiarsene, sia dal punto di vista economico, sia rafforzando la loro postura di sicurezza.

### **3 - Gestire il ciclo di vita della catena di fornitura**

Analizziamo più dettagliatamente i punti prima citati, riportando l'indicazione di dove il requisito è citato nella normativa, ma precisando che in realtà lo stesso requisito può essere richiamato in più articoli, sia del Regolamento DORA, sia dei regolamenti delegati su fornitori e subfornitori.

Nell'ambito della governance (art. 28.2 del Regolamento DORA) della relazione cliente fornitore l'entità finanziaria deve:

- adottare e riesaminare periodicamente (almeno una volta all'anno) una strategia per i rischi informatici derivanti da terzi, che includa una politica per l'utilizzo dei servizi ICT a supporto di funzioni essenziali o importanti
- definire una metodologia per determinare quali siano i servizi ICT che supportano funzioni essenziali o importanti
- assegnare chiaramente le responsabilità interne per l'approvazione, la gestione, il controllo e la documentazione dei pertinenti accordi contrattuali
- istituire un ruolo per monitorare gli accordi con i fornitori.

Per quanto attiene il registro delle informazioni (art. 28.3 del Regolamento DORA) deve:

- mantenere e aggiornare il registro di tutti gli accordi contrattuali per l'utilizzo di servizi ICT prestati da fornitori terzi, a livello di entità, e su base subconsolidata e consolidata
- documentare gli accordi contrattuali, distinguendo quelli che si riferiscono a servizi ICT a supporto di funzioni essenziali o importanti dagli altri
- comunicare alle autorità competenti, almeno una volta all'anno, il numero di nuovi accordi, le categorie di fornitori terzi di servizi ICT, il tipo di accordi contrattuali e le funzioni e i servizi ICT forniti
- informare tempestivamente l'autorità competente in merito a eventuali accordi contrattuali previsti per l'utilizzo di servizi ICT a supporto di funzioni essenziali o importanti e quando una funzione diventa essenziale o importante
- assicurare che le informazioni contenute nel registro siano accurate e coerenti.

Per quanto attiene la valutazione pre-contrattuale e la due diligence (artt. 28.4 ,29 del Regolamento DORA) deve:

- definire le esigenze aziendali prima della conclusione di un accordo contrattuale
- effettuare una valutazione dei rischi prima della conclusione di un accordo contrattuale, considerando i rischi operativi, giuridici, informatici, reputazionali, i rischi legati alla protezione dei dati e alla disponibilità dei dati e i rischi di concentrazione a livello di entità
- verificare se sono soddisfatte le condizioni di vigilanza per la conclusione del contratto
- definire un processo adeguato e proporzionato per la selezione e la valutazione dei potenziali fornitori terzi di servizi ICT, assicurandone l'idoneità. Ciò include la valutazione della loro reputazione commerciale, risorse (finanziarie, umane, tecniche), standard di sicurezza delle informazioni e struttura organizzativa
- valutare se il fornitore ricorre o intende ricorrere a subappaltatori ICT per funzioni essenziali o importanti
- considerare i rischi legati alla località del fornitore/società madre e del luogo di trattamento o conservazione dei dati, specialmente in un paese terzo
- valutare se il fornitore terzo di servizi ICT aderisce ad accordi che garantiscano il diritto dell'entità, di terze parti designate e delle autorità competenti di effettuare audit/ispezioni (anche in loco).

Per quanto attiene il monitoraggio continuo (art. 9 del Regolamento 2024/1773) e la gestione delle inadempienze deve:

- monitorare in modo continuativo le prestazioni dei fornitori terzi di servizi ICT, verificando il rispetto dei requisiti di riservatezza, disponibilità, integrità e autenticità dei dati
- valutare le prestazioni dei fornitori tramite indicatori chiave di prestazione, indicatori chiave di controllo, audit, autocertificazioni e revisioni indipendenti
- assicurare che i servizi ICT essenziali o importanti siano soggetti a un riesame indipendente e siano inclusi nel piano di audit

- non fare esclusivo affidamento sulle certificazioni di terze parti o sulle relazioni di audit interne dei fornitori
- stabilire le opportune misure da adottare se si individuano carenze dei fornitori terzi di servizi ICT (compresi gli incidenti) e monitorare l'attuazione di tali misure entro un periodo di tempo definito
- richiedere ai fornitori la notifica degli incidenti ICT e degli incidenti operativi o di sicurezza dei pagamenti che possono avere un impatto sull'entità finanziaria.

Per quanto attiene la risoluzione del contratto (art. 28.8 del Regolamento DORA) e la gestione delle strategie di uscita deve:

- predisporre strategie di uscita per i servizi ICT a supporto di funzioni essenziali o importanti
- identificare soluzioni alternative ed elaborare piani di transizione per trasferire i servizi ICT e i relativi dati a fornitori alternativi o per reintegrarli internamente in modo sicuro e completo
- testare i piani di continuità operativa dei sistemi informativi, includendo scenari che simulano potenziali perturbazioni, e che comprendano il test dei servizi ICT forniti da fornitori terzi di servizi ICT
- nei test, prendere in debita considerazione gli scenari legati all'insolvenza o a disfunzioni dei fornitori terzi di servizi ICT
- disporre di misure di emergenza idonee per mantenere la continuità operativa in caso di disfunzioni dei fornitori terzi di servizi ICT a supporto di funzioni essenziali o importanti.

Alla gestione del contratto è dedicato il successivo paragrafo.

#### **4 – Formalizzare il contratto**

Le entità finanziarie sono tenute a introdurre una serie di requisiti essenziali nei contratti stipulati con i fornitori ICT. Tali condizioni sono dettate principalmente dall'articolo 30 del Regolamento 2022/2554 e da alcuni articoli dei regolamenti delegati che disciplinano il rapporto con i fornitori e con i subfornitori.

Rispetto a quest'ultimo, è importante sottolineare con lo stesso sia stato pubblicato circa 6 mesi dopo la piena efficacia del regolamento, una grave mancanza da parte del legislatore, che non ha consentito alle entità finanziarie di adeguare nei tempi utili a rispettare i requisiti normativi, i contratti che regolano i loro rapporti con i fornitori ICT.

Innanzitutto, gli accordi contrattuali devono essere redatti in forma scritta e questo adempimento è in carico sia all'entità finanziaria, sia al fornitore (unico obbligo normativo di DORA per un fornitore ICT).

Inoltre, accanto alle clausole esplicitamente previste e imposte dalla normativa, l'entità finanziaria ha l'obbligo di inserire un'ulteriore serie di disposizioni, che si possono desumere solo indirettamente dal testo, e derivanti dagli obblighi in capo alle entità finanziarie. L'introduzione di queste clausole supplementari è cruciale, poiché in loro assenza l'entità finanziaria non sarebbe in grado di garantire il rispetto della normativa.

Un esempio di come gli obblighi si estendano a tali requisiti che definiremo impliciti, è dato dalla cifratura dei dati; se l'entità finanziaria ha l'obbligo di cifrare i propri dati e una porzione di tali dati viene gestita da un fornitore ICT, è indispensabile che anche il fornitore ICT provveda alla cifratura di tali dati.

Complessivamente, il numero di clausole che derivano, in modo esplicito o implicito, dal Regolamento 2022/2554 e dalle norme che lo integrano, sono diverse decine.

Per quanto attiene le clausole contrattuali esplicite, inoltre, queste sono molto diverse fra di loro e comprendono:

- prescrizioni molto puntuali, quali l'indicazione delle località in cui si devono svolgere le funzioni e trattare i dati, con obbligo per il fornitore di segnalare in anticipo l'intenzione di cambiare tali località
- prescrizioni assolutamente generiche, come l'indicazione delle disposizioni in materia di sicurezza dei dati (disponibilità, autenticità, integrità e riservatezza).

Il secondo tipo di clausola, ad esempio, si presta ad ampia interpretazione e in realtà potrebbe contenere numerose delle clausole implicite, come quella sopra citata relativa alla cifratura.

La normativa, inoltre, indica quali siano gli aspetti che devono essere regolati dal rapporto contrattuale, ma non entra nel merito del come e nemmeno di quanto tali azioni possano costare in termini monetari.

Questi aspetti sono elemento di trattativa nel rapporto fra cliente e fornitore.

Per tale motivo, sebbene le entità finanziarie nel loro processo di adeguamento stiano puntando su contratti il più possibile standardizzati, sarebbe in realtà opportuna una maggiore personalizzazione degli stessi.

Il rischio concreto per le entità finanziarie è di chiedere a tutte i fornitori di applicare, ad esempio, gli stessi presidi di sicurezza.

Questo potrebbe tradursi in richieste assolutamente inutili per alcuni fornitori; si pensi ad esempio ad un fornitore ICT che si limiti a vendere delle licenze software che l'entità finanziaria installa presso il proprio data center (uno dei servizi ICT espressamente previsti dal regolamento), quali presidi di sicurezza dovrebbe avere?

Sicuramente non quelli che è possibile richiedere a chi invece eroga in modalità SAAS lo stesso software.

Oltre ad un aggravio di costo diretto, per l'entità finanziaria una richiesta di requisiti di sicurezza inutili, si traduce anche in un successivo gravoso impegno in termini di monitoraggio ed audit.

## 5 - il punto di vista del fornitore

Come accennato nei paragrafi precedenti, la presenza di una normativa come la NIS2 alla quale devono sottostare molti dei fornitori ICT, non costituisce solo un vantaggio per le entità finanziari.

Questo a causa dell'esistenza di un delta temporale fra la piena efficacia di DORA (gennaio 2025) ed il momento in cui un'organizzazione soggetta alla NIS2 dovrà implementare i requisiti di sicurezza previsti da quest'ultima (Ottobre 2026).

Quindi un fornitore ICT soggetti alla NIS2, può implementare i requisiti di sicurezza previsti da DORA che gli sono imposti da una entità finanziaria, girando a quest'ultima i costi, e trovandosi in tal modo già conforme alla NIS2.

Ma non sono solo questi i vantaggi per i fornitori derivanti dalla introduzione di queste normative; l'implementazione dei requisiti normativi per rispondere alle richieste delle entità finanziarie è, come evidenziato nel paragrafo precedente, una opportunità commerciale in quanto tale attività non è gratuita.

È inoltre possibile offrire nuovi servizi, come la gestione della segnalazione degli incidenti, oppure offrirsi come fornitore alternativo nell'ambito dello sviluppo, da parte delle entità finanziarie, dei piani di uscita verso altri fornitori, permettendo così anche l'esecuzione dei test degli stessi, come previsto dalla normativa.

Per i fornitori non soggetti alla NIS2, aderire alle richieste contrattuali delle entità finanziarie consente di aumentare la sicurezza dei propri servizi anche nei confronti degli altri clienti, sfruttando il contributo economico delle entità finanziarie.

## 6 – Conclusioni

Il quadro normativo introdotto dal Regolamento DORA e dalle normative ad esso collegate offre una guida molto pratica per la gestione dell'intero ciclo di vita dei fornitori, indipendentemente dalla loro tipologia e dal settore di appartenenza.

Inoltre, rispetto ad altri strumenti o normative di alto livello, che si limitano ad affermazioni di principio, in questo regolamento vengono fornite indicazioni pratiche e precise, che consentono un reale presidio sulla catena di fornitura.

## 7 - Bibliografia

- [1] Aamir Jamil, "DORA and NIS2: Connection Points and Key Differences", ISACA, 2025
- [2] "Digital Operational Resilience Act (DORA)", EIOPA, 2025
- [3] "Adeguamento della normativa nazionale alle disposizioni del regolamento (UE) 2022/2554 relativo alla resilienza operativa digitale per il settore finanziario", Senato della Repubblica, 2025
- [4] Butti, G., "Manuale di resilienza", ITER, 2023
- [5] Butti, G., "Supply chain: gestire i rischi con strumenti di IA gratuita", ITER, 2025
- [6] Butti, G., "Resilienza operativa digitale: Regolamento 2022/2554 (DORA)", La Comunicazione - Note, Recensioni e Notizie n. 69 - Anno 2025
- [7] "Data Act explained", Commissione Europea, 2025
- [8] "European Supervisory Authorities designate critical ICT third-party providers under the Digital Operational Resilience Act", EIOPA, 2025

## **Studio sperimentale e numerico della perdita di penetrazione veicolare in scenari V2X**

### ***Experimental and numerical study of vehicle penetration loss in V2X scenarios***

Marina Lotti<sup>♦</sup>, Andrea Garzia<sup>♦</sup>, Claudia Carciofi<sup>♦</sup>, Simona Valbonesi<sup>♦</sup>

♦ Fondazione Ugo Bordoni – Roma - Italy

#### **Sommario**

Una valutazione corretta e rigorosa delle perdite del segnale radio all'interno delle auto, in inglese *Car Penetration Loss* (CPL), e dei mezzi di trasporto in generale, è un fattore rilevante nell'ambito degli studi riguardanti la propagazione radio e la copertura delle reti 5G e 6G, in particolare per quanto riguarda gli scenari di comunicazioni mobili avanzate nel settore automotive, incluse le applicazioni *vehicle-to-vehicle* (V2V) e soprattutto *vehicle-to-everything* (V2X).

Questo articolo presenta i risultati di una nuova campagna sperimentale multifrequenza nelle bande 4G e 5G nel range 700 – 3800 MHz finalizzata allo studio del comportamento del segnale radio all'interno di una vettura ed alla valutazione delle perdite di penetrazione dovute all'auto. Tale campagna sperimentale integra analoghe misurazioni eseguite in prossimità di un diverso sito radiomobile caratterizzato da un diverso ambiente di propagazione e da diverse configurazioni di misura.

Lo studio esamina come il comportamento del segnale misurato all'interno dell'auto sia influenzato da una serie di variabili rilevanti come, l'orientamento della vettura rispetto alla direzione di provenienza del segnale radio, la posizione del dispositivo ricevente che si trova a bordo e le caratteristiche dei vetri dell'auto. Inoltre, viene presentata una valutazione simulativa del segnale radio effettuata con tecniche di ray-tracing 3D finalizzata allo studio ed alla caratterizzazione delle perturbazioni del campo elettromagnetico causate da un veicolo.

## **Abstract**

A proper and rigorous assessment of Car Penetration Loss (CPL) is a crucial factor for propagation and coverage prediction of 5G and 6G networks, especially for automotive mobile advanced communications scenarios, V2V and V2X included. This paper presents a novel multi-frequency measurement campaign of in-car penetration loss in the frequency range 700–3800 MHz, which complements previous experimental measurements performed in a different environment and for different scenarios. The study examines how signal behaviour is influenced by a set of relevant variables, including frequency, vehicle orientation relative to the signal, the on-board device's position, and characteristics of the car glazing. Additionally, a preliminary analysis using 3D ray-tracing techniques is proposed to investigate the electromagnetic field perturbations caused by a vehicle.

## **Keyword**

*Automotive, CPL, measurements, Penetration Loss, ray-tracing, simulations, V2X, 5G, 6G*

## **1 - Introduzione**

La comprensione delle modalità di propagazione del segnale radio all'interno dei veicoli è diventata rilevante dal momento che le auto ospitano un numero sempre crescente di dispositivi connessi, che vanno dai sistemi di infotainment, agli smartphone, fino ad arrivare alle unità avanzate di assistenza alla guida autonoma. Inoltre, la caratterizzazione del canale radio all'interno ed in prossimità dei veicoli è fondamentale per la sicurezza e l'affidabilità delle comunicazioni V2X e per ottimizzare l'integrazione del 5G-NR nel settore automotive.

Questo articolo affronta la necessità di identificare tramite diverse tipologie di campagne sperimentali una metodologia affidabile per il calcolo delle perdite di penetrazione in-car, un parametro chiave per garantire la copertura e la potenza di segnale richiesta dai dispositivi connessi e dai sistemi di guida autonoma.

Studi scientifici condotti in ambito CEPT [1], ITU [2] e 3GPP [3] hanno dimostrato che le perdite di penetrazione all'interno della carrozzeria delle auto dipendono da molteplici parametri

(materiali, geometrie, direzioni del segnale). Tuttavia, manca ancora una metodologia generale e scalabile per il calcolo delle perdite di penetrazione in-car, e la letteratura disponibile è limitata; tutto ciò rende urgente l'indagine scientifica su questa tematica.

L'articolo presenta i risultati di uno studio scientifico che combina misurazioni e simulazioni finalizzate a stabilire un approccio coerente alla definizione di valori di CPL da applicare in diversi scenari attuali e futuri.

La nuova campagna di misurazione CPL (che integra e completa altri test sul campo effettuati in precedenza) è stata condotta nell'intervallo di frequenza 700–3800 MHz utilizzando un analizzatore di spettro, per raccogliere dati in diverse posizioni all'interno dell'abitacolo e con diversi orientamenti dell'auto rispetto alla Stazione Base (BS).

I risultati sperimentali sono stati confrontati con i valori di riferimento specificati nel documento 3GPP ETSI TR38.901 [3] per identificare eventuali deviazioni tra il modello standardizzato ed i contesti operativi reali.

Sono state eseguite anche simulazioni con tecniche di 3D ray-tracing nell'intervallo 700 MHz–3800 MHz, e nelle bande 6 GHz e 26 GHz. Tali simulazioni sono state effettuate al fine di identificare i meccanismi di propagazione all'interno dell'abitacolo (multi-cammino, riflessioni, diffrazioni, schermature), di fornire un metodo di calcolo simulativo rigoroso della CPL da confrontare con le misure e di caratterizzare la propagazione nelle immediate vicinanze del veicolo ("Near-Car"), elemento ritenuto fondamentale per le comunicazioni V2V e V2X.

Come già anticipato, in letteratura è disponibile un numero limitato di lavori specifici: alcuni esempi si possono trovare in [5], dove la CPL è stata misurata nell'intervallo di frequenza 600 MHz–2400 MHz con valori medi ottenuti che variano da 3.2 dB a 23.8 dB. Un altro studio [6] focalizzato sulle frequenze fino a 6 GHz ed effettuato impiegando una berlina di ultima generazione, ha fornito come risultati un valore medio di CPL di 3 dB in caso di vetri senza rivestimento, 6.6 dB in caso di finestrini con pellicola e 20.7 dB in caso di finestrini ricoperti con pellicola metallica in alluminio. Infine, uno studio condotto da OFCOM/LSTelcom relativo al range frequenziale 800-2600 MHz e che ha coinvolto diversi modelli di auto [7], ha ottenuto risultati comparabili a quelli ottenuti con le indagini che costituiscono il focus di questo

articolo. Preliminarmente all'analisi oggetto del lavoro qui presentato erano stati effettuati, da parte della Fondazione Ugo Bordoni, studi sia di tipo compilativo, sia basati su campagna di misura e simulazioni numeriche [4], [8], [9], che hanno messo in evidenza l'elevata complessità degli scenari in-car ed in-train. Le misurazioni effettuate per lo scenario in-car nella banda 700 – 3700 MHz hanno evidenziato valori medi della CPL compresi tra 2 e 6 dB con massimo attorno ai 13 dB [2], [3], in linea con quanto pubblicato in letteratura.

## 2 – Descrizione della nuova campagna di misure e risultati ottenuti

La catena strumentale utilizzata per la campagna di misura è costituita da un analizzatore di spettro portatile (Narda SRM-3006) [10] in grado di misurare selettivamente il campo elettrico sia all'interno sia all'esterno del veicolo.

Come sorgente di segnale radio è stata scelta una stazione base operativa sul territorio del Comune di Bologna a Casteldebole, in un contesto di periferia urbana.

Le misurazioni sono state eseguite in modalità Channel Power inizialmente in assenza di veicolo, al fine di ottenere una base di riferimento, poi considerando tre diversi orientamenti del veicolo rispetto alla stazione base (frontale, retro e laterale), come mostrato in Figura 1.



*Figura 1 – Orientamenti del veicolo rispetto alla stazione base*

All'interno della vettura sono state considerate cinque diverse posizioni (Figura 2):

- Sedile anteriore sinistro e destro (S1, S2)
- Sedile posteriore sinistro e destro (S3, S4)
- Pianale del veicolo (solo per S1, limitato alla configurazione frontale)
- Bagagliaio (R)

Per ciascuna frequenza e ciascun canale sono stati acquisiti più di 1000 spettri (istantanee temporali dell'evoluzione dello spettro); la CPL è stata stimata calcolando la differenza tra il campo elettrico misurato all'esterno del veicolo e quello misurato al suo interno.

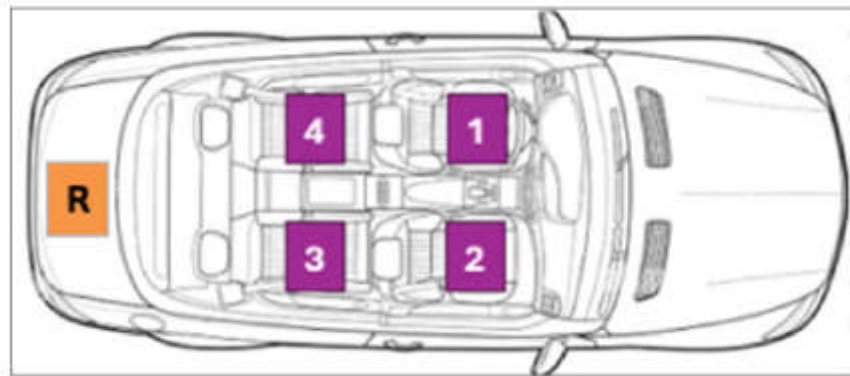


Figura 2 – Posizioni interne all'auto selezionate per la misura

La CPL, infatti, è definita come rapporto tra due valori:

$$CPL(f) = 20 \log_{10} \left( \frac{|E_{out}(f)|}{|E_{in}(f)|} \right) \quad (1)$$

dove  $E_{out}(f)$  ed  $E_{in}(f)$  sono il campo elettrico misurato per la frequenza  $f$  all'esterno ed all'interno dell'auto rispettivamente. Questo calcolo viene eseguito per ciascun canale che presenta un segnale non trascurabile all'interno della larghezza di banda considerata. Attraverso una analisi sui singoli canali di frequenza è possibile caratterizzare le perdite di penetrazione su tutta la banda oggetto di studio.

## 2.1 - Analisi dei risultati: indagine sulla frequenza

Per questo studio il veicolo è stato trattato come una entità unica, aggregando i risultati (Tabella 1) senza distinguere tra le singole posizioni dei passeggeri (Sedili 1 – 4, Figura 2). La tabella presenta i valori medi misurati (con la relativa deviazione standard) ed i valori massimi. I dati delle misure ottenuti con l'analizzatore di spettro sono stati combinati

indipendentemente dai tre orientamenti del veicolo rispetto alla Stazione Base (BS). Sono stati esclusi dall'analisi posizioni non standard come l'interno del bagagliaio e la zona sotto i sedili. In alcuni scenari, i valori di CPL calcolati sono risultati negativi, probabilmente a causa della natura riflettente della carrozzeria metallica dell'auto.

**Tabella 1.** Valori massimi e medi della CPL al variare della frequenza

<b>Frequenza (MHz)</b>	<b>CPL<sub>medio</sub> +/- dev std (dB)</b>	<b>CPL<sub>max</sub> (dB)</b>
700	3.22 ± 2.8	9.1
800	2.88 ± 1.8	5.72
900	1.81 ± 3.6	8.61
1800	4.97 ± 2.6	13.9
2100	4.82 ± 3.4	11.49
2600	2.64 ± 3.4	9.6
3700	4.98 ± 5	16.6

Le riflessioni multiple e lo scattering all'interno della struttura del veicolo possono infatti causare una sovrapposizione costruttiva del segnale, creando un guadagno apparente anziché l'attesa attenuazione [5].

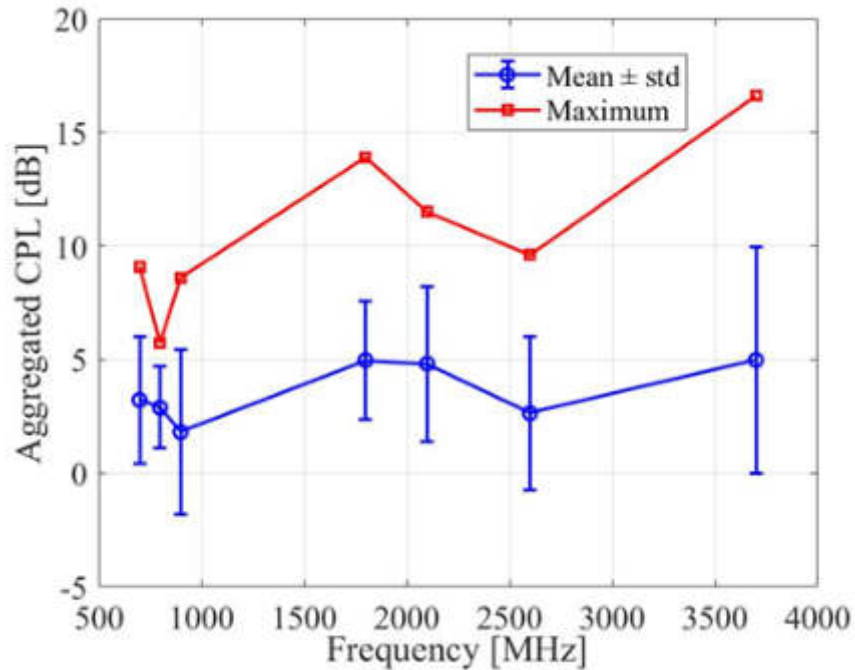
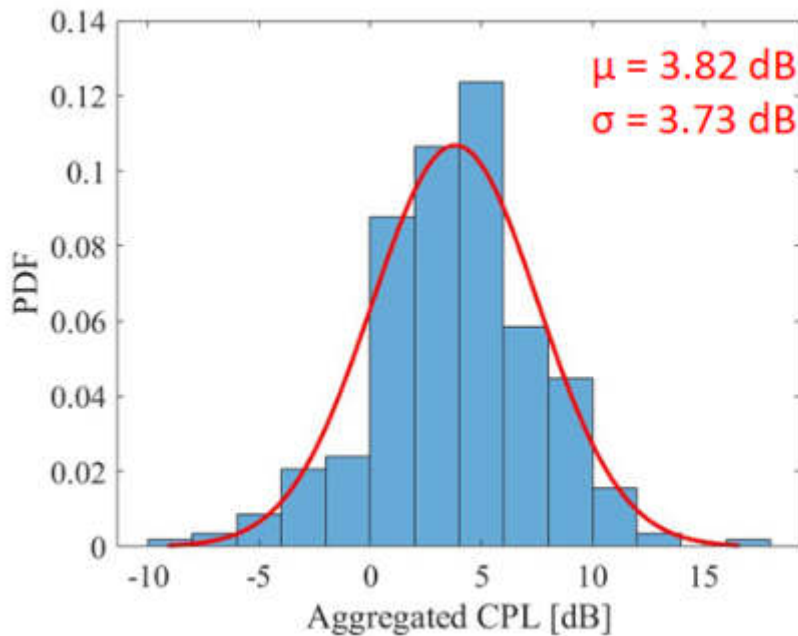


Figura 3 – Analisi in frequenza della CPL

In Figura 3 sono riportati i valori medi (con relative deviazioni standard) e massimi della CPL in funzione della frequenza; il dato è relativo alle posizioni standard interne all'abitacolo (sedili S1-S4). L'analisi visiva degli andamenti conferma che non è possibile definire una chiara relazione (lineare o esponenziale) tra CPL e frequenza; questa conclusione è supportata da analisi statistiche basate sul parametro  $R^2$  per il modello lineare e pseudo  $R^2$  per il modello non lineare. Il parametro  $R^2$  confronta la varianza del modello applicato con la varianza dei dati ed è un numero compreso tra 0 e 1. Più il valore è vicino a 1, migliore sarà l'aderenza dei dati al modello selezionato; nel caso specifico, il valore di  $R^2$  più alto riscontrato è pari a 0.37 a confermare l'assenza di relazioni a legare la CPL media alla frequenza nell'intervallo oggetto di indagine. L'andamento del valore massimo della CPL mostra una tendenza crescente all'aumentare della frequenza.



*Figura 4 – Distribuzione della CPL totale*

Successivamente, è stato condotto uno studio statistico sulla distribuzione dei dati di misura considerando le posizioni S1-S4 ed aggregando i valori ottenuti per tutte le frequenze. Da questa analisi, i cui risultati sono riportati in Figura 4, emerge che la CPL segue una distribuzione Gaussiana per la quale sono stati calcolati la media ( $\mu$ ), la deviazione standard ( $\sigma$ ) ed i rispettivi intervalli di confidenza al 95%. La densità di probabilità per una distribuzione gaussiana è data da:

$$f(x) = \frac{1}{\sigma\sqrt{2\pi}} \exp\left[-\frac{(x-\mu)^2}{2\sigma^2}\right] \quad (2)$$

Sulla base dei valori di CPL ottenuti tramite misurazioni all'interno dell'abitacolo, i parametri ottenuti sono  $\mu = 3.82 \text{ dB}$  con un intervallo di confidenza del 95% di  $[3.39 - 4.25] \text{ dB}$  e  $\sigma = 3.73 \text{ dB}$  con un intervallo di confidenza del 95% di  $[3.45 - 4.06] \text{ dB}$ . L'elevata deviazione standard conferma la già segnalata variabilità dei dati misurati.

## 2.2 – Variazioni della CPL in funzione dell'orientamento della vettura

L'obiettivo di questo studio consiste nel verificare l'effetto dell'orientamento dell'auto sui valori della CPL. L'analisi è stata condotta considerando l'auto come entità unica (senza distinguere le posizioni al suo interno) e aggregando tutti i dati di frequenza; questo è stato possibile dal momento che non è emersa alcuna relazione specifica tra frequenza e CPL nella banda oggetto di indagine.

Tabella 2. CPL media e massima per diversi orientamenti

Posizione	Angolo $\vartheta$	CPL <sub>media</sub> (dB)	CPL <sub>max</sub> (dB)
Frontale	0°	3.02 ± 4.0	16.6
Retro	180°	3.80 ± 2.6	11.4
Laterale	90°	4.60 ± 3.7	13.9

Come evidente da Tabella 2, la CPL media più bassa (3.02 dB) si ottiene nella posizione frontale, suggerendo che il segnale radio penetra agevolmente attraverso il parabrezza e le riflessioni generate dal cofano creano uno scenario multi-cammino con fenomeni di somma costruttiva che tendono ad abbassare i valori di CPL. Questo complesso fenomeno verrà trattato in dettaglio nella Sezione 4.

### 2.3 – Variabilità della CPL per diverse posizioni all'interno della vettura

La tabella 3 mostra i valori medi e massimi di CPL calcolati per diverse posizioni all'interno del veicolo, includendo il bagagliaio e il pavimento dell'auto (come indicato nelle specifiche di Figura 2).

**Tabella 3.** CPL media e massima per differenti posizioni all'interno dell'abitacolo

Posizione	Frontale	Laterale	Retro
S1 - Media	2.16 ± 4.8	5.4 ± 2.9	4.02 ± 2.9
S1 - Max	12 ± 4.8	11.1 ± 2.9	8.99 ± 2.9
S2 – Media	2.33 ± 4.3	4.72 ± 3.2	4.46 ± 2.7
S2 – Max	10.2 ± 4.3	11.3 ± 3.2	11.4 ± 2.7
S3– Media	3.49 ± 3.5	3.29 ± 4.9	3.27 ± 2.1
S3 – Max	11.7 ± 3.5	13.9 ± 4.9	7.3 ± 2.1
S4 – Media	4.12 ± 4.9	5.22 ± 3.7	3.48 ± 2.7
S4 – Max	16.6 ± 4.9	11.5 ± 3.7	8.6 ± 2.7
Bagagliaio – Media	6.71 ± 4.5	0.26 ± 4.7	3.8 ± 4.6
Bagagliaio - Max	15.7 ± 4.5	7.9 ± 4.7	13.1 ± 4.6
Pavimento – Media	3.39 ± 4.8	-	-
Pavimento – Max	13.8 ± 4.8	-	-

Dal momento che le analisi riportate nella Sezione 2.1 hanno evidenziato la non variabilità della CPL rispetto alla frequenza, l'analisi statistica è stata eseguita aggregando tutte le frequenze e focalizzandosi solo sull'orientamento dell'auto rispetto alla BS e sulla posizione del ricevitore al suo interno.

Dalla analisi dei dati di Tabella 3 sono emerse le seguenti considerazioni:

- **Sedili posteriori:** posizionare lo User Equipment (UE) sui sedili posteriori aumenta la CPL media di 1.32 - 1.97 dB. L'effetto è massimo quando l'auto si trova in una posizione frontale rispetto alla stazione base trasmittente. I valori massimi di CPL subiscono un aumento maggiore, variabile da 2.9 a 6.4 dB.
- **Bagagliaio:** la posizione dello UE nel bagagliaio causa un incremento della CPL media che varia da 0.26 dB (per orientamento laterale) a 6.71 dB (per orientamento frontale).
- **Pavimento dell'Auto:** La misurazione singola effettuata sul pavimento dell'auto in prossimità del sedile anteriore sinistro (auto frontale) non ha mostrato variazioni significative di CPL rispetto al posizionamento dello UE sui sedili. Tuttavia, la limitatezza dei dati impedisce di trarre conclusioni generali senza ulteriori analisi.

#### **2.4 - Effetto della composizione dei vetri sulla CPL**

Il veicolo utilizzato per la campagna di misure presenta due tipologie di vetratura: i finestrini anteriori (posizione S1 ed S2) sono realizzati in vetro ordinario mentre quelli posteriori (posizioni S3 ed S4) sono in vetro oscurato contenente una minima percentuale di materiale metallico. Ciò ha permesso un confronto di massima sull'impatto dei due tipi di vetro sulla CPL, limitato alla posizione laterale dove il segnale incide direttamente sui finestrini. I risultati delle analisi hanno mostrato che l'utilizzo di vetri oscurati aumenta la CPL media di 0.24 - 0.94 dB, con effetto più marcato a 2600 MHz (0.94 dB) e nella banda 3.4-3.8 GHz (0.64 dB). Questo dato è in linea con i risultati delle precedenti analisi [4].

Si prevede, anche sulla base di riscontri in letteratura [11], che aumenti maggiori possano verificarsi in caso di vetri completamente metallizzati. Tuttavia, non è stato possibile indagare questo aspetto a causa dell'indisponibilità di un veicolo idoneo.

## **2.5 – Confronto tra dato misurato e modello teorico**

La CPL a valore singolo è una metrica statistica usata per rappresentare in un unico numero l'attenuazione complessiva del segnale all'interno di un veicolo, semplificando un fenomeno altamente variabile; tale variabilità è stata registrata nella prima campagna di misura [4], [8], [9] e confermata ulteriormente dalle indagini oggetto di questo articolo.

Sebbene la definizione di un singolo valore di CPL sia complessa a causa di variabili come l'orientamento del veicolo rispetto alla direzione del segnale radio, la posizione del ricevitore e la composizione dei finestrini, l'uso di tale metrica è giustificato dalla assenza di una relazione tra CPL e frequenza nel range oggetto di studio.

I risultati della presente campagna di misurazione confermano la variabilità della CPL (supportata dalle elevate deviazioni standard) i cui valori variano da 1.81 a 4.98 dB, in linea con studi precedenti [4].

Ai fini del confronto tra dato misurato e dato teorico, i valori medi e le deviazioni standard ottenuti sono stati confrontati con i valori medi ( $\mu$ ) e le deviazioni standard ( $\sigma$ ) del modello CPL O2I standardizzato dal 3GPP nel Report Tecnico 3GPP TR38.901 [3] e valido nel range di frequenza 0.6 – 60 GHz.

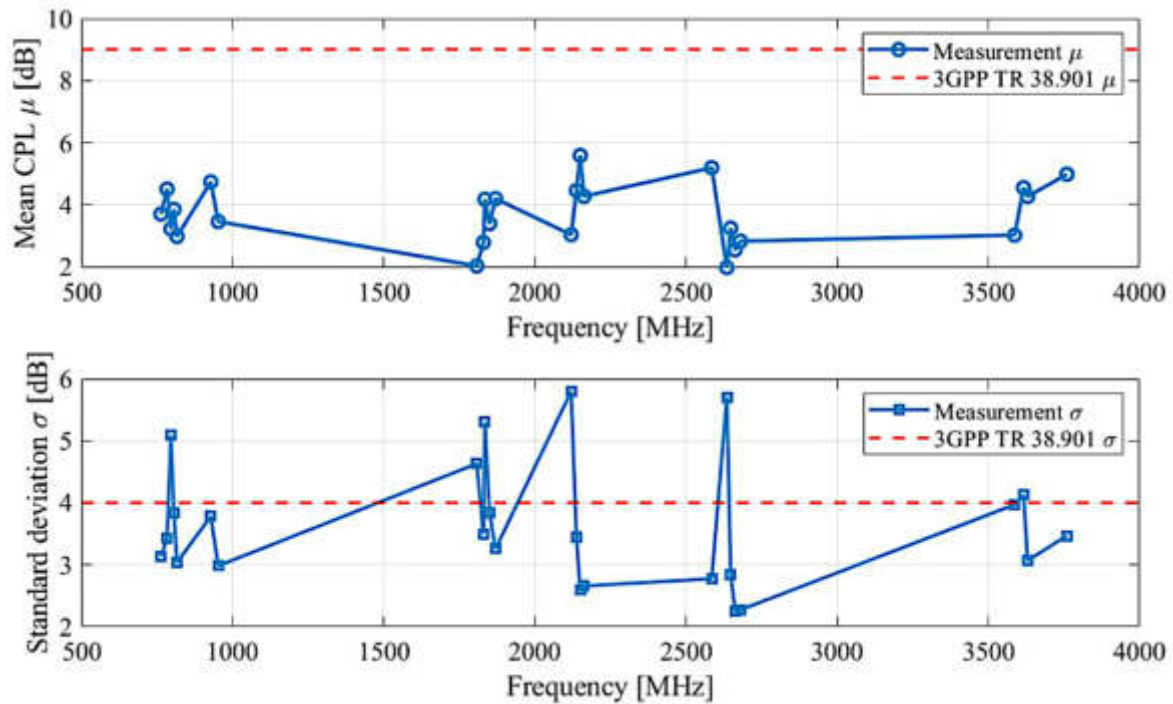


Figura 5 - Confronto con modello 3GPP38.901 – dati aggregati

È opportuno notare che anche il 3GPP [3] fornisce un valore unico di CPL inteso come media ( $\mu$ ) con la relativa deviazione standard ( $\sigma$ ). Di seguito viene riportata una breve descrizione, non esaustiva, del modello [3] riguardante i contesti in-car.

In [3] la perdita di cammino che incorpora la perdita di penetrazione O2I di un veicolo è modellata come segue:

$$PL = PL_b + N(\mu, \sigma_p^2) \quad (3)$$

Dove  $PL_b$  sono le perdite di cammino in ambiente outdoor,  $\mu = 9$  e  $\sigma_p = 5$ ; per le macchine con finestrini in vetro metallizzato viene posto  $\mu = 20$ . I due parametri  $\mu$  e  $\sigma$  rappresentano la CPL e la relativa deviazione standard.

L'esito del confronto tra la CPL media misurata e la relativa deviazione standard e i valori di  $\mu$  e  $\sigma$  riferibili al modello [3] è mostrato in Figura 5 dove sono state considerate tutte le posizioni analizzate, bagagliaio incluso.

Dalla analisi di Figura 5 emerge che la CPL media misurata è inferiore al valore di riferimento indicato da 3GPP (pari a 9 dB) [3], mentre la deviazione standard è comparabile.

Questa discrepanza nella media potrebbe essere attribuibile a diversi fattori:

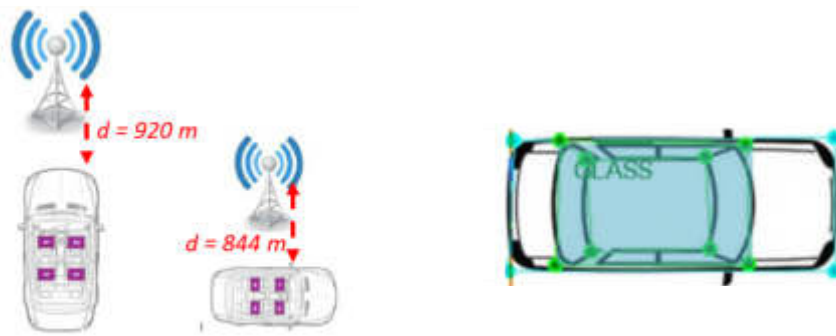
1. **Condizioni ambientali e materiali:** Le condizioni ambientali durante la campagna di misura potrebbero essere state più favorevoli rispetto a quelle assunte da 3GPP [3]. Ad esempio, la presenza di vetri meno attenuanti o finestrini più ampi, o l'effetto di riflessioni esterne (come quelle provenienti dal terreno, non incluse nel modello) potrebbero avere giocato un ruolo fondamentale.
2. **Somma costruttiva:** In un ambiente reale le riflessioni multiple all'interno del veicolo possono creare fenomeni di somma costruttiva, aumentando l'intensità del campo interno al veicolo e riducendo così la perdita di penetrazione apparente.
3. **Range di frequenza:** Il range di frequenza considerato nella campagna di misura (700 – 3800 MHz) potrebbe comportare un'attenuazione media inferiore rispetto al range più esteso considerato nel Technical Report TR38.901 [3].

La deviazione standard, comparabile con quella indicata in [3], conferma invece l'elevata e prevista variabilità del segnale causata dagli effetti multipath e dalla complessa geometria del veicolo.

### 3 - Simulazioni numeriche

Le simulazioni numeriche sono state condotte, al fine di un confronto con i dati misurati, su due scenari distinti illustrati in Figura 6-a:

- Scenario 1 – vettura posizionata frontalmente rispetto alla direzione del segnale
- Scenario 2 – vettura posizionata lateralmente rispetto alla direzione del segnale radio



a) Scenari e distanze

b) Modello per la vettura

Figura 6 – Scenari simulati e modellizzazione della vettura

### 3.1 – Tool di simulazione e parametri

Data la complessità intrinseca che caratterizza la creazione del modello di una automobile, per non complicare ulteriormente lo scenario si è deciso di ricorrere ad un ambiente semplificato dal punto di vista della geometria che include unicamente il veicolo e la Stazione Radio Base. Si è quindi assunto che il ricevitore sia posto all'interno della macchina e che non siano presenti altri ostacoli tra la BS trasmittente (Tx) ed il ricevitore (Rx).

Il modello veicolare (Figura 6-b) consiste in un telaio metallico con finestrini in vetro ordinario e il tettuccio metallico; risultano quindi tre microambienti distinti al fine della propagazione del segnale radio:

1. Parte inferiore dell'abitacolo, dal pavimento dell'auto fino ai finestrini, caratterizzata dalla presenza predominante di materiale metallico che blocca completamente o parzialmente l'ingresso del segnale radio ma non le riflessioni di quest'ultimo all'interno;
2. Area dei finestrini – zona vetrata che permette una facile penetrazione del segnale;
3. Bagagliaio dell'auto – costituisce un ambiente separato e distinto.

Nel modello non sono stati considerati gli interni dell'auto (sedili inclusi), tipicamente costituiti in plastica o pelle.

Le simulazioni numeriche, destinate al confronto con i dati misurati, sono state eseguite con il tool proprietario ARMONICA [12] (sviluppato dalla Fondazione Ugo Bordoni in collaborazione con l'Università di Bologna) basato su tecniche di ray-tracing 3D che tengono conto dei fenomeni di assorbimento, riflessione e diffrazione [13].

Sono state eseguite due simulazioni distinte per ciascuna posizione di ricezione:

- Simulazione ad alta risoluzione (dimensioni del pixel  $0.01 \times 0.01 \text{ m}^2$ ) dei livelli di campo  $E$  nell'area evidenziata in blu di Figura 6-b effettuata con l'obiettivo di ottenere valori di CPL interni all'abitacolo da utilizzare negli studi di compatibilità, condivisione, copertura, impatto ambientale e comunicazione V2X.
- Simulazione dell'intero veicolo all'interno di uno scenario più ampio (scenario Near-Car) finalizzata a visualizzare gli effetti della presenza del veicolo sulla propagazione del segnale radio outdoor. Questa analisi, al momento solo preliminare, è destinata ad applicazioni Vehicle-to-Vehicle e soprattutto Vehicle-to-Everything.

I parametri utilizzati per le simulazioni numeriche sono riepilogati in Tabella 4.

**Tabella 4.** Parametri per simulazioni numeriche

Parametro	Valore
Frequenza	700, 1800, 2100, 2600, 3700 MHz, 6 GHz, 26 GHz
Altezza della BS	4 m
EIRP	59.83 dBm
Piano di simulazione	Orizzontale
Altezza del piano di simulazione	1.05 m da terra
Dimensioni pixel	$0.01 \times 0.01 \text{ m}^2$ per scenario in-car $0.10 \times 0.10 \text{ m}^2$ per scenario near-car

Il segnale radio viene generato da una singola BS, posizionata a una distanza variabile dall'auto a seconda dello scenario (come illustrato in Figura 6-a): 920 cm dall'inizio del cofano (Scenario 1) o 844 cm dalla portiera laterale (Scenario 2).

## 4 - Risultati delle simulazioni e confronti

Per il calcolo della CPL è stato adottato l'approccio "point to point" descritto in [4] che segue tre passaggi chiave:

1. Simulazione del campo elettrico E interno all'auto (area blu di Figura 5-b) con ray-tracing 3D;
2. Simulazione del campo elettrico E in spazio libero nell'area occupata dalla vettura;
3. Confronto dei due valori di campo (espressi in dB).

I risultati numerici sono stati poi messi a confronto con i dati misurati per entrambi gli scenari definiti e descritti in Sezione 3.1.

### 4.1 – Scenario 1 – Posizione frontale

Figura 7-a e Tabella 5 mostrano il confronto tra i valori medi di CPL ottenuti dalle simulazioni (colonna 2) con i risultati delle misure. Le colonne successive di Tabella 5 riportano la CPL media calcolata per la posizione frontale sull'intera auto (colonna 3) e i valori medi assoluti di CPL aggregati per tutte le posizioni di misura e gli orientamenti (colonna 4).

**Tabella 5.** CPL simulate e confronto con i risultati delle misure – scenario frontale

Frequenza (MHz)	CPL <sub>simulata</sub> (dB)	CPL <sub>mis-front</sub> (dB)	CPL <sub>mis_gen</sub> (dB)	% fenomeni costruttivi*
700	1.63	2.16 ± 6.4	3.22 ± 2.8	69.2
1800	3.09	4.26 ± 2.1	4.97 ± 2.6	40.82
2100	4.02	4.64 ± 3.9	4.82 ± 3.4	34.62
2600	5.1	0.38 ± 2.9	2.64 ± 3.4	32.4
3700	3.13	4.7 ± 5.9	4.98 ± 5	38.4
6000	3.84	-	-	35.8
26000	1.72	-	-	52.4

\* Nota: per pixel con fenomeni costruttivi si intendono i pixel per i quali è vera la relazione  $E_{RT-pix}(i) > E_{FS-pix}(i)$

L'analisi dei dati in Tabella 5 ed in Figura 6 evidenzia, tenendo conto delle elevate deviazioni standard che caratterizzano i dati sperimentali, una concordanza complessiva tra i dati misurati e quelli simulati sia in termini di tendenza che di valori assoluti.

La Figura 8-a mostra come la distribuzione del campo elettrico all'interno del veicolo vari con la frequenza e mette a confronto i pattern simulati a 3.7 GHz (immagine in alto) e a 26 GHz (immagine in basso); tale variazione è causata dalle diverse dinamiche di riflessione del segnale all'interno dell'abitacolo. Figura 8-b mostra l'impatto del veicolo sulla propagazione esterna del segnale radio. Dal confronto tra lo scenario con l'auto e quello in spazio libero emerge che la vettura introduce una significativa perturbazione della distribuzione del campo elettrico che si manifesta come scattering (dispersione) che arriva ad estendersi fino a circa 3 m dal cofano. Oltre i 3 m (aree blu e verdi nella mappa di Figura 8-b), l'effetto risulta meno evidente.

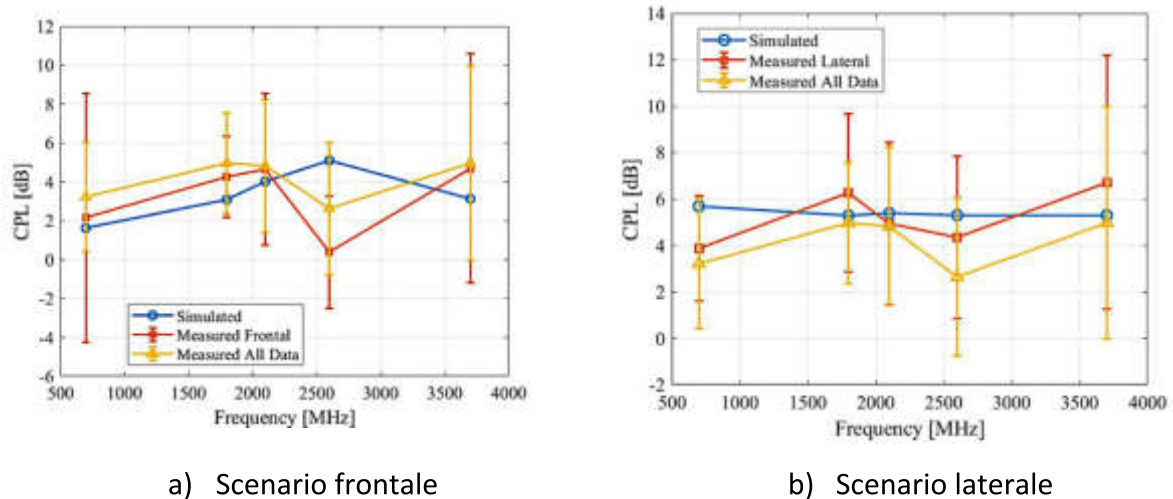


Figura 7 - Confronto tra CPL medio simulato e CPL medio misurato con deviazione standard

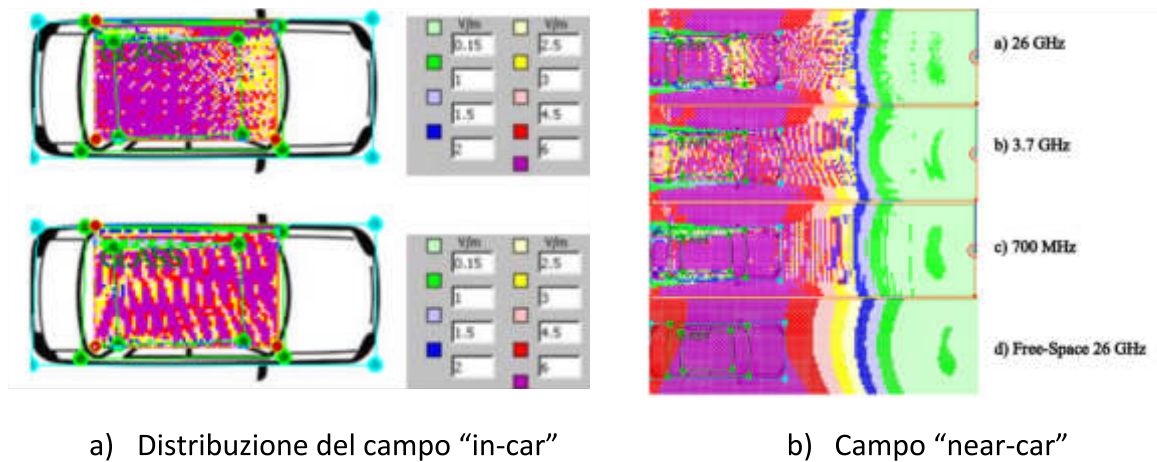


Figura 8 - Campo elettrico simulato “in-car” e “near-car” scenario frontale

Questo risultato è atteso in quanto la presenza del veicolo influenza il segnale radio attraverso complessi fenomeni fisici quali:

- **Riflessione e multipath** - I segnali radio riflessi all’interno della vettura generano percorsi multipli che possono sommarsi in modo costruttivo, aumentando l’intensità di campo ricevuto, o distruttivo (riducendone l’intensità finale), a seconda dell’allineamento di fase [14].
- **Diffrazione** –Il segnale si ‘curva’ attorno ai bordi della carrozzeria dell’auto (tetto, paraurti, specchietti laterali); ciò gli consente di raggiungere aree che altrimenti sarebbero in ombra, come le zone dietro l’auto.

In sintesi, le mappe di Figura 8 rivelano un complesso scenario multi-cammino che determina contributi sia costruttivi che distruttivi. L’entità numerica della perturbazione esterna “Near-car” e la sua dipendenza dalla distanza tra auto e BS non sono state ancora analizzate.

In caso di allineamento in fase, in alcuni pixel i livelli di campo elettrico interno al veicolo possono superare i valori simulati in spazio libero; si tratta di un fenomeno di potenziamento del segnale definito dalla relazione:

$$E_{RT-pix}(i) > E_{FS-pix}(i) \quad (3)$$

Dove  $E_{RT-pix}(i)$  è il valore del campo E nel pixel i-esimo ottenuto tramite simulazioni con tecniche di 3D ray-tracing e  $E_{FS-pix}(i)$  è il valore del campo elettrico nel pixel i-esimo ottenuto con la simulazione in spazio libero (scenario “No-Car”). L’analisi dei dati specifici (Tabella 5, ultima colonna) ha rivelato che la percentuale media di pixel che soddisfa la condizione (3) è pari al 43%, stabile nel range 2100 – 6000 MHz. L’unico dato inatteso è l’alta percentuale di fenomeni costruttivi riscontrata a 700 MHz, che riduce significativamente la CPL ed è probabilmente imputabile alle riflessioni sul cofano. Tale risultanza sarà oggetto di indagini future tramite misurazioni e simulazioni mirate. Per coerenza con il protocollo di misura, le simulazioni frontali sono state eseguite su un piano che si trova 5 cm sopra il cofano, pertanto la mappatura di Figura 8-a non mostra gli effetti di schermatura da parte del corpo metallico dell’auto. L’analisi visiva degli scenari “Near-Car” simulati (Figura 8-b) conferma che la presenza di un veicolo genera una perturbazione del segnale a radiofrequenza che si manifesta come una alternanza di aree ad alto e basso campo elettrico. Questo aspetto, unitamente alla variabilità del segnale interno alla vettura dovuta a riflessioni e multipath (confermata sia da misure che da simulazioni), deve essere considerato come un fattore chiave per la caratterizzazione e la garanzia della continuità del segnale in contesti V2V e V2X, soprattutto in caso di scenari a basso impatto elettromagnetico.

#### **4.2 – Scenario 2 – Posizione laterale**

L’analisi numerica per la posizione laterale è stata condotta a sua volta con il metodo “point-to-point” sinteticamente descritto ad inizio sezione. La Tabella 6 mette a confronto i valori medi di CPL simulati con i risultati delle misurazioni relative all’orientamento laterale.

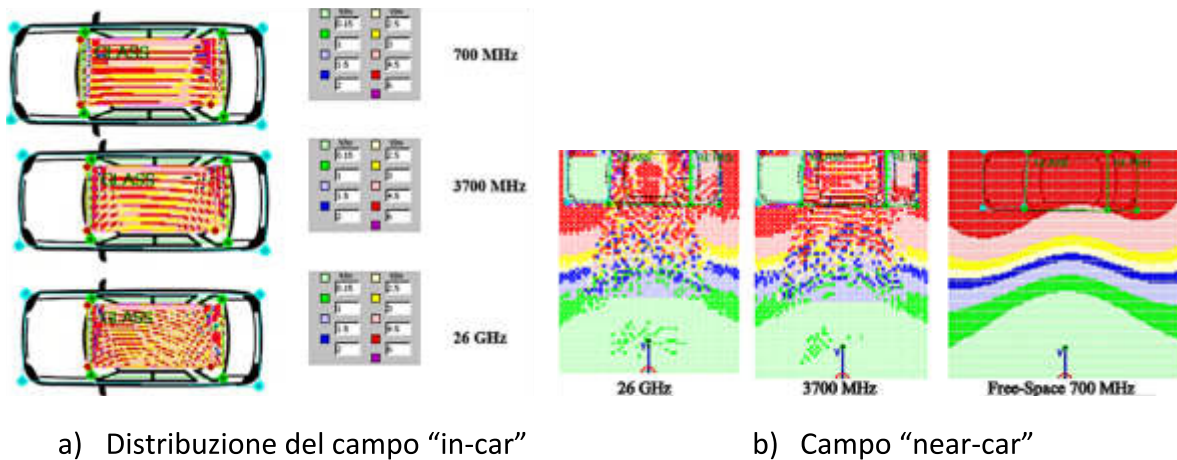
Rispetto ai dati relativi alla posizione frontale (Tabella 5) si nota una minore variabilità della CPL e percentuali inferiori di eventi costruttivi. Questa differenza è presumibilmente dovuta all'assenza delle riflessioni provenienti dal cofano, che, nello scenario frontale, aumentano la complessità del multipath.

**Tabella 6.** CPL simulate e confronto con i risultati delle misure – scenario laterale

Frequenza (MHz)	CPL <sub>simulata</sub> (dB)	CPL <sub>mis-lat</sub> (dB)	CPL <sub>mis_gen</sub> (dB)	% fenomeni costruttivi*
700	5.69	3.87 ± 2.26	3.22 ± 2.8	34.7
1800	5.29	6.26 ± 3.4	4.97 ± 2.6	39.6
2100	5.39	4.94 ± 3.49	4.82 ± 3.4	40.9
2600	5.30	4.34 ± 3.49	2.64 ± 3.4	37.4
3700	5.30	6.72 ± 5.46	4.98 ± 5	38.3
6000	5.17	na	na	40.0
26000	5.22	na	na	38.4

\* Nota: per pixel con fenomeni costruttivi si intendono i pixel per i quali è vera la relazione  $E_{RT-pix}(i) > E_{FS-pix}(i)$

Il grafico di Figura 7-b, che mette a confronto il dato simulato con quello misurato per l'orientamento laterale, conferma la minore variabilità dei risultati nello scenario laterale rispetto alla posizione frontale. Considerate le elevate deviazioni standard si riscontra un buon accordo tra dati misurati e simulati, sia in termini di andamento che in termini assoluti.



*Figura 9 - Campo elettrico simulato "in-car" e "near-car" - scenario laterale*

La Figura 9-a mostra la distribuzione del campo E interno alla vettura per lo scenario laterale. Dalla analisi delle mappe e della Tabella 6 si evince che:

- i livelli di campo elettrico all'interno della vettura sono inferiori rispetto all'orientamento frontale. I colori predominanti nelle mappe relative all'orientamento laterale sono infatti il giallo ed il rosso che indicano livelli di campo elettrico più bassi rispetto al viola che è il colore predominante per gli scenari ad orientamento frontale.
- le zone caratterizzate da fenomeni costruttivi e distruttivi seguono schemi più regolari che sembrano dipendere dalla frequenza del segnale incidente.

La Figura 9-b mostra la situazione nelle zone vicine alla vettura, dove quest'ultima genera perturbazioni del campo elettrico che si estendono fino a 5 m. Queste simulazioni sono state eseguite a un'altezza inferiore rispetto al caso frontale (5 cm in meno) per tenere conto degli effetti di schermatura del bagagliaio, consentendo la penetrazione del segnale solo tramite finestrini e piccole aperture.

## **5 - Considerazioni finali e prossime attività di studio**

La perdita di penetrazione è un parametro chiave negli studi sulla comunicazione wireless e per i sistemi V2X (Vehicle-to-Everything) e V2V (Vehicle-to-Vehicle) in quanto determina la potenza del segnale ricevuto all'interno del veicolo. La sua corretta conoscenza è essenziale per garantire le prestazioni e l'affidabilità V2X, per determinare i livelli di segnale del ricevitore all'interno dell'abitacolo e l'effettiva copertura per scenari V2V con antenne interne e, in fase di test per comprendere quali segnali esterni penetrano nell'abitacolo e in che misura al fine di creare scenari di simulazione il più possibile aderenti alle condizioni reali.

Questo studio, basato su campagne di misura e simulazioni numeriche, ha come obiettivo di caratterizzare sperimentalmente i valori di CPL e derivare per quanto possibile un modello di riferimento da applicare negli scenari futuri. La nuova campagna di misura ed i risultati delle simulazioni numeriche confermano, in linea con studi precedenti [4], l'assenza di una dipendenza della CPL dalla frequenza nell'intervallo 700 – 3800 MHz. Questo può consentire l'utilizzo di un valore di CPL rappresentativo per future ricerche in questa banda. I risultati dell'analisi dei dati di misura mostrano valori medi di CPL calcolati considerando l'auto come un'entità unica compresi tra 1.81 e 4.97 dB, in linea con le risultanze di analisi precedenti [4] e con quanto riportato in letteratura [5],[6], [7].

Lo scenario si è rivelato altamente complesso e caratterizzato da una elevata variabilità spaziale, elemento critico per la stabilità delle comunicazioni V2X. Le analisi condotte hanno mostrato che la CPL è influenzata dall'orientamento del veicolo (frontale, laterale), dalla posizione del ricevitore a bordo e dalle caratteristiche dei finestrini (ad esempio, i vetri oscurati aumentano la CPL di quasi un dB).

L'orientamento frontale presenta valori di CPL media inferiori (3.02 dB), probabilmente a causa delle riflessioni sul cofano. I ricevitori sui sedili posteriori mostrano un aumento medio della CPL variabile tra 1.32 ed 1.97 dB, mentre il bagagliaio registra l'attenuazione maggiore (fino a 6.71 dB).

I risultati di simulazioni e misure concordano nell'evidenziare che l'interferenza costruttiva crea, all'interno della vettura, "hot spots" di campo elettrico molto elevato, che risultano in CPL negative o molto basse in specifici punti, a conferma dell'alta variabilità spaziale del segnale in-car. Le simulazioni "Near-Car" hanno evidenziato che la presenza di un veicolo genera perturbazioni del campo elettromagnetico esterno (scattering) che possono influenzare la comunicazione V2X; i disturbi si estendono fino a 3 m in posizione frontale e oltre i 5 m in posizione laterale. Queste perturbazioni devono essere integrate nella progettazione dei sistemi V2X per garantire una comunicazione affidabile e prevenire problemi di carattere prevalentemente interferenziale.

L'attività di ricerca per il futuro mira a colmare le lacune per arrivare ad una caratterizzazione completa e affidabile e prevede:

1. Indagini sugli effetti specifici delle riflessioni e sull'impatto del tilt dell'antenna trasmittente sulla CPL.
2. La caratterizzazione delle perturbazioni del campo elettromagnetico indotte dal veicolo e del loro impatto sui sistemi V2X
3. L'estensione dello studio alle bande di frequenza superiori (6 GHz, 26 GHz e FR2/FR3), fondamentali per i sistemi 5G NR V2X
4. Studi in condizioni controllate attraverso l'impiego di generatori di segnale
5. L'ampliamento della ricerca con campagne di misura su diversi modelli di veicolo per convalidare l'applicabilità di un valore unico di CPL.

## **6 – Ringraziamenti**

Questo lavoro è stato sostenuto dall'Unione Europea nell'ambito del Piano Nazionale Italiano per la Ripresa e la Resilienza (PNRR) di NextGenerationEU, partenariato sulle "Telecomunicazioni del futuro" (PE00000001 - programma "RESTART", Progetto strutturale 6GWINET).

## 7 - Bibliografia

- [1] CEPT, CEPT Report 17, “Report from CEPT to the European Commission in response to the Mandate to: identify the conditions relating to the harmonised introduction in the European Union of radio applications based on Ultra-WideBand (UWB) technology” , 2017.
- [2] ITU, Report ITU-R M.2412-0, “Guidelines for evaluation of radio interface technologies for IMT-2020”, 2017.
- [3] 3GPP Technical Specification 3GPP TR 38.901, “5G; Study on channel model for frequencies from 0.5 to 100 GHz”, version 18.0.0.
- [4] S. Valbonesi, C. Carciofi, A. Garzia “Characterization of in-car and in-train Penetration Loss: measurements and simulations”, *AEIT 2025 International Annual Conference*, 2025.
- [5] E. Tanghe, W. Joseph, L. Verloock and L. Martens, “Evaluation of Vehicle Penetration Loss at Wireless Communication Frequencies,” *IEEE Transactions on Vehicular Technology*, vol. 57, no. 4, pp. 2036-2041, 2008, doi: 10.1109/TVT.2007.912164.
- [6] U. T. Virk, K. Haneda, V. -M. Kolmonen, P. Vainikainen and Y. Kaipainen, “Characterization of Vehicle Penetration Loss at wireless communication frequencies” , *The 8<sup>th</sup> European Conference on Antennas and Propagation (EuCAP 2014)*, The Hague, Netherlands, 2014, pp. 234-238, doi:10.1109/EuCAP.2014.6901733.
- [7] LSTelcom/OFCOM, “In-car Mobile Signal Attenuation Measurements –Final Report”, 2017.
- [8] C. Carciofi, M.Faccioli, A.Garzia, V.Petrini, E. Mammi, S.Valbonesi – “*Metodologie di valutazione e analisi del fattore Building Entry Loss per scenari di coesistenza indoor*” – Rivista La Comunicazione – Note, Recensioni, Notizie n.69 – 2025
- [9] S. Valbonesi, C. Carciofi, A. Garzia – “*Characterization of in-car and in-train Penetration Loss: measurements and simulations*” - CA20120 TD(25)11009, Gothenburg, Sweden, June 16-19, 2025
- [10] NARDA SRM-3006 - Frequency-selective EMF measurement  
<https://www.narda-sts.com/en/products/emf-selective-measuring-devices/srm-3006/>

[11] CEPT Report 17, “Report from CEPT to the European Commission in response to the Mandate to: identify the conditions relating to the harmonised introduction in the European Union of radio applications based on Ultra-WideBand (UWB) technology”, 2017.

[12] A. Garzia, A. Iodice, F. Lodato, F. Matera, R. Massa, G. Ruello, S. Valbonesi, "Human exposure to electromagnetic fields for new wireless technologies and frequencies: software characterization study," *2023 AEIT International Annual Conference (AEIT)*, Rome, Italy, 2023, pp. 1-6, doi: 10.23919/AEIT60520.2023.10330410. “

[13] R. G. Kouyoumjian and P. H. Pathak, “A Uniform Geometrical Theory of Diffraction for an Edge in a Perfectly Conducting Surface” , *Proc. IEEE*, vol. 62, no.11, pp. 1448-1461, 1974.

[14] P. Juyal, J. Fu and A. Zajic, "Effects of Modes on THz Wireless Channels Inside Metal Enclosures," *2020 XXXIII<sup>rd</sup> General Assembly and Scientific Symposium of the International Union of Radio Science*, Rome, Italy, 2020, pp. 1-2, doi: 10.23919/URSIGASS49373.2020.9232451.

## **Stato dell'arte sull'attività di regolamentazione del servizio di connettività diretta da satellite a terminali utente IMT (DC-MSS-IMT)**

### ***State of the art on the regulatory activity of the direct satellite connectivity service to IMT user terminals (DC-MSS-IMT)***

Massimo Celidonio<sup>♦</sup>

♦ Fondazione Ugo Bordoni

#### **Sommario**

Il presente lavoro intende fornire lo stato dell'arte riguardante le attività di carattere tecnico e normativo in svolgimento a livello internazionale su una tematica di grande attualità: il servizio mobile via satellite per la connettività diretta con i terminali utente IMT denominato DC-MSS-IMT. Lo studio è specificamente motivato e guidato dalla Risoluzione 253 approvata nel corso della Conferenza Mondiale delle Radiocomunicazioni del 2023 (WRC-23), la quale ha dato origine all'Agenda Item 1.13 (AI 1.13) per la prossima Conferenza Mondiale (WRC-27). In particolare, l'AI 1.13 è dedicato all'esame di possibili nuove allocazioni spettrali per i sistemi mobili via satellite e all'elaborazione di regolamenti tecnici e operativi, compresi i criteri di coordinamento, per proteggere i servizi esistenti. In questo contributo, oltre a fornire una breve descrizione delle funzionalità previste, vengono individuati i gruppi di lavoro in ambito ITU e CEPT che stanno studiando le problematiche connesse con l'introduzione di questo nuovo servizio e, in particolare, focalizza l'attenzione sui problemi interferenziali che si potrebbero determinare nelle zone di confine di due Stati, di cui uno ne autorizza il servizio e l'altro lo esclude. A tal riguardo vengono mostrati i parametri di riferimento per la valutazione del grado di interferenza i cui valori dovranno essere stabiliti a seguito degli studi che sono in corso.

Vengono anche descritte alcune tecniche di mitigazione delle interferenze che sono attualmente oggetto di studio per ridurre gli effetti dannosi prodotti dai segnali indesiderati.

## **Abstract**

This paper aims to provide a state-of-the-art overview of the technical and regulatory activities underway at the international level on a highly topical issue: the mobile satellite service for direct connectivity with IMT user terminals, known as DC-MSS-IMT. The study is specifically motivated and guided by Resolution 253 adopted at the 2023 World Radiocommunication Conference (WRC-23), which gave rise to Agenda Item 1.13 (AI 1.13) for the next World Conference (WRC-27). Specifically, AI 1.13 is dedicated to examining possible new spectrum allocations for mobile satellite systems and developing technical and operational regulations, including coordination criteria, to protect existing services. This paper, in addition to providing a brief description of the features envisioned for this service, identifies the ITU and CEPT working groups that are studying the issues associated with the introduction of this new service. It focuses on the interference problems that could arise in the border areas of two countries, one of which authorizes the service and the other excludes it. In this regard, it presents the reference parameters for assessing the level of interference, the values of which will be established following ongoing studies.

It also describes some interference mitigation techniques currently under study to reduce the harmful effects of unwanted signals.

## **Keyword**

Servizio mobile IMT via satellite, Aspetti di regolamentazione, Problemi interferenziali, tecniche di mitigazione

## 1 - Introduzione

Il rapido avanzamento delle tecnologie spaziali e delle telecomunicazioni ha inaugurato una nuova era per la connettività globale, in particolare con l'emergere di costellazioni di **satelliti in orbita terrestre bassa (LEO - Low Earth Orbit)**. Questi sistemi LEO, progettati per offrire servizi di *Direct-to-Cell (D2C)*, mirano a integrare la copertura radiomobile terrestre utilizzando le bande di frequenza tradizionalmente assegnate all' *International Mobile Telecommunications (IMT)*, consentendo ai comuni *smartphone* di comunicare direttamente con i satelliti. Sebbene questa innovazione prometta di estendere la connettività nelle aree remote e di colmare il divario digitale, essa introduce significative sfide nella gestione dello spettro radio a livello internazionale, in particolare riguardo al rischio di **interferenza transfrontaliera**.

Il presente studio si focalizza sull'analisi critica del potenziale impatto interferenziale generato da questi sistemi satellitari LEO-D2C sui **sistemi radiomobili terrestri** operanti nelle medesime bande di frequenza IMT, ma situati in **Paesi confinanti** a quelli che hanno autorizzato l'uso dei servizi satellitari. L'interferenza non si limita ai confini dello Stato che autorizza, ma si propaga a causa della vasta area di copertura del fascio satellitare (*footprint*), ponendo a rischio la qualità e l'affidabilità dei servizi mobili terrestri limitrofi. Infatti, il modello tradizionale di accordi bilaterali per la coordinazione transfrontaliera è reso insufficiente dalla natura intrinseca delle costellazioni satellitari LEO. La "cella" di un satellite LEO può avere un diametro superiore a 100 km, un singolo satellite può attraversare diversi confini internazionali in pochi minuti e un'intera costellazione opera come un'unica, grande rete. Ciò significa che una singola fonte di interferenza può colpire più giurisdizioni contemporaneamente, rendendo indispensabile una soluzione multilaterale e globalmente armonizzata, a differenza dei frammentati accordi bilaterali del passato. Si tratta di un cambiamento fondamentale nell'approccio alla gestione dello spettro a livello transfrontaliero.

Lo scopo principale della ricerca è **determinare il criterio di protezione più appropriato** per i terminali radiomobili terrestri. L'analisi si concentra sulla valutazione di due parametri tecnici fondamentali per la protezione:

*M. Celidonio*

1. **Rapporto Interferenza/Rumore (I/N):** Un parametro chiave utilizzato per quantificare il livello massimo di interferenza tollerabile dal terminale terrestre rispetto al rumore di sistema, garantendo che le prestazioni del servizio rimangano accettabili.
2. **Power Flux Density (PFD) al suolo:** Un limite imposto sulla potenza del segnale satellitare che raggiunge la superficie terrestre, inteso a limitare l'interferenza nelle regioni al di fuori dell'area di servizio autorizzata.

La scelta del criterio di protezione ottimale è essenziale per bilanciare l'innovazione offerta dai servizi satellitari D2C con la necessità di salvaguardare gli investimenti e la continuità operativa delle reti mobili terrestri esistenti in Paesi confinanti.

Questo lavoro si inserisce in un contesto normativo internazionale di grande attualità, rappresentando un contributo diretto alle attività in corso in seno all'**Unione Internazionale delle Telecomunicazioni (ITU)**. Lo studio è specificamente motivato e guidato dalla **Risoluzione 253 (WRC-23)** [1], la quale ha dato origine all'**Agenda Item 1.13 (AI 1.13)** per la prossima **Conferenza Mondiale delle Radiocomunicazioni (WRC-27)**. L'AI 1.13 è dedicato all'esame della necessità di nuove allocazioni spettrali per i sistemi mobili via satellite e all'elaborazione di regolamenti tecnici e operativi, compresi i criteri di coordinamento, per proteggere i servizi esistenti.

Pertanto, i risultati di questi studi mirano a fornire ai gruppi di studio dell'ITU (in particolare l'**ITU-R**, Settore delle Radiocomunicazioni dell'Unione Internazionale delle Telecomunicazioni) e alle amministrazioni nazionali una solida base tecnica e analitica per lo sviluppo di **regolamentazioni internazionali** e **accordi di coordinamento transfrontaliero** efficaci e lungimiranti, assicurando una coesistenza armoniosa tra i sistemi satellitari e terrestri nelle bande di frequenza assegnate ai servizi IMT.

## 2 - Attività in corso da parte degli Enti Internazionali e Regionali

### 2.1 – L'Unione Internazionale delle Telecomunicazioni (ITU-R)

A livello mondiale, l'ITU-R e in particolare i suoi gruppi di studio e le *Working Parties* pertinenti, costituisce il foro principale per la conduzione di studi di compatibilità e per l'elaborazione dei Rapporti ITU-R che saranno la base tecnica per le decisioni della WRC-27. Gli studi sono specificamente motivati e guidati dalla Risoluzione 253 approvato nel corso della Conferenza Mondiale delle Radiocomunicazioni del 2023 (WRC-23), la quale ha dato origine *all'Agenda Item 1.13* (AI 1.13) da discutere nella prossima Conferenza della WRC che si svolgerà nel 2027. La gestione degli studi sull'AI 1.13 all'interno dell'ITU-R è caratterizzata da una divisione del lavoro coordinata tra i suoi gruppi di lavoro. Il Gruppo di Lavoro 4C (WP 4C), responsabile dei servizi satellitari, ha la responsabilità complessiva per questo punto dell'agenda [2]. Il Gruppo di Lavoro 5D (WP 5D), che si occupa dei sistemi IMT, fornisce invece le caratteristiche tecniche e operative essenziali del componente terrestre [3]. Per coordinare le attività, una riunione congiunta tra i due gruppi si è svolta a ottobre 2024, con l'obiettivo di definire ruoli, responsabilità e una tempistica collaborativa.

Questa collaborazione non è una semplice convenienza amministrativa, ma una necessità tecnica. Per modellare e prevedere con precisione l'interferenza, gli studi devono disporre di dati precisi sia per il sistema interferente (la costellazione satellitare LEO) sia per il sistema interferito (la rete IMT terrestre). L'esperienza del WP 5D sulle implementazioni IMT terrestri, comprese le caratteristiche per gli studi di condivisione e compatibilità, è un prerequisito fondamentale affinché il WP 4C possa condurre simulazioni significative e sviluppare criteri di protezione efficaci. L'esito positivo dell'AI 1.13 dipende dall'efficace e tempestivo scambio di questi dati tecnici tra i due gruppi di lavoro. Il WP 4C ha già finalizzato un elenco di potenziali bande di frequenza da studiare sulla base dei contributi del WP 5D ed è in collegamento con altri gruppi di lavoro in ambito ITU, evidenziando il processo strutturato di condivisione delle informazioni all'interno dell'ITU.

## **2.2 – La Prospettiva Europea: I Contributi Tecnici e Politici della CEPT**

Il lavoro della Conferenza Europea delle Amministrazioni delle Poste e Telecomunicazioni (CEPT) è suddiviso tra due gruppi chiave. Il *Project Team 1* (ECC PT1) della Commissione Europea delle Comunicazioni (ECC) [4] è incaricato degli studi tecnici sull'*Agenda Item 1.13* della WRC-27, concentrandosi sulla protezione del componente terrestre delle reti IMT. Il *Project Team C* (CPG PTC) [5], orientato alla politica e facente parte del Comitato di Preparazione della Conferenza (CPG), ha la responsabilità generale del "*CEPT Brief*" (documento di posizione) e della "*European Common Proposal*" (ECP) per l'AI 1.13, ed è tenuto informato dei risultati tecnici dell'ECC PT1.

La posizione preliminare della CEPT sottolinea che le operazioni IMT terrestri "devono essere protette sia all'interno dei Paesi che in situazioni transfrontaliere, incluse le acque territoriali". La protezione dei servizi per le imbarcazioni nelle Zone Economiche Esclusive (ZEE) e in acque internazionali è una preoccupazione specifica.

Il forte accento posto dalla CEPT sulla protezione dei servizi transfrontalieri e costieri rivela una preoccupazione strategica specifica per la regione. L'Europa è un continente ad alta densità di paesi confinanti e con un'attività marittima significativa. Le reti mobili terrestri forniscono già servizi voce e dati cruciali alle imbarcazioni fino a 70-120 km dalla costa, fungendo anche da servizio di sicurezza. Il potenziale di un servizio satellitare LEO, autorizzato in un Paese, di degradare questo servizio esistente, non basato su satellite, per le navi costiere di un paese limitrofo, presenta una diretta sfida economica e di sicurezza pubblica che la CEPT sta affrontando in modo proattivo. Ciò dimostra come le discussioni normative globali siano plasmate da priorità regionali e nazionali.

Di seguito, una panoramica delle responsabilità all'interno dell'ITU-R e della CEPT.

M. Celidonio

**Tabella 1** - Gruppi di lavoro in ambito ITU e CEPT sulla tematica riguardante il servizio DC-IMT-MSS

Organizzazione	Gruppo di Lavoro	Responsabilità/Mandato
ITU-R	WP 4C	Ha il ruolo guida per gli studi sull'AI 1.13. Ha il compito di sviluppare un documento di lavoro sulle caratteristiche tecniche e operative del MSS per la comunicazione diretta con i terminali utente IMT e di finalizzare la lista delle bande di frequenza da studiare in base ai contributi del WP 5D.
ITU-R	WP 5D	Fornisce le caratteristiche tecniche e operative del componente terrestre delle reti IMT essenziali per gli studi di condivisione e compatibilità. È stato incaricato di fornire il suo parere sugli "aspetti tecnici relativi all'uso e al funzionamento del TDD per la connettività diretta" [6, 13].
CEPT	CPG PTC	Ha la responsabilità generale per il documento di posizione (CEPT Brief) e la Proposta Comune Europea (ECP) per l'AI 1.13. È tenuto informato sui risultati degli studi tecnici condotti dall'ECC PT1.
CEPT	ECC PT1	È incaricato di affrontare gli studi tecnici sull'AI 1.13, con particolare attenzione alla protezione del componente terrestre delle reti IMT. I suoi risultati sono richiesti per la preparazione dei documenti CPG PTC.

## 2.3 – Attività di Altri Organismi di Standardizzazione

### 2.3.1 – 3GPP e l'Integrazione delle Reti Non Terrestri (NTN)

Il quadro di riferimento si estende oltre l'ITU e la CEPT. Il *3rd Generation Partnership Project* (3GPP) svolge un ruolo cruciale nella standardizzazione della tecnologia stessa [6]. Il 3GPP ha formalizzato l'inclusione delle Reti Non Terrestri (*Non-Terrestrial Network*, NTN) come parte dell'ecosistema 5G nella Release 17, definendo architetture e modelli di propagazione [7]. L'obiettivo è creare un sistema di comunicazione unificato e senza interruzioni, dove i satelliti possono fornire connettività in aree remote o fungere da ridondanza in caso di disastri.

Il lavoro del 3GPP non è ridondante rispetto a quello dell'ITU, ma piuttosto complementare. Il 3GPP definisce come la tecnologia funziona (ad esempio, l'interfaccia radio, l'architettura di rete), mentre l'ITU fornisce il quadro normativo di alto livello, compresi quali bande di

frequenza possono essere utilizzate e i criteri di protezione per i servizi esistenti. I progressi del 3GPP, in particolare nella Release 17, forniscono le basi tecniche su cui si fonderanno le decisioni normative dell'ITU per l'AI 1.13. Il 3GPP si concentra su aspetti tecnici come la gestione dei ritardi di trasmissione e degli effetti *Doppler*, e lo sviluppo di tecniche avanzate di gestione dell'interferenza e della mobilità.

### 2.3.2 – Contesto Nordamericano: ATIS e il Quadro della FCC per la Copertura Supplementare dallo Spazio (SCS)

Un'altra prospettiva rilevante è fornita dal lavoro della *Alliance for Telecommunications Industry Solutions* (ATIS) e del suo gruppo di lavoro NTN in Nord America [8]. ATIS sta sviluppando una specifica per le "zone di esclusione" (EZ) a supporto del quadro normativo per la "Copertura Supplementare dallo Spazio" (SCS) della *Federal Communications Commission* (FCC) [9]. Questo quadro è un esempio concreto di un approccio normativo regionale volto a mitigare l'interferenza attraverso requisiti tecnici e di collaborazione.

Il lavoro di ATIS sulle zone di esclusione offre un prezioso caso di studio per gli studi internazionali. Il quadro EZ è uno strumento normativo tangibile che mira a gestire l'interferenza creando una separazione spaziale o temporale tra i servizi satellitari e quelli terrestri [10]. I risultati di questa iniziativa regionale potrebbero informare le discussioni globali più ampie in seno all'ITU e alla CEPT, fornendo dati e modelli pratici del mondo reale per la coesistenza. Ciò evidenzia una dinamica in cui la sperimentazione normativa a livello regionale può informare direttamente la politica globale.

### 2.3.3 – Sintesi del Progresso e Coordinamento Inter-organizzativo

L'analisi dei documenti di riferimento rivela un processo complesso e multilaterale, guidato dall'ITU-R, supportato da organismi regionali come la CEPT e con un contributo tecnologico cruciale da parte di enti di standardizzazione come il 3GPP e ATIS. Il principio guida è la protezione dei servizi esistenti, in particolare le reti IMT terrestri che già servono miliardi di persone. Gli studi attuali si concentrano sulla definizione di criteri di protezione robusti, come

*M. Celidonio*

il rapporto  $I/N$  e il parametro  $PF\Delta$ , che saranno descritti nei paragrafi successivi e che possano affrontare le sfide uniche poste dalle costellazioni LEO, inclusa l'interferenza transfrontaliera e le emissioni indesiderate. La collaborazione tra WP 4C e WP 5D nell'ITU-R è tecnicamente indispensabile, così come la divisione dei compiti tra gli organi tecnici e politici all'interno della CEPT.

### **3 – Il Servizio DC-IMT-MSS: Definizione e Bande di Frequenza in Esame**

#### **3.1 – Il servizio DC-MSS-IMT**

Il servizio Mobile via Satellite per la connettività diretta con i terminali utente IMT (DC-MSS-IMT) è un'iniziativa volta a integrare le reti satellitari con l'ecosistema IMT terrestre esistente [11]. Il suo obiettivo principale è estendere la copertura in aree remote, rurali e con scarsa connettività, fornendo una soluzione di comunicazione essenziale per le comunità non servite. Inoltre, questo servizio può offrire una maggiore resilienza della rete in caso di guasti o disastri naturali. Il *3rd Generation Partnership Project* (3GPP) ha formalizzato l'inclusione delle NTN come parte dell'ecosistema 5G, con l'obiettivo di supportare la connettività diretta con gli smartphone tradizionali. L'Unione Internazionale delle Telecomunicazioni (ITU) sta attualmente conducendo studi per definire le possibili nuove allocazioni di frequenza per questo servizio [2, 3]. Le bande di frequenza considerate si trovano nell'intervallo compreso tra 694 MHz e 2.7 GHz, in linea con gli accordi stabiliti per il servizio IMT.

#### **3.2 – Frequenze allo studio per il servizio DC-MSS-IMT**

Le frequenze elencate di seguito sono attualmente quelle candidate e oggetto di studio da parte dei gruppi di lavoro dell'ITU (come WP 4C e WP 5D) e della CEPT per la possibile assegnazione al servizio Mobile via Satellite per la connettività diretta [2, 3].

M. Celidonio

**Tabella 2** – Frequenze candidate e oggetto di studio per il servizio DC-MSS-IMT

Banda di Frequenza (uplink)	Banda di Frequenza (downlink)
814/824-849	859/869-894
880-915	925-960
832-862	791-821
698-716	716-746
776-798	746-768
698-748	753-803
1 427-1 470	1 475-1 518
1 920-1 980	2 110-2 170
1 710-1 785	1 805-1 880
1 850-1 920	1 930-2 000
1 710-1 780	2 110-2 180
2 000-2 020	2 180-2 200
2 010-2 025	1 880-1 920
2 305-2 320	2 345-2 360
2 500-2 570	2 620-2 690

### 3.2 – Modalità operative per offrire il servizio DC-MSS-IMT

Se si considera un generico Stato, il servizio fornito da un sistema DC-MSS-IMT può essere realizzato attraverso due possibili modalità: attraverso una copertura complementare a quella già esistente messa a disposizione dal MNO, a seguito di un accordo commerciale con lo stesso MNO che opera in quello Stato; oppure in modo esclusivo, dopo aver acquisito la licenza di una banda di frequenza utilizzata per il servizio IMT di quello Stato (vedi Figura 1).

In questa tipologia di servizio il satellite opera come una stazione radio base che attraverso un'antenna, tipicamente di tipo *phased array*, comunica con i terminali degli utenti a Terra. Ogni satellite della costellazione è normalmente dotato di tecnologie avanzate per facilitare la trasmissione dei dati. Oltre alle antenne *phased array*, sono presenti anche antenne paraboliche, che consentono comunicazioni ad alto guadagno con le stazioni a Terra, e

M. Celidonio

collegamenti ottici inter-satellitari utilizzati per la trasmissione dati tra i satelliti della costellazione.

Per i satelliti della costellazione, le stazioni a Terra operano come punti accesso alla rete mobile terrestre e in ultima analisi consentono di mettere in comunicazione gli utenti dei terminali mobili, collegati via satellite, con i loro interlocutori.

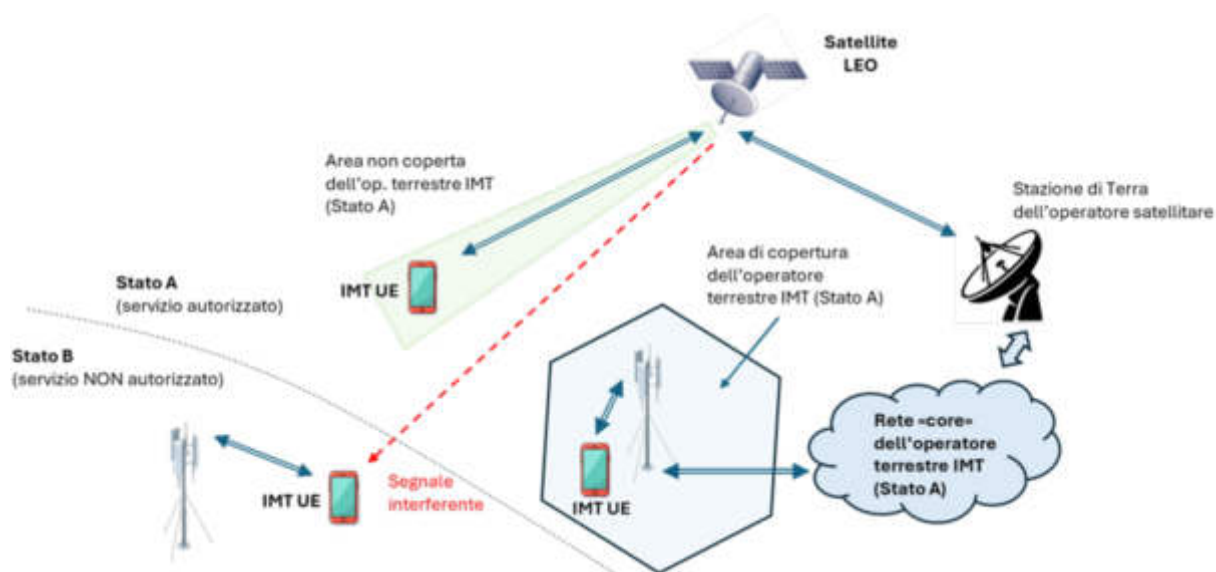


Figura 1 – Scenario interferenziale con il servizio DC-MSS-IMT

## 4 – Dati caratteristici delle costellazioni di satelliti

### 4.1 – Generalità sulle orbite dei satelliti

I satelliti, in base alle loro caratteristiche orbitali, sono generalmente classificati in tre grandi tipologie (vedi anche figura 2):

- **Orbita terrestre bassa (LEO).** I satelliti che operano su questa tipologia di orbita viaggiano ad un'altitudine relativamente vicina alla superficie terrestre, di solito, compresa tra i 200 e i 2000 km. Al di sopra di questo limite vi sono le fasce di Van Allen<sup>1</sup> che creano un ambiente ostile per i satelliti. L'altitudine inferiore a cui un satellite può orbitare è limitata dall'impatto con l'atmosfera terrestre. I piani orbitali dei satelliti LEO sono caratterizzati dall'angolo che formano rispetto il piano equatoriale. Vista la loro vicinanza alla superficie terrestre sono particolarmente indicati per acquisire immagini della superficie terrestre dallo spazio. Ultimamente, grazie anche alle basse latenze che garantiscono i collegamenti da queste orbite, si sta sviluppando un mercato che intende utilizzare questi satelliti nel settore delle comunicazioni rivolto ai consumatori di massa per fornire il servizio di Internet a banda larga e, nel prossimo futuro, anche quello dedicato ai terminali radiomobili IMT.
- **Orbita terrestre media (MEO).** In questo caso i satelliti operano su orbite che si trovano tra gli 8.000 e i 20.000 chilometri sopra la superficie terrestre. I satelliti MEO sono stati storicamente utilizzati per applicazioni GPS e per la radionavigazione. Più recentemente, costellazioni di questi satelliti, sono state implementate per fornire connettività dati a ridotta latenza (rispetto ai satelliti geostazionari) e ad alta larghezza di banda a fornitori di servizi, agenzie governative e aziende commerciali. I satelliti MEO possono offrire connessioni a larga banda in aree dove la posa della fibra non è praticabile come le navi da crociera e quelle commerciali, gli aeromobili e nelle aree critiche come quelle dove sono in svolgimento operazioni di soccorso umanitario.

---

<sup>1</sup> Le fasce di Van Allen sono regioni che circondano la Terra e che contengono particelle cariche ad alta energia, intrappolate dal campo magnetico terrestre. Sono composte principalmente da protoni ed elettroni provenienti dal vento solare e da raggi cosmici. Queste fasce sono pericolose per gli equipaggi umani e le apparecchiature elettroniche a causa dell'energia contenuta nelle particelle.

M. Celidonio

- **Orbita terrestre geostazionaria (o equatoriale geosincrona) (GEO).** Questa orbita è nota anche come Orbita di Clarke, fissata a 35.786 chilometri sopra l'equatore. I satelliti che operano su questa orbita seguono la rotazione terrestre, rimanendo quindi sempre sopra lo stesso punto sulla Terra. I satelliti GEO sono tradizionalmente dedicati alla trasmissione di servizi come dati meteorologici, trasmissioni televisive e alcune comunicazioni dati a bassa velocità. Negli ultimi anni, la tecnologia è migliorata notevolmente grazie all'uso di satelliti ad alta capacità (HTS), progettati appositamente per la trasmissione di dati.

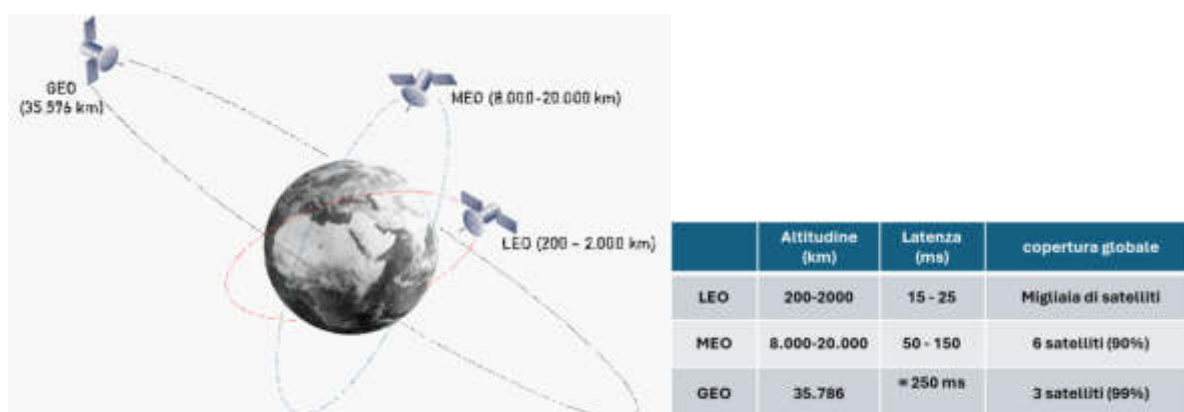


Figura 2 – Tipologie di orbite per i satelliti e principali caratteristiche

#### 4.2 – Costellazioni di satelliti che offrono il servizio DC-IMT-MSS

In ambito ITU-R sono state individuate alcune costellazioni di satelliti in orbita bassa (LEO) di riferimento per condurre gli studi di compatibilità e coesistenza tra il servizio DC-IMT-MSS e quello IMT terrestre. In tabella 3 sono riportate le caratteristiche delle costellazioni che possono essere ritenute le più significative per questi studi, se si considera che maggiore è il numero di satelliti presenti all'interno della costellazione e più aumenta la possibilità che si possano presentare situazioni di interferenza indesiderate situate nelle aree limitrofe a quelle nelle quali è autorizzato il servizio.

Come risulta evidente dalla tabella, l'uso di ciascuna costellazione è rivolto ad uno specifico insieme di bande di frequenza. Di conseguenza, gli studi che prenderanno in considerazione la costellazione denominata *System 1* si limiteranno ad utilizzare solo una banda di frequenza

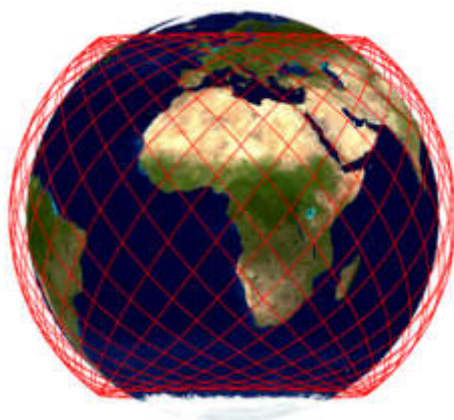
M. Celidonio

in modalità FDD, e precisamente la banda 2.5-2.57 GHz per il collegamento da Terra a satellite (*uplink*) e la banda 2.62-2.69 GHz per il collegamento da satellite a Terra (*downlink*).

Una costellazione particolarmente interessante è quella denominata *System 3-1* (Figura 3) che prevede 28 piani orbitali inclinati a 53° rispetto il piano equatoriale terrestre. Su ciascun piano orbitale vi sono 120 satelliti, separati uno dall'altro di 3° e ad un'altezza di 525 km. Tale costellazione è una di quelle che già viene sfruttata commercialmente anche se, per ora, con un numero di satelliti inferiore.

**Tabella 3** – Caratteristiche di alcune costellazioni di satelliti da utilizzare per gli studi di coesistenza

System ID	System 1	System 2	System 3-1	System 3-2
<b>Bande di frequenza (MHz)</b>	2 500-2 570/ 2 620-2 690	694/698-960	698-960	698-960
		1 427-1 518	1 427-1 518	1 427-1 518
		1 710-1 785/ 1 805-1 880	1 710-2 025/ 2 110 2 200	1 710-2 025/ 2 110 2 200
		1 920-1 980/ 2 110-2 170	2 500-2 690	2 500-2 690
		2 010-2 025/ 1 880-1 920		
		2 300-2 400		
2 500-2 690				
<b>Altitudine (km)</b>	680	500	525	340
<b>Inclinazione (gradi)</b>	97	55	53	53
<b>Numero piani orbitali</b>	12	60	28	48
<b>Numero satelliti per piano orbitale</b>	60	60	120	110
<b>Numero totale di satelliti</b>	720	3600	3360	5280



**Figura 3** – Piani orbitali relativi al System 3-1

## 5 – Problematiche interferenziali con le reti IMT terrestri

Il servizio DC-MSS-IMT, essendo offerto via satellite, potrebbe dare luogo a problemi di interferenza nei confronti del servizio IMT offerto da operatori mobili che operano in Stati che non ne hanno autorizzato l'uso e che si trovano adiacenti o comunque nelle vicinanze degli Stati che, al contrario, ne hanno concesso l'autorizzazione.

Inoltre, come avviene anche per altri servizi, se il segnale trasmesso via satellite non viene opportunamente controllato, limitando il livello di segnale presente al di fuori della banda utile, potrebbero crearsi problemi per altri servizi di radiocomunicazione, che possono essere anche differenti da quelli IMT, che operano nelle bande adiacenti a quella in uso al sistema DC-MSS-IMT.

Su queste due problematiche si stanno concentrando gli studi in ambito internazionale [2,3,5] allo scopo di fissare i livelli di potenza in trasmissione che saranno consentiti per i segnali emessi dal satellite verso Terra, sia nella banda utile sia in quelle adiacenti, al fine di garantire prestazioni adeguate al servizio DC-MSS-IMT e che, allo stesso tempo, protezione ad altri servizi esistenti che operano già sul territorio e che hanno il diritto di essere opportunamente tutelati.

### 5.1 – Studi tecnici e operativi per la protezione delle reti terrestri

#### 5.1.1 – I Principi Fondamentali della Coesistenza

Il principio cardine degli studi è la protezione dei servizi terrestri esistenti. Le ricerche indicano che la protezione deve essere garantita sia per gli scenari di condivisione del canale che per quelli in banda adiacente. Gli studi considerano l'interferenza derivante sia dalle emissioni dirette del satellite verso il terminale terrestre sia dalle sue "emissioni indesiderate" (*unwanted emissions*) [2, 3].

La necessità di considerare le emissioni indesiderate nella protezione delle reti MFCN (*Mobile/Fixed Communications Networks*) rappresenta un cambiamento significativo nella pratica normativa. Questo evidenzia una lacuna normativa che è stata esposta dall'introduzione di costellazioni LEO ad alta potenza e che ora viene affrontata attraverso gli

*M. Celidonio*

studi sull'AI 1.13. La necessità di giustificare un nuovo approccio per le emissioni indesiderate per le MFCN suggerisce che gli studi non si limiteranno ad applicare le regole esistenti, ma saranno costretti a svilupparne di completamente nuove.

#### 5.1.2 – Analisi Dettagliata dei Criteri di Protezione

##### 5.1.2.1 – Il Rapporto I/N

Il **rapporto I/N** fornisce una misura del livello del segnale interferente rispetto il rumore termico del sistema ricevente ed è una metrica chiave per valutare il degrado del bilancio di collegamento causato da uno o più segnali interferenti. Gli studi compilati dal rapporto della *National Telecommunications and Information Administration* (NTIA) [13] hanno rilevato che per le interferenze continue e a lungo termine, sono comunemente utilizzati valori di I/N compresi tra -6 e -10 dB. Tuttavia, per segnali intermittenti o a impulsi, i criteri possono variare. I satelliti LEO non sono una fonte di interferenza continua per un punto fisso, poiché il loro passaggio è temporaneo, rendendo questa intermittenza un fattore da considerare.

Le simulazioni Monte Carlo sono uno strumento essenziale per questi studi. Tale metodo modella un ricevitore "vittima" all'interno di una popolazione di "interferenti" per produrre risultati efficienti in termini di spettro.

##### 5.1.2.1 – Densità di Flusso di Potenza (PFD)

La PFD misura la potenza per unità di area e per unità di banda che un'emissione satellitare consegna a un punto a Terra ed è normalmente utilizzata come strumento normativo per limitare le emissioni satellitari e proteggere i servizi terrestri. I limiti di PFD sono presi in considerazione come un meccanismo per gestire le emissioni del satellite LEO. L'obiettivo è garantire che la potenza ricevuta a terra dal satellite non superi una soglia che possa causare interferenza dannosa ai sistemi terrestri. Gli studi in corso dovranno determinare le **soglie di PFD appropriate per vari scenari**, comprese le operazioni co-canale e in banda adiacente, e tenere conto sia delle emissioni desiderate che di quelle indesiderate. Lo scenario di riferimento per il calcolo di questo parametro è mostrato in figura 4.

M. Celidonio

L'espressione utilizzata per il calcolo di questo parametro è la seguente:

$$PFD(\vartheta) = \frac{P_T G_T(\vartheta)}{4\pi(R(\vartheta))^2}$$

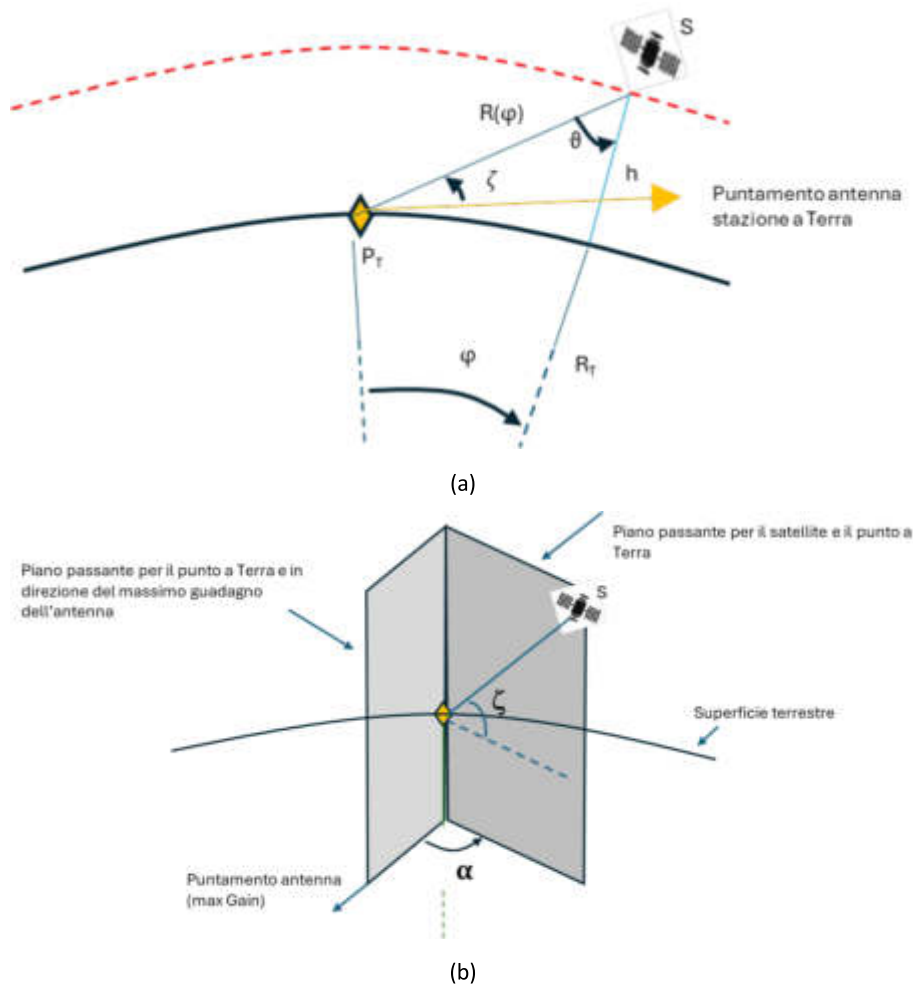
dove  $P_T$  è la potenza emessa dal trasmettitore,  $\vartheta$  è l'angolo con cui il satellite vede il punto di ricezione a Terra,  $G_T(\vartheta)$  è il guadagno dell'antenna nella direzione della stazione a Terra e  $R(\vartheta)$  è la distanza tra satellite e stazione ricevente.

Quando si considerano costellazioni di satelliti come quelle in orbita bassa (LEO), con la possibilità che un singolo punto a Terra possa essere in visibilità con più satelliti della costellazione, **la PFD viene spesso sostituita dal parametro di PFD Equivalente (EPFD)**. Storicamente, l'ITU ha stabilito limiti di EPFD per proteggere i satelliti in orbita geostazionaria (GEO) dall'interferenza causata dai satelliti non geostazionari (NGSO) [11]. L'EPFD calcola l'effetto aggregato di un insieme di satelliti NGSO su un ricevitore specifico, a differenza della PFD che si applica tipicamente a un singolo satellite. Con il lancio di un numero sempre maggiore di satelliti LEO dedicati al servizio IMT-MSS, aumenta il rischio di interferenza con i ricevitori IMT terrestri [11]. L'espressione dell'EPFD è la seguente:

$$EPFD = 10 \log_{10} \left[ \sum_{i=1}^N 10^{\frac{P_i}{10}} \cdot \frac{G_{Ti}(\vartheta_i)}{4\pi d_i^2} \cdot \frac{G_R(\zeta_i)}{G_{R,max}} \right]$$

nella quale si evidenzia una caratterizzazione dei singoli parametri riferita a ciascuno dei  $N$  satelliti che appartengono alla costellazione, visibili dalla stazione di Terra. In questa espressione  $G_{R,max}$  è il guadagno massimo dell'antenna della stazione ricevente e  $G_R(\zeta)$  il guadagno dell'antenna ricevente nella direzione del satellite.

M. Celidonio



**Figura 4** – Angoli caratteristici per il calcolo dei parametri PFD e EPFD

La scelta tra  $I/N$  e EPFD, o una combinazione di entrambi, è un aspetto critico degli studi. Il rapporto  $I/N$  si riferisce direttamente alle prestazioni del ricevitore ed è una metrica "di ricezione" (back-end) che richiede la conoscenza del rumore di fondo della vittima. La PFD è una metrica "di trasmissione" (front-end) che può essere regolamentata dal satellite trasmittente. I limiti di PFD offrono uno strumento normativo più semplice e universale, ma potrebbero non sempre cogliere accuratamente scenari di interferenza complessi, soprattutto per i diversi tipi di ricevitori. Il quadro normativo finale probabilmente utilizzerà una combinazione di queste e altre metriche per garantire una protezione completa.

M. Celidonio

Di seguito, un riepilogo dei due principali criteri di protezione:

Critério	Definizione	Applicazione negli attuali studi
<b>I/N</b> (Rapporto Interferenza/Rumore)	Rapporto tra la potenza di un segnale interferente e la potenza del rumore termico del ricevitore.	Utilizzato per quantificare il degrado del bilancio di collegamento. Valori di -6 a -10 dB sono punti di riferimento comuni per interferenze continue. Gli studi impiegano simulazioni Monte Carlo per analizzare gli effetti di aggregazione in un ambiente di rete.
<b>PFD</b> (Densità di Flusso di Potenza) e <b>EPFD</b> (PFD Equivalente)	La PFD misura la potenza per unità di area e per unità di banda che un'emissione satellitare consegna a un punto a Terra. L'EPFD estende questo concetto per calcolare l'effetto aggregato di intere costellazioni di satelliti.	La PFD è utilizzata come strumento normativo per limitare le emissioni satellitari e proteggere i servizi terrestri. L'EPFD è il parametro rilevante per valutare l'interferenza causata da costellazioni di satelliti. Gli studi stanno valutando i limiti per prevenire interferenze dannose da segnali satellitari, incluse le emissioni indesiderate.

## 6 - Possibili tecniche di mitigazione

Come è stato evidenziato nei paragrafi precedenti, la possibilità che si presentino problemi di interferenza in corrispondenza dei confini tra due Stati di cui uno ha autorizzato l'uso del servizio DC-MSS-IMT su una determinata banda di frequenza mentre l'altro Stato continua ad utilizzare la stessa banda di frequenza per il servizio IMT terrestre, è piuttosto elevata. Ciò è dovuto al fatto che l'operatore satellitare intende fornire servizio a tutti gli utenti dello Stato che ne ha autorizzato il servizio ma allo stesso tempo, il satellite, operando da un'altitudine di diverse centinaia di km, non ha la piena capacità di regolare il fascio in modo da limitare il segnale alle sole aree di interesse ma potrebbe accadere che il suo raggio di copertura si estenda facilmente in aree non autorizzate al servizio.

*M. Celidonio*

Per far fronte a questo problema sono allo studio diverse soluzioni di mitigazione del segnale che, allo stato attuale, si possono sintetizzare nelle seguenti tecniche:

- Spegnerne il segnale trasmesso dal satellite a partire da qualche chilometro prima che il *nadir* del satellite raggiunga il confine dello Stato (ad esempio 20-50 km);
- Ridurre progressivamente la potenza del segnale trasmesso dal satellite a partire da una determinata distanza dal confine dello Stato;
- Quando il satellite si avvicina al confine dello Stato, sfruttare le caratteristiche funzionali delle antenne *phased array* a bordo del satellite per indirizzare opportunamente il fascio per limitare i fenomeni interferenziali e continuare a offrire il servizio fino a che il *nadir* del satellite permane sul territorio dello Stato che lo ha autorizzato.

## **7 - Conclusioni**

Un approccio emergente per fornire connettività satellitare sulle bande terrestri IMT (*International Mobile Telecommunications*), noto come DC-MSS-IMT (*Direct Connectivity between Mobile Satellite Service stations and IMT*), è in fase di discussione presso il Settore Radiocomunicazioni dell'Unione Internazionale delle Telecomunicazioni (ITU-R). L'IMT, come definito dall'ITU-R, comprende tutte le generazioni di sistemi di comunicazione mobile, tra cui *IMT-2000* (3G), *IMT-Advanced* (4G), *IMT-2020* (5G) ecc. In questo modello, la trasmissione satellitare avverrebbe nelle bande IMT terrestri, assegnate a un MNO. Pertanto, la copertura satellitare sarebbe complementare a quella terrestre e avverrebbe sotto la responsabilità end-to-end dell'MNO. Tuttavia, le attuali normative internazionali in materia di radiocomunicazioni non consentono ai sistemi di comunicazione satellitare di operare all'interno delle bande IMT terrestri sui territori. Vari gruppi di lavoro, sia tecnici sia regolamentari, stanno attualmente discutendo la possibilità di consentire l'utilizzo del DC-MSS-IMT all'interno delle bande IMT terrestri. In particolare, il problema dell'interferenza transfrontaliera generata dai sistemi satellitari LEO-D2C è al centro di intense attività tecniche e normative a livello globale e regionale.

*M. Celidonio*

In **Europa**, la **CEPT** (Conferenza Europea delle Amministrazioni delle Poste e delle Telecomunicazioni) sta svolgendo un ruolo cruciale, in particolare attraverso i suoi gruppi di lavoro. Il **PTC (Project Team C)** e il **PT1 (Project Team 1)** sono attivamente impegnati nell'elaborazione di studi tecnici e nella preparazione di posizioni comuni europee (ECPs) in vista della WRC-27. Questi gruppi stanno esaminando i criteri di protezione, inclusi i limiti di *I/N* e *PF*, per assicurare la coesistenza armoniosa e per sviluppare proposte regolamentari per l'Agenda Item 1.13.

A livello **mondiale**, l'**ITU-R** (Settore delle Radiocomunicazioni dell'Unione Internazionale delle Telecomunicazioni), in particolare i suoi gruppi di studio e le *Working Parties* pertinenti, costituisce il foro principale per la conduzione di studi di compatibilità e per l'elaborazione dei **Rapporti ITU-R** che saranno la base tecnica per le decisioni della WRC-27. Parallelamente, anche **organizzazioni di standardizzazione extra-europee**, come il **3GPP (3rd Generation Partnership Project)**, pur non essendo un organismo regolatore, sono coinvolte nell'analisi delle specifiche tecniche e dei requisiti di **interoperabilità e coesistenza** tra le reti terrestri e le nuove componenti satellitari (NTN - *Non-Terrestrial Networks*). Grazie a questo lavoro congiunto si punta a definire un quadro normativo e tecnico solido che consenta ai servizi innovativi D2C di operare proteggendo al contempo i servizi radiomobili terrestri esistenti.

## 9 - Bibliografia

- [1] International Telecommunication Union. *Resolution 253 (WRC-23)* – “Studies on possible new allocations to the mobile-satellite service for direct connectivity between space stations and International Mobile Telecommunications (IMT) user equipment to complement terrestrial IMT network coverage”, *World Radiocommunication Conference 2023, Dubai, United Arab Emirates*, 20 November - 15 December 2023
- [2] International Telecommunication Union – Radiocommunication Sector. (n.d.). Working Party 4C – Efficient orbit/spectrum utilization for MSS and RDSS. Retrieved [data di accesso], <https://www.itu.int/en/ITU-R/study-groups/rsg4/rwp4c/Pages/default.aspx>

*M. Celidonio*

- [3] International Telecommunication Union – Radiocommunication Sector. (n.d.). Working Party 5D (WP 5D) – IMT Systems, <https://www.itu.int/en/ITU-R/study-groups/rsg5/rwp5d/Pages/default.aspx>
- [4] CEPT ECC PT1 - Group PT1 – IMT Matters., <https://www.cept.org/ecc/groups/ecc/ecc-pt1/>
- [5] CEPT ECC CPG PTC - Project Team C – Mobile Satellite Service & General Issues (CPG PTC). <https://www.cept.org/ecc/groups/ecc/cpg/cpg-ptc/>
- [6] 3rd Generation Partnership Project (3GPP), Home – The Mobile Broadband Standard. <https://www.3gpp.org/>
- [7] 3GPP Release 17 – “Specifications & Technologies”, *3rd Generation Partnership Project*, 2022
- [8] Alliance for Telecommunications Industry Solutions - Integration of Non-Terrestrial Networks (NTN) 5G Working Group. <https://www.atis.org/initiatives/non-terrestrial-networks-ntn-5g-integration/>
- [9] Federal Communications Commission, “Report and Order and Further Notice of Proposed Rulemaking: Single Network Future: Supplemental Coverage from Space”, *GN Docket No. 23-65 & IB Docket No. 22-271*, April 2024
- [10] ATIS. (version V16.00). ATIS.3GPP.38.820.V1600 (contributo ATIS a 3GPP),” Parametri RF e spatial/frequency exclusion utili per la definizione delle EZ”, <https://atisorg.s3.amazonaws.com/archive/3gpp-documents/Rel16/ATIS.3GPP.38.820.V1600.pdf>
- [11] ITU-R WP4C, , “Working Document on the possible Description and Functionality of MSS Systems for Direct Connectivity Between Space Stations and IMT User Equipment”, *R23-WP4C-251015-TD-0135*, October 2025
- [12] 3GPP TR 38.821 — “Solutions for NR to support Non-Terrestrial Networks (NTN). 3rd Generation Partnership Project”, *Technical Report*, 2021
- [13] Paul, A., Hurt, G., Sullivan, T., Patrick, G., Sole, R., Brunson, L., Wang, C.-W., Joiner, B., Drocella, E. (2005). “Interference Protection Criteria – Phase 1: Compilation from Existing Sources”, *NTIA Report 05-432. U.S. Department of Commerce, National Telecommunications and Information Administration*. October 1, 2005

## **Analisi delle opportunità di condivisione della banda di frequenza 27.5-29.5 GHz tra sistemi terrestri e sistemi satellitari**

### ***Analysis of the spectrum sharing opportunities of the frequency band 27.5-29.5 GHz between terrestrial and satellite systems***

Valeria Petrini ♦, Claudia Carciofi ♦, Manuel Faccioli ♦, Andrea Garzia ♦

♦ Fondazione Ugo Bordoni

#### **Sommario**

A livello mondiale, l'evoluzione delle reti wireless coinvolge in modo sinergico sia i sistemi terrestri tradizionali che le nuove reti non terrestri e l'interoperabilità e l'eventuale integrazione tra le diverse tipologie di rete rappresenta un elemento chiave per l'erogazione dei servizi previsti dai futuri sistemi di comunicazione basati sulla tecnologia 6G. Con la crescente domanda di spettro la condivisione e la coesistenza delle risorse frequenziali inter-sistema, e tra diverse applicazioni di radiocomunicazione, sta diventando una condizione sempre più diffusa. In questo articolo viene analizzata la condivisione delle risorse frequenziali nella banda 27.5-29.5 GHz tra i sistemi terrestri del servizio fisso (FS) e del sistema fisso satellitare (FSS). In particolare, nel lavoro presentato viene illustrata la metodologia per la valutazione delle condizioni di coesistenza tra i sistemi FS e FSS e vengono derivati i requisiti tecnici per la condivisione dello spettro nella banda 27.5-29.5 GHz tra il servizio fisso terrestre operante tramite collegamenti punto-multipunto e le stazioni di terra del servizio fisso satellitare. La metodologia che viene utilizzata nell'analisi per valutare le condizioni di coesistenza è generale e può essere facilmente estesa e utilizzata per lo studio di altri scenari di condivisione dello spettro, sia tra reti terrestri che tra reti terrestri e non terrestri.

#### **Abstract**

Globally, the evolution of wireless networks synergistically involves both traditional terrestrial systems and new non-terrestrial networks. The interoperability and possible integration between different types of networks represents a key element for the provision of services foreseen by future communication systems based on 6G technology. With the increasing

demand for spectrum, the inter-system sharing of frequency resources and between different radiocommunication applications is becoming an increasingly widespread condition.

This article analyzes the sharing of frequency resources in the 27.5–29.5 GHz band between terrestrial systems of the Fixed Service (FS) and the Fixed Satellite Service (FSS).

Specifically, the presented work illustrates the methodology for evaluating the coexistence conditions between FS and FSS systems. Technical conditions are derived for spectrum sharing in the 27.5–29.5 GHz band between the terrestrial Fixed Service, operating via point-to-multipoint links, and the earth stations of the Fixed Satellite Service. The methodology used in the analysis to evaluate the coexistence conditions is general and can be easily extended and used for the study of other spectrum sharing scenarios, both between terrestrial networks and between terrestrial and non-terrestrial networks.

### **Keyword**

Spectrum sharing, terrestrial, satellite, sharing conditions.

## **1 - Introduzione**

Per soddisfare i requisiti in termini di copertura, capacità ed esperienza d'utente delle differenti applicazioni 6G emergenti e dei nuovi casi d'uso e scenari di utilizzo, l'interoperabilità tra reti terrestri e non terrestri rappresenta un elemento sempre più importante. L'evoluzione congiunta e l'interoperabilità tra le reti terrestri IMT e non IMT (inclusi i sistemi RLAN e broadcast) e le reti non terrestri, inclusi i sistemi di comunicazione satellitare, gli HIBS (stazioni di piattaforma ad alta quota come stazioni base IMT) e i sistemi aerei senza pilota (UAS), sono considerati elementi chiave per fornire i servizi previsti dalle future reti 6G.

Anche l'RSPG report sulla visione strategica per la futura tecnologia 6G [1], in cui identifica le esigenze di spettro per facilitare il lancio iniziale e l'operatività delle reti/servizi 6G a partire dal 2030, riconosce che il 6G dovrebbe basarsi sull'evoluzione congiunta e sull'interoperabilità

delle reti terrestri e non terrestri per sfruttare le caratteristiche più vantaggiose dei sistemi non terrestri, in particolare satellitari e dei sistemi terrestri.

Nel panorama delle reti non terrestri, le comunicazioni satellitari stanno vivendo una rapida evoluzione, spinta sia dal progresso tecnologico sia dal numero crescente di reti satellitari che dalla fornitura di nuovi servizi anche attraverso nuovi paradigmi di comunicazione.

La componente satellitare del 6G si baserà su un'ampia varietà di soluzioni satellitari, operanti non solo nelle costellazioni in Orbita Terrestre Bassa (LEO), ma anche in Orbita Terrestre Media (MEO) e in Orbita Terrestre Geostazionaria (GEO), sia come piattaforme autonome che in modalità combinate.

L'agenda della Conferenza Mondiale delle Radiocomunicazioni 2027 (WRC-27) ha identificato 19 punti da trattare per la WRC-27, 16 dei quali riguardano i servizi satellitari che includono servizi come il Fisso-Satellite (FSS), Mobile-Satellite (MSS) e servizi scientifici spaziali.

I servizi forniti dalle comunicazioni Direct-to-Device (D2D) stanno conquistando sempre più l'interesse internazionale. Le comunicazioni D2D sono pensate per estendere la connettività mobile alle aree remote o scarsamente servite, consentendo agli smartphone di connettersi direttamente ai satelliti, nelle bande di frequenza MSS o MFCN. Il punto 1.13 dell'agenda della WRC-27 [2] prevede di considerare studi su possibili nuove allocazioni al servizio mobile-satellite per la connettività diretta tra stazioni spaziali e apparecchiature utente IMT per integrare la copertura della rete IMT terrestre considerando le bande IMT fino a 2.7 GHz.

A novembre 2025, la Commissione Europea ha conferito alla CEPT il mandato che riguarda lo svolgimento degli studi di fattibilità operativa, coesistenza e compatibilità considerando l'uso delle bande di frequenza armonizzate a livello UE per sistemi IMT, per sistemi satellitari che forniscano connettività D2D-IMT, garantendo la protezione degli usi esistenti.

Anche a livello nazionale sono state svolte azioni per promuovere e regolare lo sviluppo delle reti satellitari sul territorio nazionale. Lo scorso giugno è stato infatti approvato il disegno di legge concernente le "Disposizioni in materia di economia dello spazio", definendo un nuovo e organico quadro regolamentare per l'accesso e lo svolgimento delle attività spaziali

prevedendo anche iniziative per l'uso efficiente dello spettro radioelettrico per comunicazioni via satellite.

La delibera 426/21/CONS [3] nell'ambito del parere al Ministero dello Sviluppo Economico (MISE), sulle condizioni regolamentari per l'autorizzazione della proroga della durata dei diritti d'uso per le reti FS WLL (Wireless Local Loop) nella banda 27.5-29.5 GHz (la cosiddetta banda 28 GHz), definisce le procedure di coordinamento tra le stazioni di terra satellitari FSS e le stazioni del servizio fisso FS. La banda 28 GHz fa parte della banda Ka (18-40 GHz): l'espansione dei sistemi satellitari sia GSO che NGSO in questa gamma di frequenze sia in Europa che a livello nazionale sta rendendo sempre più concreta la coesistenza delle reti terrestri e non terrestri in questa banda di frequenza e quindi sempre più importante lo studio e la valutazione delle condizioni tecniche per la condivisione dello spettro su base di non interferenza tra sistemi terrestri e non terrestri operanti nella banda.

In questo articolo, viene analizzata la coesistenza tra reti terrestri e non terrestri nella banda a 28 GHz.

## **2 – Condivisione dello spettro nella banda di frequenza 28 GHz**

La banda a 28 GHz è assegnata su base co-primaria, come definito nell'articolo 5 del Regolamento Radio dell'Unione Internazionale delle Telecomunicazioni (ITU) [9] al servizio fisso (FS), al servizio fisso via satellite Terra-spazio (FSS E-s) e al servizio mobile (MS). In Europa, il quadro armonizzato per l'uso della banda di frequenza a 28 GHz considera solo le stazioni terrestri FS e FSS E-s non coordinate (ovvero la direzione di uplink), come stabilito nella Decisione ECC (05)01 [4]. Inoltre, la Tabella di Allocazione Europea (ECA), il Report ERC 025 [5], ha identificato la banda di frequenza a 28 GHz per i servizi co-primari FS e FSS E-s. L'ECA non prevede alcuna allocazione al servizio mobile, pertanto in Europa non è disponibile per la telefonia mobile o il 5G.

La Decisione ECC (05)01 fornisce un quadro normativo per l'utilizzo della banda di frequenza a 28 GHz attraverso la designazione di sotto-intervalli di frequenza specifici per le stazioni terrestri FS e FSS non coordinate. Nonostante la segmentazione di banda definita, la Decisione

ECC (05)01 sottolinea che "le stazioni terrestri FSS coordinate possono comunque utilizzare l'intera banda 27.5-29.5 GHz, seguendo procedure di coordinamento consolidate".

In questo contesto, abbiamo condotto un'indagine per valutare le condizioni tecniche di coesistenza tra stazioni terrestri FS e FSS coordinate (NGSO) in grado di operare su base co-canale nella banda di frequenza 27.5-29.5 GHz. In particolare, in Italia il servizio FSS opera tramite la tecnologia WLL con collegamenti Punto-Punto (P-P) e Punto-Multi-Punto (P-MP). Questo scenario di coesistenza è di notevole interesse perché la connettività spaziale diventerà sempre più importante, con un numero sempre crescente di operatori satellitari che offrono una gamma di servizi nello spettro dei 28 GHz utilizzando sia gateway di stazioni terrestri NGSO che gateway GSO.

Per garantire l'assenza di interferenza, è necessario studiare quali siano le condizioni di coesistenza che garantiscono la protezione reciproca di entrambi i sistemi. In questo lavoro è stata applicata una metodologia sviluppata per valutare le condizioni di coesistenza che garantiscono il soddisfacimento dei requisiti di protezione dei sistemi FS sia Punto-Punto (P-P) che Punto-Multi-Punto (P-MP).

In [6], sono stati identificati gli scenari di coesistenza tra le stazioni di terra FSS e i links FS operanti nella banda 27.5–29.5 GHz e sono state valutate le condizioni di coesistenza tra il sistema FSS E-S e il sistema FS WLL P-P. In [7], la metodologia già sviluppata per lo studio di coesistenza tra sistemi FSS E-S (GSO) e sistemi FS WLL P-P è stata estesa e adattata allo scenario di coesistenza tra i sistemi FSS E-S (GSO) e i sistemi FS WLL P-MP. In questo articolo, la stessa metodologia è stata applicata alla valutazione della coesistenza tra i sistemi FSS E-S (NGSO) e i sistemi FS P-MP.

### **3- Scenario di coesistenza, metodologia e parametri di simulazione**

#### **3.1 Scenario di coesistenza e metodologia**

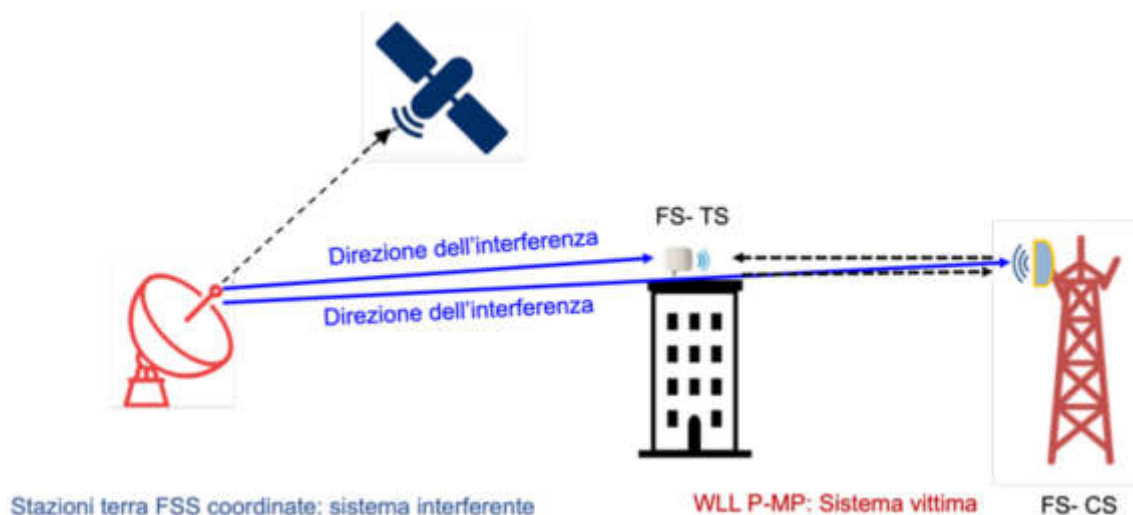
Lo scenario di coesistenza che verrà analizzato in questo lavoro è mostrato in Figura 1 e prevede la valutazione delle condizioni di coesistenza tra i sistemi FSS E-S (NGSO) che

rappresenta il sistema interferente e i sistemi FS P-MP che rappresenta il sistema vittima per il quale deve essere garantita la protezione.

Le stazioni di terra del servizio FSS E-S (NGSO) si suppone operino, per le valutazioni del segnale interferente, con il diagramma verticale puntato con il massimo guadagno verso l'elevazione minima e che questo diagramma venga riprodotto per ogni angolo di azimut.

I sistemi WLL P-MP permettono la connessione di una stazione centrale (CS) a diverse stazioni terminali (TS), consentendo così di fornire servizi wireless a banda larga. Nell'analisi di coesistenza tra la stazione di terra FSS e il collegamento P-MP, deve essere garantita la protezione sia della CS che della TS. Le condizioni di coesistenza finali tengono conto dei risultati congiunti delle due analisi, considerando che la protezione della TS deve essere valutata su tutte le posizioni (pixel) dell'area di copertura del servizio FS in cui si ipotizza la presenza di un ricevitore P-MP che punta verso la CS servente. Nelle analisi svolte è stata ipotizzata:

1. una distanza tra la CS e la stazione di terra FSS di 3 km
2. un'area di copertura del link P-MP di raggio 4.5 km segmentata in pixel 100 m x 100 m.



*Figura 1* Scenario di coesistenza: FSS E-S sistema interferente e FS P-MP sistema vittima

La metodologia adottata per valutare l'interferenza sui collegamenti P-MP FS dovuta alle stazioni terrestri FSS si basa sull'approccio Minimum Coupling Loss (MCL) [8-9], tenendo conto del criterio di protezione per i sistemi FS a lungo termine basato sul rapporto I/N (rapporto interferenza/rumore). Il rapporto I/N in dB viene valutato con la seguente formula:

$$I/N (\Delta f, d, \vartheta_1, \vartheta_2) = P_t + A_{tt}(\Delta f) + G_t(\vartheta_1) + G_r(\vartheta_2) - PL(d) - N$$

Nella formula,  $P_t$  rappresenta la potenza trasmessa (dBm) dall'interferente che nello scenario analizzato è rappresentato dalla stazione terrestre FSS E-S;  $\Delta f$  è la separazione di frequenza (in MHz) tra la frequenza portante dell'interferente e quella del sistema vittima;  $A_{tt}(\Delta f)$  è l'attenuazione dovuta alla separazione frequenziale dell'interferente e dell'interferito che deve essere calcolata in base alla larghezza di banda dei sistemi;  $G_t(\vartheta_1)$  e  $G_r(\vartheta_2)$  sono, rispettivamente, i guadagni (dBi) dell'antenna interferente FSS all'angolo  $\vartheta_1$  e dell'antenna FS WLL CS/TS vittima all'angolo  $\vartheta_2$  tra il sito del sistema interferente e il sito del sistema vittima;  $PL(d)$  è l'attenuazione della perdita di percorso (dB) dovuta alla propagazione lungo la distanza  $d$  (km);  $N$  è il livello di rumore (dBm) del ricevitore vittima. In questo articolo è stata studiata l'identificazione delle condizioni tecniche per garantire la coesistenza tra i sistemi FSS E-S (NGSO) e FS WLL P-MP, analizzando lo scenario di coesistenza co-canale (ovvero,  $A_{tt}(\Delta f) = 0$  dB).

### 3.2 Parametri di simulazione

Le caratteristiche tecniche del trasmettitore FSS, del ricevitore FS CS e TS utilizzati nelle simulazioni sono riportate rispettivamente nella Tabella 1, nella Tabella 2 e nella Tabella 3.

**Tabella 1.** Parametri di simulazione del sistema FSS E-S

<b>Caratteristiche dalla stazione FSS E-S nella banda 27.5-29.5 GHz</b>	
Guadagno antenna	52.44 dB
Altezza antenna	2 m
Diametro dell'antenna	1.8 m
Elevazione dell'antenna	10°-20°-30°-40°
Larghezza di banda	320 MHz
Potenza trasmessa	7.2 dBW

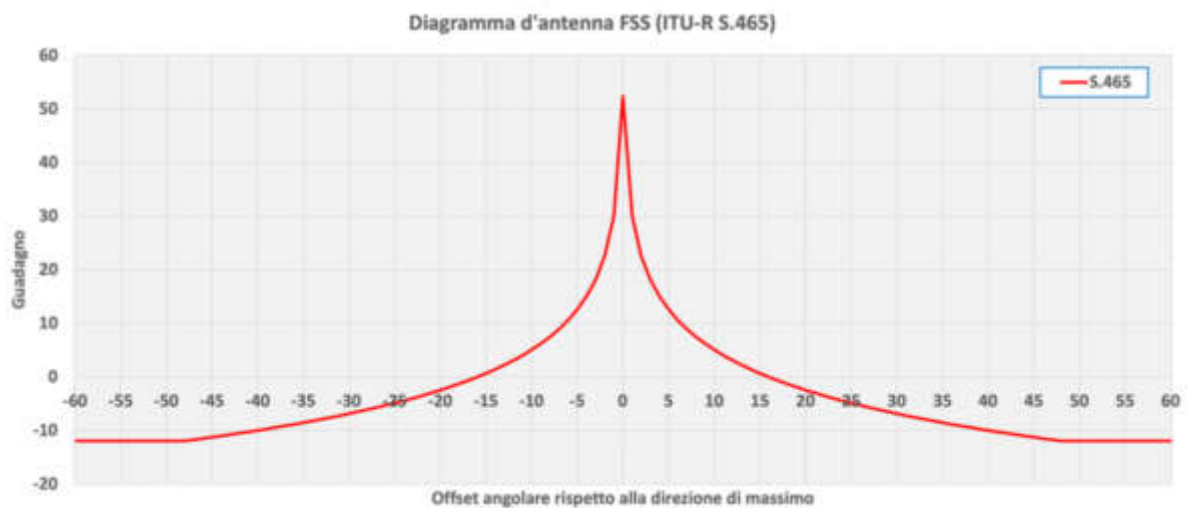
**Tabella 2.** Parametri di simulazione del sistema FS CS

<b>Caratteristiche dalla stazione FS CS nella banda 27.5-29.5 GHz</b>	
Guadagno antenna	27 dB
Altezza antenna	15 m
Elevazione dell'antenna	0°-2.5°
Azimut dell'antenna	0°-5°-10°-15°-180°
Larghezza di banda	28 MHz
Figura di rumore	6.5 dB
I/N max	-10 dB [10]

**Tabella 3.** Parametri di simulazione del sistema FS TS

<b>Caratteristiche dalla stazione FS TS nella banda 27.5-29.5 GHz</b>	
Guadagno antenna	42 dB
Altezza antenna	15 m
Larghezza di banda	28 MHz
Figura di rumore	6.5 dB
I/N max	-10 dB [10]

Il diagramma di antenna della stazione di terra trasmittente FSS segue la Raccomandazione ITU-R S.465-6 [11] ed è mostrato in Figura 2.



*Figura 2– Diagramma d'antenna della stazione di terra FSS trasmittente*

La Figura 3 mostra il diagramma di antenna del FS TS ricevente che segue la Raccomandazione ITU-R F.699-8 [12] e la Figura 4 mostra il diagramma di antenna del FS CS ricevente che segue la Raccomandazione ITU-R F.1336-5 [13].

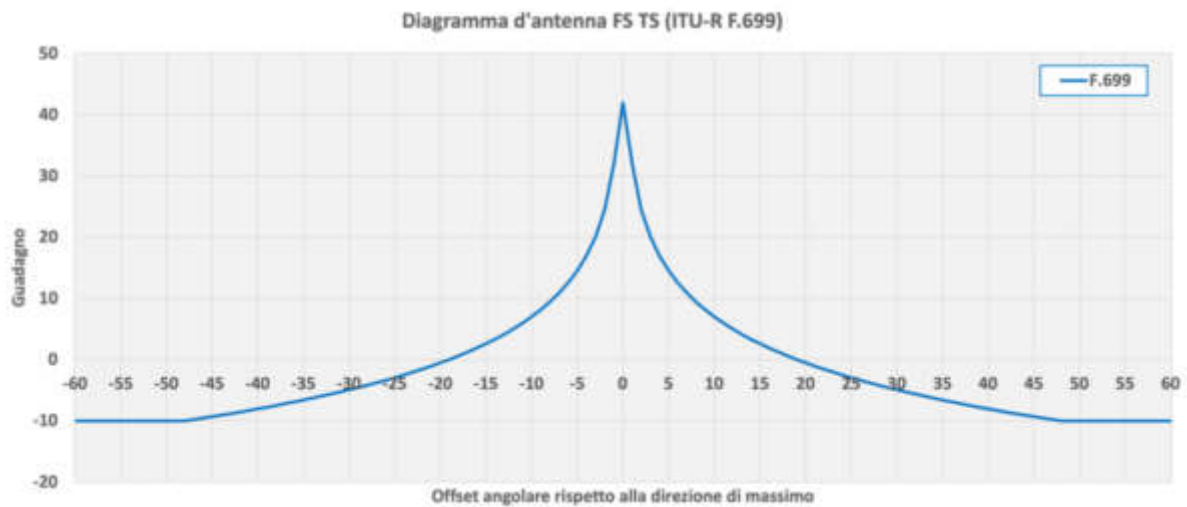


Figura 3– Diagramma d'antenna della stazione FS TS ricevente

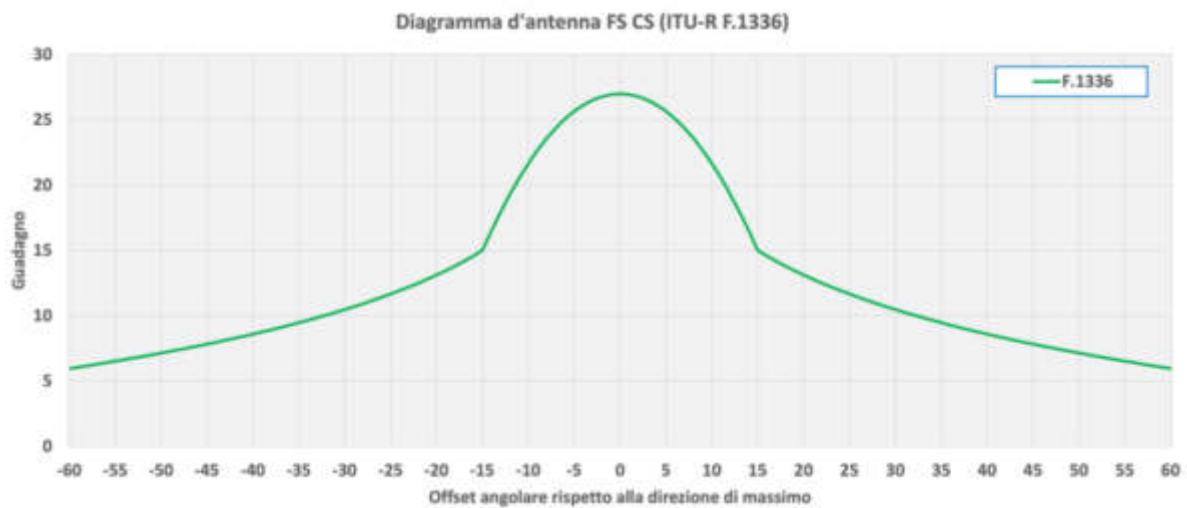


Figura 4– Diagramma d'antenna della stazione FS CS ricevente

Il modello di propagazione utilizzato nelle simulazioni si basa sulla Raccomandazione ITU-R P.452-17 [14] al 20% del tempo (ovvero, l'interferenza è caratterizzata come la potenza di interferenza superata del 20% del tempo all'ingresso del ricevitore vittima) che rappresenta la percentuale di tempo per la protezione del sistema FS definita in [10]. Tale raccomandazione è utilizzata anche per la valutazione dell'effetto del clutter ambientale che viene caratterizzato tramite un modello definito in [14]. Nell'analisi svolta, la stazione di terra FSS e il link P-MP sono stati considerati installati in un ambiente reale, in cui la stazione FSS è installata in ambiente rurale e la CS del servizio FS in ambiente urbano denso. Questo modello

di propagazione è comunemente utilizzato a livello internazionale per studi di coesistenza (ad esempio, [9, 15, 16]). Per ciascun ricevitore CS e TS, viene valutato il rapporto I/N e il valore ottenuto viene confrontato con la soglia di protezione (I/N max). Questa metodologia è solitamente utilizzata a livello ITU e CEPT per la valutazione delle condizioni tecniche di coesistenza tra sistemi diversi. Per effettuare le analisi di simulazione, questa metodologia è stata implementata nel tool per le valutazioni di coesistenza proprietario della Fondazione Ugo Bordoni (FUB) che viene utilizzato in molti progetti, sia a livello nazionale che internazionale, commissionati alla FUB dall'Amministrazione italiana, in particolare dal Ministero delle Imprese e del Made in Italy (MIMIT).

#### **4 – Risultati dell'analisi di coesistenza**

I risultati delle analisi presentati in questa sezione valutano l'impatto della trasmissione FSS sui ricevitori FS (CS e TS). I risultati degli studi sono presentati come segue:

- A. Valutazione dell'impatto interferenziale del sistema FSS sulla CS al variare dell'offset dell'azimut tra la CS e la stazione di terra FSS (0°-5°-10°-15°-180°), dell'elevazione della CS (0° e 2.5°) e della stazione di terra FSS.
- B. Valutazione dell'impatto interferenziale del sistema FSS sulle TS al variare dell'elevazione della stazione di terra FSS.

##### **4.1 Analisi dell'impatto interferenziale sulla CS al variare dell'offset dell'azimut tra CS e stazione di terra FSS e dell'elevazione della CS**

Nella Tabella 4 e nella Tabella 5 viene mostrato l'impatto interferenziale della stazione di terra FSS in termini di I/N sulla CS del sistema FS al variare dell'offset dell'azimut tra CS e la stazione di terra FSS e considerando un'elevazione per la stazione di terra FSS di 10°, 20°, 30° e 40° e un valore dell'elevazione della CS rispettivamente di 0° e di 2.5°.

**Tabella 4.** I/N valutato alla CS al variare dell'offset dell'azimut tra CS e stazione di terra FSS e dell'elevazione della stazione di terra FSS considerando un'elevazione della CS = 0°

I/N [dB]	Offset azimut CS-FSS				
	0°	5°	10°	15°	180°
Elevazione FSS = 10°	-26.9	-28.2	-32.1	-38.4	-59.1
Elevazione FSS = 20°	-35.5	-36.8	-40.7	-46.9	-67.7
Elevazione FSS = 30°	-40.3	-41.5	-45.5	-51.7	-72.5
Elevazione FSS = 40°	-43.5	-44.8	-48.7	-55	-75.7

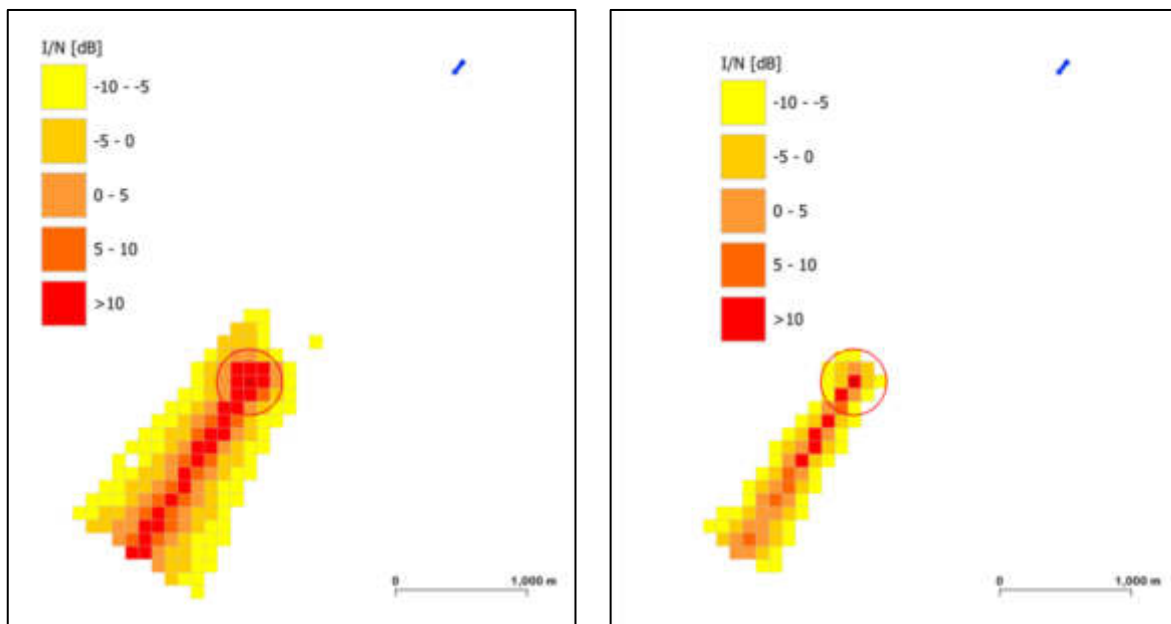
**Tabella 5.** I/N valutato alla CS al variare dell'offset dell'azimut tra CS e stazione di terra FSS e dell'elevazione della stazione di terra FSS considerando un'elevazione della CS = 2.5°

I/N [dB]	Offset azimut CS-FSS				
	0°	5°	10°	15°	180°
Elevazione FSS = 10°	-30.4	-31.6	-35.6	-39.2	-59
Elevazione FSS = 20°	-38.9	-40.3	-44.2	-47.8	-67.6
Elevazione FSS = 30°	-43.7	-45	-48.9	-52.5	-72.4
Elevazione FSS = 30°	-47	-48.3	-52.2	-55.8	-75.7

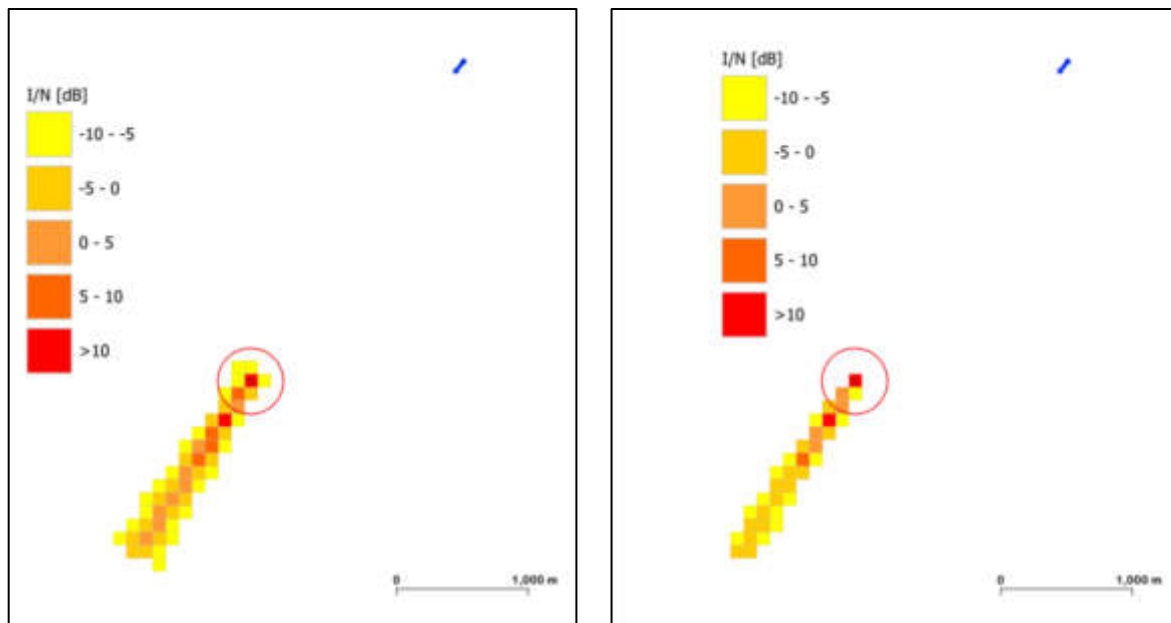
Come si può vedere dalle tabelle, l'impatto interferenziale sulle CS dovuto alla stazione interferente FSS è molto inferiore al valore di I/N di protezione per il servizio FS (I/N = -10 dB) in tutte le configurazioni considerate.

## 4.2 Analisi dell'impatto interferenziale sulle TS al variare dell'elevazione della stazione di terra FSS

La Figura 5 e la Figura 6 mostrano l'impatto interferenziale sulle TS distribuite all'interno dell'area di copertura della CS al variare dell'elevazione della stazione FSS considerando un offset dell'azimut tra CS e stazione di terra FSS pari a  $0^\circ$ . Nella Figura 5 e nella Figura 6, il cerchio rosso indica dove si trova la stazione di terra FSS e la freccia blu dove è installata la CS.



**Figura 5** Impatto interferenziale dovuto alla stazione di terra FSS sulle TS distribuite sull'area di copertura della CS considerando elevazione FSS =  $10^\circ$  (immagine a sinistra) ed elevazione FSS =  $20^\circ$  (immagine a destra)



**Figura 6** Impatto interferenziale dovuto alla stazione di terra FSS sulle TS distribuite sull'area di copertura della CS considerando elevazione FSS = 30° (immagine a sinistra) ed elevazione FSS = 40° (immagine a destra)

Nella Tabella 6 viene mostrata la percentuale di TS interferiti per un settore FS al variare dell'elevazione della stazione di terra FSS e dell'offset dell'azimut tra CS e stazione di terra FSS e considerando l'elevazione della CS pari a 0°.

**Tabella 6.** I/N valutato alla CS e percentuale di TS interferiti per un settore FS al variare dell'elevazione FSS e dell'offset dell'azimut tra CS e stazione di terra FSS.

Offset azimut CS-FSS	Elevazione FSS	I/N CS	% TS interferiti
0°	10°	-26.9 dB	<b>65.2 %</b>
5°	10°	-28.2 dB	<b>50.2 %</b>
10°	10°	-32.1 dB	<b>27.8 %</b>
15°	10°	-38.4 dB	<b>4.9 %</b>
180°	10°	-59.1 dB	<b>12.7 %</b>
0°	20°	-35.5 dB	<b>30.7 %</b>

<b>Offset azimut CS-FSS</b>	<b>Elevazione FSS</b>	<b>I/N CS</b>	<b>% TS interferiti</b>
5°	20°	-36.8 dB	<b>26.6 %</b>
10°	20°	-40.7 dB	<b>5.6 %</b>
15°	20°	-46.9 dB	<b>0 %</b>
180°	20°	-67.7 dB	<b>0 %</b>
0°	30°	-40.3 dB	<b>19.5 %</b>
5°	30°	-41.5 dB	<b>19.5 %</b>
10°	30°	-45.5 dB	<b>0.4 %</b>
15°	30°	-51.7 dB	<b>0 %</b>
180°	30°	-72.5 dB	<b>0 %</b>
0°	40°	-43.5 dB	<b>12.7 %</b>
5°	40°	-44.8 dB	<b>12.7 %</b>
10°	40°	-48.7 dB	<b>0 %</b>
15°	40°	-55 dB	<b>0 %</b>
180°	40°	-75.7 dB	<b>0 %</b>

Come mostrato nella Tabella 6, la percentuale di TS interferite nell'area di copertura di un settore FS diminuisce aumentando l'elevazione della stazione di terra FSS e aumentando l'offset dell'azimut tra stazione di terra FSS e CS FS. Nel caso di elevazione della stazione di terra FSS pari a 10° e offset pari a 180°, il numero di TS interferiti aumenta rispetto agli offset compresi tra 0° e 15° in quanto in questa configurazione l'elevazione della stazione FSS è molto bassa e le TS presentano il puntamento diretto verso la stazione FSS.

## **5 – Conclusioni**

Questo articolo analizza la coesistenza tra i sistemi FSS NGSO E-S e i sistemi FS P-MP operanti nella banda 27.5-29.5 GHz. Per valutare la coesistenza tra una stazione di terra FSS e un collegamento FS P-MP il criterio di protezione deve essere soddisfatto sia al ricevitore CS che ai TS operanti nell'area di servizio della CS FS. Sono stati mostrati alcuni esempi dei risultati ottenuti con il tool di condivisione FUB, considerando l'effetto della trasmissione del sistema FSS sui ricevitori CS e TS del servizio fisso.

L'analisi dell'impatto interferenziale legato alla variazione delle configurazioni dei sistemi FSS ed FS consente di comprendere quanto il ricevitore FS sia sensibile alle variazioni dei parametri di configurazione del servizio fisso satellitare al fine, eventualmente, di ottimizzare i parametri di deployment per facilitare la coesistenza tra i due sistemi.

I risultati mostrano che per le configurazioni considerate non emergono problemi di coesistenza con la CS. A seconda delle configurazioni considerate di elevazione della stazione FSS ed offset tra la stazione FSS e la stazione FS, il numero di TS interferiti diminuisce aumentando l'elevazione della stazione di terra FSS e aumentando l'offset dell'azimut tra stazione di terra FSS e CS FS. Nel caso di elevazione della stazione di terra FSS pari a 10° e offset pari a 180°, il numero di TS interferiti aumenta rispetto agli offset compresi tra 0° e 15° in quanto in questa configurazione l'elevazione della stazione FSS è molto bassa e le TS presentano il puntamento diretto verso la stazione FSS. Ciò è dovuto, inoltre, al diagramma di antenna delle TS che risulta essere molto direttivo. L'analisi condotta mira a fornire indicazioni generali utili agli operatori e alle amministrazioni per coordinare lo sviluppo delle reti. Situazioni simili in termini di parametri dei sistemi ma riferite a differenti scenari possono portare a risultati anche molto diversi in funzione dell'orografia presente.

## **9 - Bibliografia**

- [1] RSPG Report, “6G Strategic vision”, February 2025
- [2] <https://www.itu.int/en/ITU-R/study-groups/rcpm/Pages/wrc-27-studies.aspx>
- [3] Delibera 426/21/CONS, “Parere al Ministero dello sviluppo economico sulle condizioni regolamentari per l’autorizzazione della proroga della durata dei diritti d’uso esistenti per reti radio a larga banda WLL nella banda 27.5-29.5 GHz e valutazione delle istanze presentate”
- [4] ECC Decision(05)01, “The use of the band 27.5-29.5 GHz by the Fixed Service and uncoordinated Earth stations of the Fixed-Satellite Service (Earth-to-space)”, March 2013
- [5] ERC report 025, “THE EUROPEAN TABLE OF FREQUENCY ALLOCATIONS AND APPLICATIONS IN THE FREQUENCY RANGE 8.3 kHz to 3000 GHz (ECA TABLE)”, November 2025
- [6] Petrini, V.; Carciofi, C.; Faccioli, M.; Neri, A. Coexistence Analysis Between Terrestrial and Non Terrestrial Networks in the 27.5–29.5 GHz Frequency Band; European Wireless : 2023 (<https://ieeexplore.ieee.org/document/10461443>)
- [7] Petrini, V.; Carciofi, C.; Faccioli, “Spectrum Sharing Opportunities for 6G Terrestrial and Non-Terrestrial Networks”, Engineering proceedings, 2025
- [8] ERC Report 101, “A comparison of the Minimum Coupling Loss method, Enhanced Minimum Coupling Loss and the Monte-Carlo simulation”, May 1999. (<https://docdb.cept.org/download/2205>)
- [9] ECC Report 304, “Advanced technologies for fixed GSO FSS Earth Stations in the 27.5-29.5 GHz band”, October 2019. (<https://docdb.cept.org/download/1401>)
- [10] Recommendation ITU-R F.758-7 (11/2019). System Parameters and Considerations in the Development of Criteria for Sharing or Compatibility Between Digital Fixed Wireless Systems in the Fixed Service and Systems in Other Services and Other Sources of Interference; ITU Publications: Geneva, Switzerland, 2019.
- [11] Recommendation ITU-R S.465-6 (01/2010). Reference Radiation Pattern for Earth Station Antennas in the Fixed-Satellite Service for Use in Coordination and Interference Assessment in the Frequency Range from 2 to 31 GHz; ITU Publications: Geneva, Switzerland, 2010.

[12] Recommendation ITU-R F.699-8 (01/2018). In Reference Radiation Patterns for Fixed Wireless System Antennas for Use in Coordination Studies and Interference Assessment in the Frequency Range from 100 MHz to 86 GHz; ITU Publications: Geneva, Switzerland, 2018.

[13] Recommendation ITU-R F.1336-5 (01/2019). Reference Radiation Patterns of Omnidirectional, Sectoral and Other Antennas for the Fixed and Mobile Services for Use in Sharing Studies in the Frequency Range from 400 MHz to About 70 GHz; ITU Publications: Geneva, Switzerland, 2019.

[14] Recommendation ITU-R P.452-17 (07/2015). Prediction Procedure for the Evaluation of Interference Between Stations on the Surface of the Earth at Frequencies Above About 0.1 GHz; ITU Publications: Geneva, Switzerland, 2015.

[15] ECC Report 271, "Compatibility and sharing studies related to NGSO satellite systems operating in the FSS bands 10.7-12.75 GHz (space-to-Earth) and 14-14.5 GHz (Earth-to-space)", approved January 2018, amended April 2021.

[16] ECC Report 303 "Guidance to administrations for Coexistence between 5G and Fixed Links in the 26 GHz band ("Toolbox")".

## Gli standard ISO a supporto dell'AI ACT

### *ISO standards supporting AI ACT*

Fabrizio Cirilli<sup>◆</sup>, Massimiliano Perrone<sup>◆</sup>, Luca Tufarelli<sup>□</sup>, Maria Lilia La Porta<sup>□</sup>

◆ PDCA Srl

□ Avvocato – Studio Ristuccia & Tufarelli

#### **Sommario**

Le IA hanno aperto fronti inesplorati e lanciato l'umanità verso nuovi traguardi, impensabili fino a un decennio fa. Questa accelerazione richiede però un adeguamento dei nostri modi di fare, pensare e vivere le nuove tecnologie e in particolare ciò che le IA possono (o non possono) fare.

L'AI Act è un primo tentativo Europeo di regolare la materia, i progetti di armonizzazione in corso potranno aiutare a migliorare e rendere operativo un quadro di riferimento.

In questo contesto assumono un ruolo particolare gli standard ISO che possono aiutare le organizzazioni ad impostare modelli organizzativi atti a garantire il rispetto dei regolamenti, delle direttive e delle leggi applicabili in un insieme di processi correlati.

Di quali norme ISO parliamo? Come organizzarle? In quale sequenza e perché?

Questo è ciò che affronteremo in questo articolo, mantenendo sempre fede alle richieste dell'AI Act.

Ulteriormente, durante la redazione del presente articolo, è entrata in vigore la legge 132 del 2025. Tale provvedimento normativo ha reso l'Italia il primo paese europeo con una normativa *ad hoc* sul tema IA. Infine verranno anche approfonditi i rapporti tra l'AI Act e gli standard ISO di riferimento.

#### **Abstract**

AI has opened unexplored frontiers and launched humanity towards new goals, unthinkable a decade ago. However, this acceleration requires an adaptation of our ways of doing, thinking and experiencing new technologies and in particular what AI can (or cannot) do.

The AI Act is the first European attempt to regulate the matter; the ongoing harmonization projects may help to improve and operate a framework.

In this context, ISO standards play a special role. They can help organizations set up organizational models to ensure compliance with regulations, directives and applicable laws in a set of related processes.

Which ISO standards are we talking about? How to organize them? In what sequence and why?

This is what we will address in this article, always keeping to the requirements of the AI Act.

Furthermore, while this article was being drafted, the draft law on artificial intelligence (DDL 1146 recepito con legge 132/2025) was also approved, making Italy the first European country with internal legislation on the subject. What are the links with the AI Act and the relevant ISO standards? Particular attention will be paid to this topic, with an initial comment.

### **Keyword**

AI Act, Standard ISO, ISO/IEC 42001

### **Introduzione**

Il rapido sviluppo delle IA e delle loro applicazioni, unito all'entrata in vigore dell'AI Act e della legge italiana in materia di IA hanno avviato in tutto il mondo produttivo lunghe e articolate analisi per la comprensione del quadro normativo di riferimento e delle implicazioni pratiche.

La pubblicazione della ISO/IEC 42001:2023 ha ulteriormente complicato il quadro normativo in materia, per quanto si tratti di una normativa volontaria.

Lungi dal voler risolvere il tema e dal dare una soluzione confezionata e definitiva sul tema, si proveranno a descrivere le esperienze pratiche affrontate negli anni, sperando possano essere utili al lettore per un primo orientamento all'interno di un contesto normativo (come si vedrà, volontario e cogente) non proprio di facile comprensione.

### **Obblighi introdotti dall'AI Act**

Il Regolamento UE 2024/1689 - Artificial Intelligence Act (di seguito "AI Act") ha delineato il quadro normativo europeo in materia di intelligenza artificiale, con l'obiettivo principale di stabilire un sistema di obblighi con particolare riferimento ai sistemi di IA "ad alto rischio".

Tali obblighi sono proporzionati all'impatto potenziale dei sistemi di IA e, secondo l'approccio basato sul rischio che permea l'intero AI Act, sono strutturati rispetto a quattro categorie di rischio: Inaccettabile, Alto, Limitato e Minimo. Il rischio secondo l'AI Act deve essere valutato rispetto ai diritti fondamentali e alle libertà delle persone fisiche, con particolare attenzione ai principi etici e alla funzione antropocentrica dell'IA.

Il rischio Inaccettabile riguarda Pratiche di IA espressamente vietate ai sensi dell'art. 5), tra le quali rientrano i sistemi di manipolazione cognitivo-comportamentale, la sorveglianza biometrica in tempo reale in spazi pubblici e la creazione di "crediti sociali" basati su comportamenti personali.

I sistemi identificati ad Alto rischio sono disciplinati dall'art. 6 e dall'Allegato III all'AI Act e costituiscono il fulcro del sistema di conformità alla normativa e agli obblighi da essa prescritti.

Per i sistemi di IA ad Alto rischio devono essere rispettati i seguenti obblighi:

- a) deve essere istituito, attuato, documentato e mantenuto un sistema di gestione dei rischi (art. 9);
- b) deve essere garantita la qualità, pertinenza e rappresentatività dei dati (art. 10);
- c) deve essere predisposta documentazione tecnica completa (art. 11),;
- d) devono essere registrati i log e garantita la tracciabilità (art. 12);
- e) devono essere sviluppati in modo da garantire la trasparenza (art. 13);
- f) devono essere accompagnati da procedure di sorveglianza umana volte a garantire che l'intervento umano possa prevenire o correggere comportamenti dannosi o illegittimi (art. 14);
- g) devono essere progettati e sviluppati in modo da garantire robustezza, accuratezza e sicurezza informatica, affinché i sistemi risultino affidabili e resistenti a malfunzionamenti o attacchi esterni (art. 15);
- h) deve essere previsto un monitoraggio continuo post-commercializzazione del sistema di IA (art. 72).

A questi obblighi si aggiungono ulteriori obblighi previsti specificatamente per i fornitori e per i deployer di un sistema di IA ad alto rischio e in particolare:

- I. i fornitori devono:
  - a) implementare e mantenere un sistema di gestione della qualità proporzionato alla natura e alla complessità del sistema di IA (art. 17);
  - b) conservare e rendere disponibili alle autorità competenti: la documentazione tecnica, la dichiarazione di conformità e i registri delle versioni e modifiche del sistema (art. 18);
  - c) conservare i log generati automaticamente dal sistema (art. 19);
  - d) cooperare con le autorità competenti (art. 21).
- II. i deployer devono (art. 26):
  - a) usare il sistema in conformità con le istruzioni fornite dal fornitore;
  - b) garantire la supervisione umana e il controllo sui dati di input;
  - c) monitorare il funzionamento del sistema;
  - d) notificare incidenti seri o malfunzionamenti.

In materia di trasparenza, sono previsti obblighi orizzontali (artt. 50 - 52): gli utenti devono essere informati quando interagiscono con un sistema d'intelligenza artificiale e i contenuti generati o manipolati devono essere chiaramente identificabili come artificiali.

Alcuni obblighi specifici sono poi previsti per i sistemi di IA ad uso generale o GPAI (General Purpose AI) con rischio "sistemico" ai sensi degli artt. 52 – 55. Il Fornitore di tali sistemi è tenuto a svolgere valutazioni di sicurezza e test di conformità, valutare e attenuare i possibili rischi sistemici, a notificare incidenti gravi all'AI Office e alle autorità nazionali competenti e a collaborare con le istituzioni europee per garantire la gestione dei rischi transfrontalieri.

Fatto questo breve excursus sui principali obblighi dell'AI Act, per comprendere in che modo uno standard può essere utile nella compliance normativa, è opportuno un confronto con i requisiti della norma ISO/IEC 42001 (requisiti per i sistemi di gestione per l'intelligenza artificiale), mettendo in luce analogie, differenze, punti di forza e limiti.

La ISO/IEC 42001 è uno standard di adozione volontaria che può essere utilizzato al fine di implementare un sistema di gestione della governance per i sistemi di IA.

L'AI Act, come detto, introduce un sistema di norme e obblighi vincolanti in base ai diversi livelli di rischio dei sistemi di IA.

Si tratta di due strumenti che utilizzati in modo complementare possono garantire all'organizzazione di essere conforme ai requisiti e agli obblighi in materia di IA.

Si si riporta qui di seguito una tabella di confronto tra obblighi dell'AI Act e requisiti previsti dallo standard ISO/IEC 42001, divisa in due parti in base al livello di rischio. La prima tra rischio inaccettabile e alto, la seconda tra rischio limitato, minimo e relativo a modelli GPAI.

Tabella di Confronto tra Obblighi dell'AI Act e Requisiti dello Standard ISO/IEC 42001:2023			
Livello di rischio AI Act	Obblighi principali previsti dall'AI Act	Copertura ISO/IEC 42001:2023	Commento operativo
<b>Rischio inaccettabile</b>	Divieto di sistemi che manipolano il comportamento umano, riconoscimento biometrico in tempo reale, social scoring, sfruttamento di vulnerabilità (art. 5).	<b>✗ Non coperto (vedere commento operativo)</b>	La ISO/IEC 42001 è uno standard volontario. Nonostante non presenti riferimenti a norme e leggi, queste fanno parte integrale dei suoi requisiti, come dimostrato dal punto 4.1 con riferimento al contesto esterno per l'individuazione del campo di applicazione
<b>Rischio alto</b>	a) Sistema di gestione del rischio (art. 9)	<b>✓ Pienamente coperto</b>	Punti 6.1 e seguenti (nello specifico anche 6.1.4), 6.2, 8.1, 8.2, 8.3, 8.4. Nei requisiti della ISO/IEC 42001 si richiama anche la valutazione d'impatto in quanto questa, nell'ottica del sistema di gestione, deve guidare la valutazione e poi il trattamento del rischio.





Tabella di Confronto tra Obblighi dell'AI Act e Requisiti dello Standard ISO/IEC 42001:2023			
Livello di rischio AI Act	Obblighi principali previsti dall'AI Act	Copertura ISO/IEC 42001:2023	Commento operativo
	b) qualità dei dati (art. 10)	 <b>Parzialmente coperto</b>	Annex A – A.7.4. La qualità dei dati utilizzati per sviluppare e gestire i sistemi di IA può avere, potenzialmente, un impatto significativo sulla validità dei risultati del sistema di IA. Nonostante l'Art. 10 parli di qualità dei dati, all'interno della ISO/IEC 42001 i punti da attenzionare sono compresi in tutto il controllo A.7.X
	c) documentazione tecnica (art. 11)	 <b>Coperto concettualmente</b>	Oltre al punto 7.5 (relativo alle informazioni documentate, concetto distinto da quello di documentazione), la documentazione tecnica trova la propria sede al punto A.6.2.7 dell'Annex A. La guida per l'implementazione, di cui all'Annex B, copre quanto richiesto dal Regolamento.
	d) tracciabilità e registrazioni log (art. 12)	 <b>Coperto concettualmente</b>	Punto A.6.2.8, il quale fa proprio riferimento alla conservazione dei log di evento per tutto il ciclo di vita del sistema IA (o almeno successivamente al <i>deploy</i> ).
	e) Trasparenza e informazioni all'utente (art. 13)	 <b>Pienamente coperto</b>	Oltre alle comunicazioni di cui al punto 7.4 (parte strutturale della nuova struttura armonizzata delle norme ISO) vi sono anche i controlli relativi






Tabella di Confronto tra Obblighi dell'AI Act e Requisiti dello Standard ISO/IEC 42001:2023			
Livello di rischio AI Act	Obblighi principali previsti dall'AI Act	Copertura ISO/IEC 42001:2023	Commento operativo
			alla comunicazione degli incidenti (A.8.4) e delle comunicazioni alle parti interessate identificate nel contesto (A.8.5).
	f) sorveglianza umana (art. 14)	 <b>Pienamente coperto</b>	Sez. 8.4 – Human oversight and accountability mechanisms. La norma ISO/IEC 42001 copre il concetto di <i>human oversight</i> in più punti norma e controlli. Al di là del punto norma strutturale su ruoli, responsabilità e autorità (5.3 che trova un proprio controllo all'interno dell'Annex A – A.3.2), vi sono anche i controlli A.4.6 sulle risorse umane. Ulteriormente, tutta una serie in cui il concetto di supervisione umana fa parte dell'analisi (A.5.3, A.6.1.3, A.8.2, A.9.3, A.9.4).
	g) robustezza, sicurezza e accuratezza (art. 15)	 <b>Pienamente coperto</b>	Controllo A.6.2.4, ove il concetto di robustezza viene esplicitato. Accuratezza compare all'interno della documentazione tecnica di cui al controllo A.6.2.7 e in quello sullo sviluppo e potenziamento del sistema di IA (A.7.2). Il concetto di sicurezza è trasversale a tutti i controlli.

Tabella di Confronto tra Obblighi dell'AI Act e Requisiti dello Standard ISO/IEC 42001:2023			
Livello di rischio AI Act	Obblighi principali previsti dall'AI Act	Copertura ISO/IEC 42001:2023	Commento operativo
<b>Rischio limitato</b>	Obblighi di trasparenza, quali informare gli utenti quando interagiscono con IA, dichiarare contenuti artificiale, garantire uso corretto (artt. 50–52).	 <b>Parzialmente coperto</b>	Lo standard ISO/IEC 42001 promuove trasparenza e comunicazione etica, ma non impone etichettatura o obblighi di disclosure pubblica. Vi sono due controlli che prendono esplicitamente in carico il concetto: A.7.2 e A.5.4 (relativo questo alla valutazione d'impatto su individui o gruppi di individui).
<b>Rischio minimo</b>	Nessun obbligo legale specifico; incoraggiato l'uso di codici di condotta volontari (art. 95) e trasparenza (art. 13).	 <b>Pienamente coperto</b>	Lo standard ISO/IEC 42001 fornisce la struttura per gestire in modo etico e trasparente IA a basso rischio.
<b>Modelli di IA a uso generale (GPAI)</b>	Obbligo di valutazione del rischio, sicurezza informatica, trasparenza sui dataset, notifica incidenti gravi, collaborazione con l'AI Office (artt. 52–55).	 <b>Coperto concettualmente</b>	Lo standard ISO/IEC 42001 copre risk management e sicurezza informatica, ma non prevede obblighi di coordinamento con autorità europee. Tuttavia sono presenti controlli che esplicano il reporting nei confronti delle parti interessate (A.8.3) e quindi un riferimento alle autorità di cui sopra può esistere all'interno di questo controllo.

### **Cosa è uno standard e sue caratteristiche**

Iniziamo con il chiarire alcuni elementi che spesso generano confusione quando si tratta di norme ISO e certificazioni collegate.

Il termine “norma” che viene usato per definire gli standard ISO ha un senso diverso rispetto al concetto di norma usato nel linguaggio comune ed in particolare in quello giuridico.

La norma, secondo la definizione maggiormente accreditata tra i giuristi, costituisce l'elemento base del diritto all'interno dell'ordinamento giuridico, la quale si ricava attraverso l'interpretazione del testo (c.d. proposizione normativa) in cui la stessa è contenuta, cioè il provvedimento normativo. Le caratteristiche principali di quanto esposto sopra sono:

- La generalità, ossia che la stessa si rivolge ad una pluralità di soggetti determinati o determinabili;
- L'astrattezza, ossia il riferimento ad una fattispecie ipotetica;
- La positività poiché riconosciuta dallo Stato o da altra autorità legittimata ad emanarla
- Bilateralità, ossia la presenza di un obbligo per una parte e di un diritto per l'altra;
- Coattività o coercibilità: in caso di inosservanza della norma è prevista una sanzione o comunque la possibilità di attuarla in modo coattivo

Esaurite tali considerazioni e sgomberato il tavolo da possibili equivoci terminologici, il concetto di norma utilizzato nel presente documento è quello di standard (volontario), come si andrà adesso ad esaminare con riferimento alla ISO/IEC 42001.

### **La ISO/IEC 42001**

La ISO/IEC 42001 è uno standard internazionale (o norma), ad adozione volontaria; come tutti gli standard consolida le conoscenze mondiali sul tema della governance per i sistemi IA. Nessuno standard innova, uno “standard” per sua definizione consolida lo stato delle conoscenze a quella data; sembra una riflessione scontata ma a volte ci si dimentica di cosa sia uno standard.

Per meglio definire una norma standard ISO (o norma tecnica) vale la pena utilizzare quanto scritto da UNINFO<sup>1</sup>, per cui una norma tecnica è:

- un documento che dice “come fare bene le cose”, garantendo sicurezza, rispetto per l’ambiente e prestazioni certe.
- Secondo il Regolamento UE 1025 del Parlamento Europeo e del Consiglio del 25 ottobre 2012 sulla normazione europea, per “norma” si intende: *“una specifica tecnica, adottata da un organismo di normazione riconosciuto, per applicazione ripetuta o continua, alla quale non è obbligatorio conformarsi, e che appartenga a una delle seguenti categorie:*
  - **norma internazionale:** *una norma adottata da un organismo di normazione internazionale;*
  - **norma europea:** *una norma adottata da un’organizzazione europea di normazione;*
  - **norma armonizzata:** *una norma europea adottata sulla base di una richiesta della Commissione ai fini dell’applicazione della legislazione dell’Unione sull’armonizzazione;*
  - **norma nazionale:** *una norma adottata da un organismo di normazione nazionale”.*

Le norme tecniche, quindi, sono documenti che definiscono le caratteristiche (dimensionali, prestazionali, ambientali, di qualità, di sicurezza, di organizzazione ecc.) di un prodotto, processo o servizio, secondo lo stato dell’arte e sono il risultato del lavoro di decine di migliaia di esperti in Italia e nel mondo. Le caratteristiche peculiari delle norme tecniche sono:

- **consensualità:** deve essere approvata con il consenso di coloro che hanno partecipato ai lavori;
- **democraticità:** tutte le parti economico/sociali interessate possono partecipare ai lavori e, soprattutto, chiunque è messo in grado di formulare osservazioni nell’iter che precede l’approvazione finale;
- **trasparenza:** UNI segnala le tappe fondamentali dell’iter di approvazione di un progetto di norma, tenendo il progetto stesso a disposizione degli interessati;
- **volontarietà:** le norme sono un riferimento che le parti interessate si impongono spontaneamente.

---

<sup>1</sup> <https://www.uninfo.it/>

Con un diverso grado di approfondimento, si può proseguire aggiungendo anche il soggetto responsabile dello sviluppo delle norme tecniche. Il quale si distingue, da un punto di vista gerarchico, in:

- per le norme internazionali: International Standard Setting Organizations, ovvero:
  - IEC (International Electrotechnical Commission) per il settore elettrotecnico,
  - ITU (International Telecommunication Union) per il settore delle telecomunicazioni e
  - ISO (International Organization for Standardization) per tutti i settori diversi dai primi due;
- per le norme europee: European Standard Setting Organizations, ovvero:
  - CEN (*Comité européen de normalisation*) che si situa verticalmente sotto a ISO,
  - CENELEC (*Comité européen de normalisation en électronique et en électrotechnique*) per il settore elettrotecnico
  - ETSI (*European Telecommunications Standards Institute*) per il settore telecomunicazioni;
- per le norme nazionali: National Standard Bodies, per l'Italia, ovvero:
  - CEI (Comitato Elettrotecnico Italiano) e
  - UNI (Ente Nazionale Italiano di Unificazione).

Questo assetto gerarchico si riflette anche nella formulazione del titolo dello standard, ad esempio, la versione inglese della norma ISO si scrive ISO/IEC 42001:2023, laddove il successivo recepimento italiano si scrive, e si dovrebbe anche leggere, UNI CEI ISO/IEC 42001:2024 (o 2025 a seconda che si prenda come riferimento la fine dei lavori o la pubblicazione da parte di UNI). Per una serie di ragioni di opportunità terminologica, traduzione e interconnessione normativa si farà riferimento alla versione inglese, ai fini del presente contributo.

## Scopo e funzioni della ISO/IEC 42001

Dalla stessa norma<sup>2</sup> si apprendono i seguenti elementi cardine:

- La norma specifica i requisiti e fornisce una guida per la creazione, l'implementazione, la manutenzione e il miglioramento continuo di un sistema di gestione dell'IA (intelligenza artificiale) nel contesto di un'organizzazione.
- Il documento è destinato a un'organizzazione che fornisca o utilizzi prodotti o servizi che si avvalgano di sistemi di IA.
- La norma ha lo scopo di aiutare l'organizzazione a sviluppare, fornire o utilizzare sistemi di IA in modo responsabile nel perseguire i propri obiettivi e soddisfare i requisiti applicabili, gli obblighi relativi alle parti interessate e le aspettative nei loro confronti. Il presente documento è applicabile a qualsiasi organizzazione, indipendentemente dalle dimensioni, dal tipo e dalla natura, che fornisca o utilizzi prodotti o servizi che utilizzano sistemi di IA.

Un altro elemento essenziale per comprendere qualsiasi norma ISO (dei sistemi di gestione) è che si tratta di un *modello di governo* di una organizzazione (di qualsiasi settore e dimensione) per un determinato tema.

Le norme di requisiti (come la ISO/IEC 42001) indicano *cosa* occorre dimostrare per essere efficaci e conformi ma non *come* fare. Ogni azienda è quindi libera di stabilire come fare quanto specificato dalla norma. Questo è il rovescio della medaglia della standardizzazione che non può arrivare al grado di granularità che si può ad esempio richiedere ad un atto normativo nazionale (o anche ad un Regolamento europeo).

Le linee guida, a supporto delle norme, possono indicare come implementare i requisiti della norma. Ad esempio, la guida ISO/IEC 42005 fornisce indicazioni sul come strutturare un processo di valutazione degli impatti, richiesto nel requisito 6.1.4 della ISO/IEC 42001.

Questo aspetto e i precedenti devono essere tenuti in considerazione per una corretta interpretazione e utilizzazione della norma. Il discorso come visto, per quanto parallelo alle considerazioni di interpretazione che si possono fare sulle norme giuridiche segue esattamente lo stesso iter logico.

---

<sup>2</sup> UNI CEI ISO/IEC 42001 traduzione italiana della ISO/IEC 42001:2023

## Struttura HS e PDCA

Dal 2012 tutti gli standard ISO dei sistemi di gestione si sono conformati secondo la struttura denominata HLS (High Level Structure) consolidando il ruolo del ciclo PDCA (Plan-Do-Check-Act) al loro interno e fissando i contenuti minimi di ogni requisito.

Ciò ha permesso innanzitutto l'integrazione di diversi sistemi di gestione (permettendo notevoli economie di scala per le aziende con più certificazioni) e ha unificato la scrittura e la verifica degli standard ISO.

Nel 2021 la HLS ha subito una revisione "terminologica" ma non sostanziale (contenuta nell'Appendix "dell'Annex SL delle Direttive ISO/IEC Parte 1), il termine "High Level Structure" diventa HS, ossia "Harmonized Structure", calcando di fatto sul carattere armonizzato dei dieci punti della vecchia HLS. Nel 2023 UNI ha prodotto la correlata traduzione in italiano di quanto detto sopra. (<https://www.uni.com/sistemi-di-gestione-efficaci-e-integrati-una-guida-alla-harmonized-structure/>). Nella immagine che segue uno schema di quanto detto sopra per la ISO/IEC 42001:



Tutte le norme ISO sono composte da requisiti (da 1 a 10) e dagli eventuali Annex.

I requisiti “applicativi”, cioè quelli che servono per dimostrare il ciclo PDCA del sistema di gestione (e in definitiva la conformità), vanno dal 4 al 10.

Brevemente, il ciclo PDCA (o ciclo di Deming) è un modello di gestione in quattro fasi (Plan, Do, Check, Act) usato per il controllo e il miglioramento continuo di processi, prodotti e servizi.

Volendo fornire una mera definizione dei vari requisiti, senza scendere nel dettaglio della singola norma, ma restando ancorati alla HS si può osservare quanto segue:

- la prima fase (Plan) prevede solitamente la pianificazione e definizione del contesto, delle parti interessate e del campo di applicazione, unitamente alla politica dell'organizzazione, gli obiettivi e la valutazione dei rischi (rispettivamente i punti 4, 5 e 6) dell'immagine vista sopra. Il requisito 7 (Supporto) di fatto è considerato trasversale all'intero ciclo PDCA stesso (giacché di solito comprende aspetti concernenti risorse, competenze del personale, comunicazione, consapevolezza e informazioni documentate, aspetti che per forza di cose non possono non essere considerati non trasversali, pena la vulnerabilità stessa del ciclo PDCA).
- Nella fase successiva (Do) si guarda all'esecuzione di quanto pianificato, che sia l'esecuzione dei processi, la realizzazione dei prodotti/servizi. In questo punto (il numero 8) si attua solitamente il trattamento dei rischi identificati nel punto 6.
- La fase di cui al punto 9 (Check) si occupa del monitoraggio, della valutazione e dell'efficacia del sistema di gestione. Ma non solo, comprende altresì le fasi di audit e di riesame della direzione (aspetti il cui approfondimento esula dal presente contributo). Da quanto emerso nel Check si può cercare una *baseline* di miglioramento per il successivo ciclo PDCA (che di fatto costituisce l'esemplificazione del concetto di miglioramento continuo).
- Infine, la fase di Act (punto 10), quella in cui l'Organizzazione implementa i cambiamenti necessari per la conformità e il miglioramento continuo, ponendo fine al ciclo attuale ed il conseguente inizio di un secondo (e così via) ciclo PDCA.

Si è sempre parlato di dieci requisiti, ma operativamente si parte dal quattro. Gli altri tre hanno una valenza più introduttiva che operativa (rispetto al ciclo PDCA), ossia:

- Scopo e campo di applicazione [della norma] (requisito 1),
- Riferimenti normativi (requisito 2), la cui guida segue la Parte 2 delle Direttive ISO/IEC)
- Termini e definizioni (requisito 3).

Ogni norma, oltre a questi requisiti, può contenere anche un numero variabile di Annex, i quali possono avere due funzioni:

- *Annex normativi* – sono parte della norma e devono essere utilizzati come i requisiti della norma richiedono
- *Annex informativi* – sono contributi atti a favorire la comprensione degli argomenti trattati della norma ma non costituiscono obblighi per gli utilizzatori della norma.

La ISO/IEC 42001, ad esempio dispone di quattro Annex (A, B, C e D), di cui i primi due sono normativi e gli altri due informativi.

### La terminologia, i principi e i concetti di base

Come anticipato sopra, tutte le norme ISO hanno nei requisiti 2 e 3 i richiami alla terminologia utilizzata e ad altri standard utili alla comprensione e applicazione della norma.

La ISO/IEC 42001, non fa differenza ed utilizza i requisiti 2 e 3 proprio in questo modo e rimanda alla ISO/IEC 22989<sup>[1]</sup> per la comprensione dei concetti e dei termini utilizzati.

La ISO/IEC 22989 svolge un ruolo fondamentale per un Sistema di Gestione per l'IA (da qui in poi SGIA). Non tenerne conto si rivela quasi sistematicamente un errore che si pagherà a livello di corretta implementazione e funzionamento del sistema di gestione.

Il mondo degli standard adotta un linguaggio comune definito in sede di definizione di ogni norma (la funzione di standardizzazione). Non sempre il linguaggio degli standard è perfettamente allineato al mercato, alla lingua comune e tanto meno alle leggi. Pertanto, è bene conoscere la terminologia di una norma prima di utilizzarla, ciò per evitare incomprensioni ed errori che possono rivelarsi nelle fasi successive.

Alcuni termini sono indispensabili per poter comprendere la ISO/IEC 42001:

<b>Automazione, automatica, automatizzata</b>	pertinente a un processo o a un sistema che, in condizioni specifiche, funziona senza l'intervento umano.
<b>Agente di IA</b>	entità <i>automatizzata</i> che percepisce e risponde al proprio ambiente e intraprende azioni per raggiungere i propri obiettivi.
<b>Sistema di IA</b>	sistema ingegnerizzato che genera output come contenuti, previsioni, raccomandazioni o decisioni per un determinato insieme di obiettivi definiti dall'uomo.
<b>Componente di IA</b>	elemento funzionale che costruisce un <i>sistema di IA</i> .

<b>Intelligenza Artificiale (IA)</b>	<disciplina> ricerca e sviluppo di meccanismi e applicazioni di <i>sistemi di IA</i> .
<b>Conoscenza</b>	<intelligenza artificiale> informazioni astratte su oggetti, eventi, concetti o regole, sulle loro relazioni e proprietà, organizzate per un uso sistematico orientato agli obiettivi.
<b>Modello</b>	rappresentazione fisica, matematica o comunque logica di un sistema, di un'entità, di un fenomeno, di un processo o di dati.
<b>Compito</b>	<intelligenza artificiale> azione necessaria per raggiungere un obiettivo specifico.
<b>Previsione</b>	risultato primario di un sistema di IA quando gli vengono forniti dati di ingresso o informazioni.
<b>Dati di input</b>	dati per i quali un <i>sistema di IA</i> calcola un output previsto o un'inferenza.
<b>Obiettivi</b>	risultati da conseguire <sup>3</sup>

La ISO/IEC 22989 (gratuita nel sito ISO) riporta anche altre informazioni necessarie per un SGIA:

- Termini relativi all'IA
- Termini relativi ai dati
- Termini relativi all'apprendimento automatico
- Termini relativi alle reti neurali
- Termini relativi all'affidabilità
- Termini relativi all'elaborazione del linguaggio naturale
- Termini relativi alla visione artificiale
- Concetti di intelligenza artificiale
- Modello del ciclo di vita del sistema IA
- Panoramica funzionale del sistema AI.

Al momento, è in fase *draft* il primo *Amendment* della ISO/IEC 22989 (identificato come DAmD.1) il quale aggiunge, a una norma relativamente giovane, una serie di nuove definizioni, tra cui il richiamo ai sistemi di intelligenza artificiale generativa (di cui gli LLM fanno parte), la definizione di RAG (*Retrieval Augmented Generation system*), di *Foundation model* e altri termini (tra cui *Prompt*), proprio a dimostrazione della relativa rapidità di adattamento degli standard ISO al contesto globale.

---

<sup>3</sup> Gli obiettivi in un SGIA corrispondono agli obiettivi del Sistema IA

### **Gli standard collegati**

L'esperienza in campo ci porta a considerare alcuni standard a corredo della ISO/IEC 42001:

- ISO/IEC 42005:2025 - Information technology — Artificial intelligence — AI system impact assessment
- ISO/IEC 23894:2023 - Information technology - Artificial intelligence - Guidance on risk management
- ISO/IEC 5338:2023 - Information technology - Artificial intelligence - AI system life cycle processes
- ISO/IEC 23053:2022 - Framework for Artificial Intelligence (AI) Systems Using Machine Learning (ML)
- ISO/IEC TR 24027:2021 - Information technology - Artificial intelligence (AI) - Bias in AI systems and AI aided decision making

Senza considerare tutti quelli inerenti ai dati, a partire dalla ISO/IEC 5259-X (dove X indica le parti da 1 a 5 di cui è composto lo standard).

Per gli auditor degli Organismi di Certificazione è richiesta anche la conoscenza della:

- ISO/IEC 42006:2025 - Information technology - Artificial intelligence - Requirements for bodies providing audit and certification of artificial intelligence management systems

All'interno della quale sono riportati tutti gli standard di cui ogni auditor dei SGIA deve essere a conoscenza<sup>4</sup>:

- ISO/IEC 42001
- ISO/IEC 22989
- ISO/IEC 5338
- ISO/IEC 42005
- ISO/IEC 23894
- ISO/IEC 5259-3
- ISO/IEC TR 24027
- ISO/IEC 17021-1
- ISO/IEC 27001 e ISO/IEC 27701 per la sicurezza delle informazioni e dei dati personali, se applicabili al contesto del SGIA, cui potremmo aggiungere:
  - ISO/IEC 27017 per la sicurezza delle informazioni per i servizi in cloud
  - ISO/IEC 27018 per la sicurezza delle informazioni in cloud pubblici quando l'azienda opera in qualità di responsabile del trattamento dei dati personali

Oltre alla conoscenza ed esperienza su queste norme occorre anche dimostrare esperienza su:

- requisiti generali per i SGIA
- standard del sistema di gestione dell'intelligenza artificiale, documenti normativi e schemi di certificazione
- obblighi legali relativi all'intelligenza artificiale e al SGIA
- terminologia, principi, pratiche, strumenti, metodi e tecniche specifici dell'intelligenza artificiale e del SGIA
- settore di attività del cliente (cliente qui è inteso come azienda che riceve l'audit)
- prodotti, processi e organizzazione del cliente.

Questo colloca la ISO/IEC 42001 tra le norme più articolate al momento disponibili.

In funzione del settore in cui si opera potrebbero essere di interesse anche le:

- ISO/IEC 20000-1:2018 - Information technology — Service management Part 1: Service management system requirements
- ISO 9001:2015 - Quality management systems — Requirements

---

<sup>4</sup>Questi standard sono applicabili anche per la conduzione degli audit interni.

Ciò a causa del fatto che praticamente tutte le aziende hanno come base la ISO 9001 per i processi aziendali e la ISO/IEC 20000-1 per i servizi IT.

Pur non essendo una verità assoluta, molte IA “girano” in cloud; per questo sarebbe auspicabile anche la conoscenza delle:

- ISO/IEC 22123-1:2023 Information technology — Cloud computing Part 1: Vocabulary
- ISO/IEC 22123-2:2023 Information technology — Cloud computing Part 2: Concepts
- ISO/IEC 22123-3:2023 Information technology — Cloud computing Part 3: Reference architecture.

Queste ultime sono gratuite nel sito ISO e forniscono un quadro chiaro dei sistemi in cloud e delle loro caratteristiche.

### **Il diverso significato di certificazione tra AI Act e ISO/IEC 42001**

**La certificazione 42001 non certifica l'IA ma il Sistema di Gestione dell'Intelligenza Artificiale, la certificazione dell'IA rientra nell'AI Act.** Questa precisazione è doverosa per evitare ogni possibile confusione concettuale.

Prima di intraprendere la strada per l'implementazione e certificazione di un SGIA è utile fare alcune considerazioni di ordine pratico:

1. si tratta di un sistema di gestione diverso dagli altri, più evoluto, con molte differenze innovative rispetto ad altre norme, inclusa la ISO/IEC 27001 da cui è tratta la struttura di base (ad es. 2 Annex normativi da utilizzare nel trattamento dei rischi).
2. Per affrontare correttamente la ISO/IEC 42001 si dovrebbe partire con lo studio approfondito degli standard associati, come minimo:
  - la ISO/IEC 22989
  - la ISO/IEC 42005 (la valutazione di impatto è una novità nel mondo ISO ma soprattutto è la chiave di volta della ISO/IEC 42001).
3. Quando si parla di ISO/IEC 42001 si parla anche del ciclo di vita del sistema IA (DevOps) e quindi sarebbe opportuno avere idee chiare per quanto concerne il ciclo di vita del software<sup>5</sup> e dei sistemi<sup>6</sup>.

---

<sup>5</sup> ISO/IEC/IEEE 12207:2017 - Systems and software engineering — Software life cycle processes

<sup>6</sup> ISO/IEC/IEEE 15288:2023 - Systems and software engineering — System life cycle processes

4. Ogni tentativo di paragonare la ISO/IEC 42001 ad altri standard o, peggio ancora, adattarla ad altre norme si rivela spesso inefficace se non controproducente. In particolare, per la gestione dei rischi e delle opportunità (molto più orienta agli HS rispetto ad altri standard certificabili).
5. La ISO/IEC 42001 vede l'azienda in tre ruoli possibili: sviluppatrice, fornitrice e utilizzatrice di Sistema IA. Questa è una caratteristica unica che permette ad una azienda di strutturare un unico sistema di gestione con 3 diverse declinazioni, in funzione del ruolo che essa ha in relazione al sistema IA. Occorre avere chiaro per cosa si utilizzerà il SGIA fin dalle prime battute. Parliamo di *sistema IA* e non di *sistemi IA*. Questa è un'altra delle caratteristiche che occorre aver ben chiare: ogni sistema IA ha obiettivi, rischi e opportunità, può usare parte o tutto il ciclo di vita ecc. In definitiva, è come avere un sistema di gestione per ogni sistema IA, e il discorso si lega anche al settore in cui opera il sistema IA.

Passiamo ora ad analizzare alcuni elementi tipici della ISO/IEC 42001 che possono creare qualche difficoltà nella fase implementativa.

### **Valutazione degli impatti**

La valutazione degli impatti è di tale importanza da avere una specifica guida a supporto (ISO/IEC 42005). La stessa norma ISO/IEC 42001 vi dedica una approfondita sezione sia in termini di processo (req. 6.1.4) sia di conduzione operativa (req. 8.4).

La valutazione degli impatti è vista come un set di informazioni che occorre prendere in considerazione, la stessa norma ci chiarisce cosa è necessario considerare:

- L'organizzazione deve definire un *processo di valutazione delle potenziali conseguenze per individui o gruppi di individui*, o entrambi, e per le *società* che possono derivare dallo *sviluppo*, dalla *fornitura* o dall'*utilizzazione* di sistemi di IA.
- La valutazione dell'impatto del sistema di IA determina le potenziali conseguenze che l'impiego, l'*uso previsto* e l'*abuso prevedibile* (o uso improprio) di un sistema di IA hanno sugli individui o sui gruppi di individui, o su entrambi, e sulle società.
- La valutazione dell'impatto del sistema di IA tiene conto dello specifico *contesto tecnico* e *sociale* in cui il sistema di IA viene impiegato e delle *giurisdizioni applicabili* (contesto legale).

Da tenere in considerazione che quello che legalmente è ammesso nel nostro stato potrebbe non esserlo nello stato dell'utilizzatore. La progettazione e sviluppo, l'erogazione e l'utilizzazione sono quindi sensibili ai contesti sociali e giuridici.

Argomento non poco complesso, specie per i realizzatori di sistemi IA multimodali a larga diffusione o, peggio, “open”.

La ISO/IEC 42005 è una ricca fonte di informazioni per avere un approccio concreto alla valutazione degli impatti in un approccio by design e by default preventivo alla fase di sviluppo di qualsivoglia sistema e/o strumento basato sull' AI. Va però considerato che si tratta di una linea guida a supporto della norma ISO/IEC 42001, quindi non può sostituire quanto richiesto dalla norma ma può, semmai, ampliare e chiarire gli argomenti relativi alla valutazione degli impatti delle IA.

Il mercato ha messo a disposizione qualche esempio ma si tratta pur sempre di modelli “proprietary”<sup>7</sup> che non necessariamente si adattano alla realtà di tutte le aziende.

### **Gestione dei rischi e delle opportunità**

Su questo argomento è bene fare chiarezza.

La valutazione degli impatti (di un sistema IA) deve precedere la valutazione dei rischi e delle opportunità; infatti, la valutazione dei rischi utilizzerà i risultati della valutazione degli impatti, non viceversa, come chiarisce il req. 6.1.4 della ISO/IEC 42001:

*L'organizzazione deve prendere in considerazione i risultati della valutazione dell'impatto del sistema di IA nella valutazione dei rischi*

Inoltre, i rischi di un sistema IA (e quindi anche le opportunità) si riferiscono ai suoi obiettivi, come chiarisce il req. 6.1.2.c della ISO/IEC 42001:

*identifichi i rischi che favoriscono o impediscono il raggiungimento degli obiettivi di IA;*

Gli obiettivi per la ISO/IEC 42001 sono i principi cui il sistema IA dovrà aderire.

---

<sup>7</sup> <https://msblogs.thesourcemediaassets.com/sites/5/2022/06/Microsoft-RAI-Impact-Assessment-Template.pdf>

Un esempio, non esaustivo, è nell'Allegato C<sup>8</sup> (informativo) della ISO/IEC 42001:

- Accountability
- Fairness
- Robustness
- Transparency
- AI expertise
- Maintainability
- Safety
- Explainability
- Environmental impact
- Privacy
- Security

Supponendo che il sistema IA sviluppato abbia il compito di supportare l'utilizzatore nella ricerca e nella selezione del personale, pare chiaro che un sistema del genere non possa prescindere da principi quali l'etica, le pari opportunità, la privacy ecc.

Assicurare etica, pari opportunità, privacy ecc. deve essere un connotato da valutare prima della fase di sviluppo al fine di trovare i presidi adeguati a prevenirne l'accadimento e/o mitigarne gli effetti negativi qualora sussistano probabilità ritenute significative.

Il rischio, a livello di norme ISO, è di fatto il prodotto tra l'impatto (o conseguenze) che un determinato evento possa causare e la probabilità che questo si verifichi:

$$R=I \times P$$

Nell'esempio:

- l'impatto costituito dalle potenziali violazioni di etica, pari opportunità, privacy ecc. (quindi degli obiettivi dell'IA)
- la probabilità (o possibilità se non si dispone di dati pregressi) che il sistema IA possa violare gli obiettivi (principi) di etica, pari opportunità o privacy.

Ovviamente ogni obiettivo può avere valori di rischio diversi oppure presentarsi come opportunità; alcuni parlano di rischi per R negativo e opportunità per R positivo altri fanno l'inverso, e questo è il bello delle norme ISO: il *come* fare è libero, il *cosa* è dettato dalla norma. Altra particolarità è che la valutazione degli impatti e la *gestione del rischio* conseguente (intesa come *valutazione e trattamento del rischio*) sia legata alle fasi del ciclo di vita di un sistema IA.

---

<sup>8</sup> Lo stesso elenco è ripreso nell'Allegato A della ISO/IEC 23894

Infatti, alcuni elementi di rischio possono emergere solo in determinate fasi del ciclo. Ad esempio, per un addestramento basato su dati impropri gli effetti potrebbero essere “visibili” solo nel corso della validazione del sistema IA e non prima.

Quindi, rispetto alle altre norme, si parla di un rischio dinamico all'interno del ciclo di vita. Nessuna norma ISO aveva mai ipotizzato uno scenario così dinamico in precedenza. Dinamicità che, molto probabilmente, fa parte dell'*ontos* stesso dell'IA.

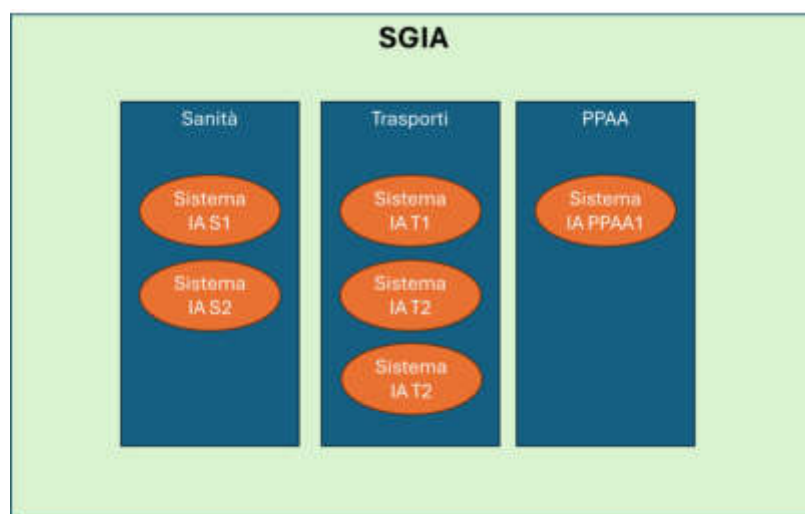
### Dalla politica in poi tutto è relativo al sistema IA

Questo aspetto viene scoperto dalle aziende non appena iniziano a mettere in pratica la ISO/IEC 42001. In alcuni casi ha spiazzato l'azienda (creando non pochi problemi nel corso dell'audit) in altri è stata considerata come una caratteristica ovvia.

Analizzando i requisiti della norma, e la sua terminologia, appare chiaro che il riferimento all'IA è inteso come sistema IA:

- 6.1.2/8.2 Valutazione del rischio dell'IA
- 6.1.3/8.3 Trattamento del rischio dell'IA
- 6.1.4/8.4 Valutazione dell'impatto del sistema di IA
- 6.2 Obiettivi per l'IA

Ogni sistema IA è poi legato al settore specifico in cui opera, il che porta ad una impostazione che possiamo schematizzare come segue:



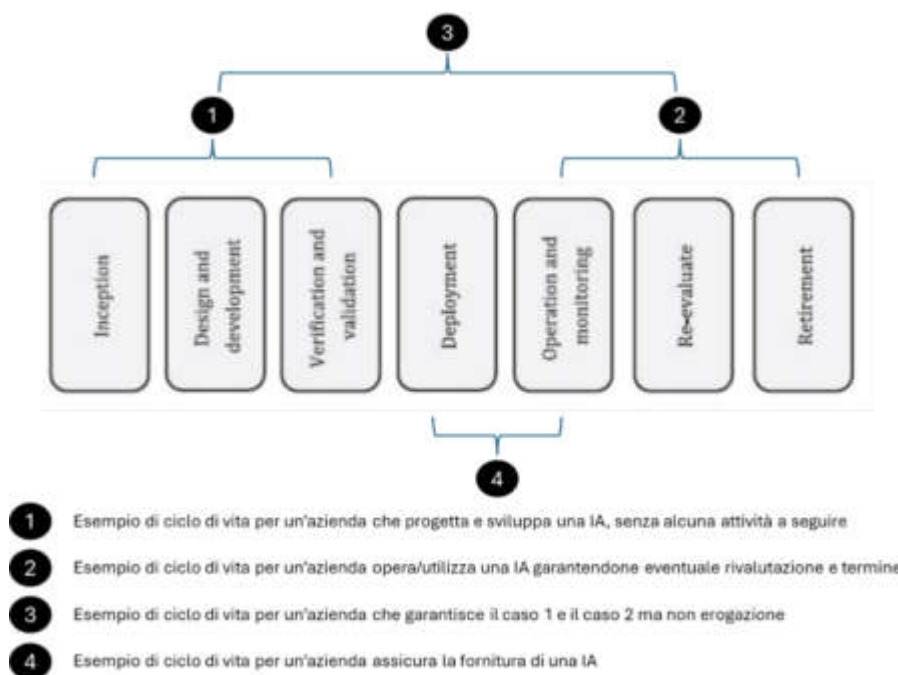
Ogni sistema IA ha una storia a sé, le differenze possono essere anche rilevanti.

Questa caratteristica della ISO/IEC 42001 determina uno sviluppo diverso dagli altri sistemi di gestione (e di conseguenza anche gli audit sono strutturati in modo diverso).

### I tre ruoli della norma

I tre ruoli dell'azienda di cui parla la norma (sviluppo, fornitura, uso) influenzano il sistema di gestione, in modo particolare per il ciclo di vita. L'azienda deve quindi capire, in funzione del ruolo, quali parti del ciclo di vita occorre considerare.

Ancora una volta si può far uso di uno schema esemplificativo dei possibili ruoli e combinazioni con le fasi del ciclo di vita:



Ovviamente può esistere anche il caso di una azienda che assicura l'intero ciclo di vita in relazione a tutti e 3 i ruoli previsti dalla norma, in funzione del sistema IA considerato.

Lo schema riporta situazioni effettivamente incontrate nel corso degli audit condotti.

Questa articolazione potrebbe riferirsi anche ad aziende dello stesso gruppo operanti in stati/continenti diversi e contesti giuridici molto diversi.

È facile immaginare la complessità di un sistema di gestione con una tale organizzazione, impatti e rischi diversi per IA, per settore e per utilizzatore. Una combinazione complessa che ha portato alcune aziende a considerare un solo sistema IA per la prima certificazione e un progetto di estensione progressiva nel tempo, in modo da includere tutti i sistemi IA nel SGIA nell'arco di un biennio o più.

### **Struttura della norma e sequenza di implementazione**

L'ordine dei requisiti segue il ciclo PDCA (Plan-Do-Check-Act) caratteristico di ogni norma ISO certificabile (come già visto in apertura). Questo ordine permette di approcciare una sequenza di attività organizzata e sistematica per affrontare le varie tematiche<sup>9</sup>.

All'interno di ogni requisito si possono trovare i riferimenti (correlazioni) con altri requisiti e determinare così la giusta sequenza di implementazione. Ad esempio, la frase:

*L'organizzazione deve prendere in considerazione i risultati della valutazione dell'impatto del sistema di IA nella valutazione dei rischi*

fornisce una chiara spiegazione di quale sia la sequenza esatta tra valutazione degli impatti e valutazione dei rischi.

In definitiva un requisito della norma rappresenta un processo (con i suoi input, output e collegamenti con altri processi). Questa struttura permetterà di integrare i processi della norma con i processi dell'azienda, determinando il sistema di gestione risultante.

Rispetto a quanto visto in apertura, sul ciclo "lineare" allineato alla HLS (o HS) vi sono notevoli specificazioni e aggiunte proprie (al di là dei già citati Annex) della ISO/IEC 42001.

---

<sup>9</sup> Al momento attuale non è ancora disponibile una guida all'implementazione del SGIA (come invece esiste per altre norme ISO), è però stato avviato un progetto di norma (per ora a livello di Working Draft) che potrebbe portare, nel giro di qualche anno, ad avere anche per la ISO/IEC 42001 una guida specifica.

Nella fase Plan si trovano i processi “preparatori” e trasversali del sistema di gestione:

- 4 CONTESTO DELL'ORGANIZZAZIONE
  - 4.1 Comprendere l'organizzazione e il suo contesto
  - 4.2 Comprendere le esigenze e le aspettative delle parti interessate
  - 4.3 Determinazione del campo di applicazione del sistema di gestione dell'IA
  - 4.4 Sistema di gestione dell'IA
- 5 LEADERSHIP
  - 5.1 Leadership e impegno
  - 5.2 Politica
  - 5.3 Ruoli, responsabilità e autorità
- 6 PIANIFICAZIONE
  - 6.1 Azioni per affrontare rischi e opportunità
  - 6.2 Obiettivi per l'IA e pianificazione per il loro raggiungimento
  - 6.3 Programmazione delle modifiche
- 7 SUPPORTO
  - 7.1 Risorse
  - 7.2 Competenze
  - 7.3 Consapevolezza
  - 7.4 Comunicazione
  - 7.5 Informazioni documentate

Nella fase Do si trovano i processi per la messa in opera di quanto pianificato (nella fase Plan):

- 8 ATTIVITÀ OPERATIVE
  - 8.1 Pianificazione e controlli operativi
  - 8.2 Valutazione del rischio dell'IA
  - 8.3 Trattamento del rischio dell'IA
  - 8.4 Valutazione dell'impatto del sistema di IA

Nella fase Check si trovano i processi per la misurazione delle prestazioni del sistema di gestione (dimostrazione che quanto pianificato e quanto fatto sono in linea tra loro, efficaci e conformi):

- 9 VALUTAZIONE DELLE PRESTAZIONI
  - 9.1 Monitoraggio, misurazione, analisi e valutazione
  - 9.2 Audit interno
  - 9.3 Riesame di direzione

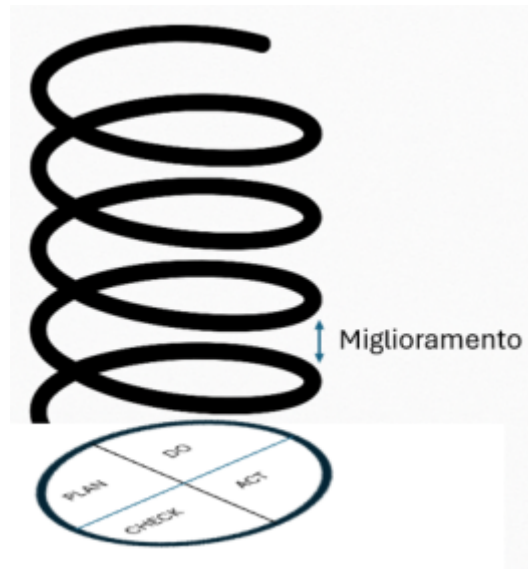
Nella fase Act si trovano i processi per il miglioramento (un sistema di gestione deve per definizione migliorare):

- 10 MIGLIORAMENTO
  - 10.1 Miglioramento continuo
  - 10.2 Non conformità e azioni correttive

Importante notare che le famigerate *non conformità* si trovano nel miglioramento, questo a conferma del fatto che una non conformità non è un fatto negativo ma l'inizio di un miglioramento, fattore determinante per affrontare i successivi audit con un atteggiamento collaborativo e propositivo.

Il ciclo PDCA non deve essere visto come un cerchio suddiviso in 4 sezioni (come viene spesso rappresentato) ma piuttosto come una spirale, un solenoide, dove ogni spira è un ciclo PDCA e la distanza tra le spire dimostra il miglioramento tra un ciclo e l'altro.

Anche questa "visione" è determinante per capire e sviluppare correttamente il sistema di gestione, non si tratta di un sistema statico ma dinamico, dove ogni miglioramento è voluto, pianificato nella fase precedente e dimostrato nella fase successiva, qualcosa di simile a:



Visione necessaria per affrontare correttamente il processo di implementazione e certificazione del SGIA.

### **Gli allegati, la loro relazione con la norma, le correlazioni tra i controlli**

La ISO/IEC 42001, tra le tante particolarità, ha due Allegati normativi (dette Appendici o Annex), unica altra norma ad avere qualcosa di simile è la ISO/IEC 27001 che però ha un solo Allegato normativo.

Questi due Allegati hanno funzioni diverse:

- Allegato A – utilizzazione obbligatoria per la scelta dei controlli, utili al processo di trattamento del rischio (req. 6.1.3) – non tutti i controlli sono obbligatori, è la norma che fornisce regole per la comprensione dell'utilizzo di questo Allegato
- Allegato B - “da considerare” nell’ambito della scelta dei controlli.

Situazione complessa a prima vista ma facilmente comprensibile dopo un accurato studio e comprensione dei contenuti dei due Allegati e del loro richiamo nelle varie sezioni della norma.

Vediamo cosa la ISO/IEC 42001 ci dice per questi allegati:

- *I controlli descritti nell'Allegato A forniscono all'organizzazione un riferimento per raggiungere gli obiettivi dell'organizzazione e affrontare i rischi legati alla progettazione e al funzionamento dei sistemi di IA. Non tutti gli obiettivi di controllo e i controlli elencati nell'Allegato A sono da utilizzarsi obbligatoriamente e l'organizzazione può progettare e attuare i propri controlli.*
- *L'Allegato B fornisce una guida all'implementazione di tutti i controlli elencati nell'Allegato A.*

Altra caratteristica della ISO/IEC 42001 è che alcuni controlli dell'Allegato A sono richiamati direttamente dai requisiti della norma (rendendoli di fatto obbligatori) mentre altri sono da selezionare in base alle considerazioni fatte in relazione a rischi/opportunità (opzioni di trattamento).

Facciamo un esempio per spiegare il tutto.

Il requisito 5.2 della ISO/IEC 42001 parla della politica di IA. All'interno del requisito è chiaramente richiamato il controllo A.2<sup>10</sup> dell'Annex A:

*Gli obiettivi di controllo e i controlli per la definizione di una politica di IA sono riportati nel punto A.2 del prospetto A.1. Le linee guida per l'attuazione di tali controlli sono fornite nel punto B.2.*

Questo passaggio ci fa capire la diversa destinazione d'uso dei due Allegati.

Vedasi ora cosa dice l'Allegato A.2:

<b>A.2 Politiche relative all'IA</b>		
Obiettivo: Fornire indirizzi e supporto di gestione per i sistemi di IA secondo i requisiti aziendali.		
	Argomento (Topic)	Controllo
A.2.2	Politica di IA	L'organizzazione deve documentare una politica per lo sviluppo o l'utilizzo di sistemi di IA.
A.2.3	Allineamento con altre politiche dell'organizzazione	L'organizzazione deve determinare in quali casi eventuali altre politiche possono essere influenzate o essere applicate agli obiettivi dell'organizzazione in relazione ai sistemi di IA.
A.2.4	Riesame della politica di IA	La politica di AI deve essere rivista a intervalli pianificati o, se necessario, in più occasioni, per garantire l'idoneità, l'adeguatezza e l'efficacia.

<sup>10</sup> La numerazione dei controlli nell'Allegato A non ha alcuna correlazione con la numerazione dei requisiti della norma

Quindi nella preparazione della politica di IA, richiesta dalla norma, si devono includere anche gli elementi riportati nei controlli da A.2.2 ad A.2.4.

Certo è che la spiegazione del controllo risulta alquanto laconica, qui ci viene in soccorso l'Allegato B. Vediamo il controllo A.2.4 come esempio, nel corrispondente numero dell'Allegato B troviamo:

<b>B.2.4</b>	<b>Riesame della politica di IA</b>
	<b>Controllo</b>
	La politica di IA dovrebbe essere riesaminata a intervalli pianificati o, se necessario, in più occasioni, al fine di assicurarne la continua idoneità (suitability), adeguatezza (adequacy) ed efficacia (effectiveness).
	<b>Guida di attuazione</b>
	Una figura approvata dalla Direzione dovrebbe essere responsabile dello sviluppo, del riesame e della valutazione della politica sull'IA o delle sue sezioni. La revisione dovrebbe includere la valutazione delle opportunità di miglioramento delle politiche e dell'approccio dell'organizzazione alla gestione dei sistemi di IA in risposta ai cambiamenti del contesto organizzativo, delle circostanze aziendali (business circumstances), delle condizioni legali (legal conditions) o dell'ambiente tecnico (technical environment) dell'organizzazione.
	La revisione della politica di IA dovrebbe tenere conto dei risultati dei Riesami della Direzione.]

In questo modo l'azienda trova nell'Allegato B una spiegazione di come implementare quanto richiesto nell'Allegato A. L'uso del *dovrebbe* (a differenza del *deve* usato nei requisiti e nell'Allegato A) chiarisce l'ambito di scelta lasciato all'azienda nella definizione della soluzione desiderata.

Un approccio articolato ma estremamente pratico in fase di implementazione dei requisiti della norma.

Non tutti i requisiti della norma hanno controlli dell'Allegato A associati in forma obbligatoria. Si osservi dove i controlli sono richiamati in forma obbligatoria (richiamati nel testo) e dove in forma volontaria (richiamati nelle note):

Requisiti ISO/IEC 42001	Controlli richiamati
5.2 Politica	A.2 Politiche relative all'IA
6.1.4 Valutazione dell'impatto del sistema di IA	A.5 Valutazione dell'impatto dei sistemi di IA

Note dei Requisiti ISO/IEC 42001	Controlli richiamati
5.3 Ruoli, responsabilità e autorità	A.3.2 Ruoli e responsabilità dell'IA
6.2 Obiettivi per l'IA e pianificazione per il loro raggiungimento	A.6.1 Guida alla gestione per lo sviluppo di sistemi di IA A.9.3 Obiettivi per un utilizzo responsabile (responsibile) del sistema di IA
7.1 Risorse	A.4 Risorse per i sistemi di IA

Da qui si evince che molti dei controlli dell'Allegato A restano una scelta volontaria legata a vari fattori:

- Richieste cogenti (regolamenti, direttive, leggi ecc.)
- Richieste contrattuali
- Richieste di mercato o di settori specifici
- Scelte interne all'azienda
- Come risposta al trattamento dei rischi.

I controlli sono in totale 38 distribuiti su 9 "argomenti" (numerati da A.2 ad A.10)

- 3 controlli in **A.2 Politiche relative all'IA\***
- 2 controlli in **A.3 Organizzazione interna**
- 5 controlli in **A.4 Risorse per i sistemi di IA**
- 4 controlli in **A.5 Valutazione dell'impatto dei sistemi di IA\***
- 9 controlli in **A.6 Ciclo di vita del sistema di IA**
- 5 controlli in **A.7 Dati per i sistemi di IA**
- 4 controlli in **A.8 Informazioni per le parti interessate ai sistemi di IA**
- 3 controlli in **A.9 Utilizzo di sistemi di IA**
- 3 controlli in **A.10 Rapporti con terzi e clienti**

Gli asterischi indicano i controlli obbligatori richiamati dalla norma per la politica e per la valutazione degli impatti.

## Informazioni documentate e documenti

Un discorso particolare meritano le *informazioni documentate*, termine piuttosto complesso per i non addetti ai lavori. Una semplificazione può aiutare a capire di quali documenti si tratta e di quali abbiamo bisogno in un sistema di gestione basato sulla ISO/IEC 42001.

Per informazioni documentate, qualsiasi norma ISO intende:

- *le informazioni documentate richieste dal presente documento [cioè dalla norma];*
- *le informazioni documentate che l'organizzazione determina come necessarie per l'efficacia del sistema di gestione dell'IA.*

Nonostante questa precisazione il termine informazione documentata potrebbe non essere del tutto chiaro. Per risolvere la questione occorre risalire alla ISO 9000:2015 dove sono riportati i termini di base dei sistemi ISO:

<b>3.8.6</b>	<b>informazioni documentate</b> [documented information]: <i>Informazioni</i> (3.8.2) che devono essere tenute sotto controllo e mantenute da parte di un'organizzazione (3.2.1) ed il mezzo che le contiene.
Nota 1	Le informazioni documentate possono essere in un qualsiasi formato, su qualsiasi mezzo e provenire da qualsiasi fonte.
Nota 2	Le informazioni documentate possono riferirsi a: <ul style="list-style-type: none"> <li>- il sistema di gestione (3.5.3), compresi i relativi processi (3.4.1);</li> <li>- le informazioni create per il funzionamento dell'organizzazione (documentazione);</li> <li>- l'evidenza dei risultati conseguiti [registrazioni (3.8.10)].</li> </ul>
Nota 3	Il presente termine fa parte è uno dei termini comuni e delle definizioni di base per le norme ISO di sistemi di gestione riportati nell'Appendice SL del Supplemento consolidato alla Parte 1 delle Direttive ISO/IEC.

Si tratta quindi dei documenti richiesti dalla norma, necessari per dimostrare l'applicazione, l'efficacia e la conformità del sistema di gestione.

Il req.7.5 di ogni norma spiega cosa occorre fare per questo tipo di documenti.

Si immagini una informazione documentata come un contenitore (elettronico o cartaceo) dove conservare i dati che la norma richiede di dimostrare. Un esempio pratico può aiutare:

*L'organizzazione deve conservare informazioni documentate sui risultati di tutte le valutazioni di impatto del sistema di IA.*

La norma chiede di fare in modo che i risultati di tutte le valutazioni di impatto siano informazioni documentate e che siano conservate. Le caratteristiche di questo contenitore devono però assicurare quanto richiesto dal req. 7.5 della norma, in termini di creazione, aggiornamento e controllo.

In questo modo la norma si assicura che i dati necessari per dimostrare efficacia e conformità siano documentati, controllati, conservati e utilizzabili per la dimostrazione dello stato del SGIA negli audit interni e dell'Organismo di Certificazione.

Tutte le norme hanno in comune le medesime informazioni documentate, poiché facenti parte del HS:

- (4.3) il campo di applicazione
- (5.2) la politica
- (6.2) gli obiettivi
- (7.2) le competenze del personale
- (8.1) la pianificazione e controllo dei processi
- (9.1) i risultati di monitoraggio e misurazione
- (9.2) l'attuazione del programma degli audit interni e i risultati degli audit interni
- (9.3) i risultati del riesame della direzione
- (10.1) la natura delle non conformità, le eventuali azioni successive intraprese, i risultati di eventuali azioni correttive

La ISO/IEC 42001 aggiunge:

- (6.1.1) le azioni intraprese per identificare e gestire i rischi e le opportunità dell'IA
- (6.1.2) il processo di valutazione del rischio dell'IA
- (6.1.3) il processo di trattamento del rischio dell'IA
- (6.1.4) il processo di valutazione dell'impatto del sistema IA
- (8.2) i risultati di tutte le valutazioni del rischio dell'IA
- (8.3) i risultati di tutti i trattamenti del rischio dell'IA; la documentazione per i controlli ritenuti necessari e la dichiarazione di applicabilità (SoA) richiesto nel 6.1.3
- (8.4) i risultati di tutte le valutazioni di impatto del sistema di IA

Cui si aggiungono i documenti richiesti dai controlli dell'Allegato A (sia quelli obbligatori sia quelli liberamente scelti dall'azienda), ad esempio quelli evidenziati nella seguente immagine:

<b>A.7 Dati per i sistemi di IA</b>		
Obiettivo: Assicurare che l'organizzazione comprenda il ruolo e l'impatto dei dati nei sistemi di IA nell'applicazione e nello sviluppo, nella fornitura o nell'utilizzo dei sistemi di IA durante il loro ciclo di vita.		
	Argomento (Topic)	Controllo
A.7.2	Dati per lo sviluppo e il potenziamento del sistema di IA.	L'organizzazione deve definire, documentare e implementare i processi di gestione dei dati (data management processes) relativi allo sviluppo dei sistemi di IA.
A.7.3	Acquisizione dei dati	L'organizzazione deve determinare e documentare i dettagli relativi all'acquisizione e alla selezione dei dati utilizzati nei sistemi di IA.
A.7.4	Qualità dei dati per i sistemi di IA	L'organizzazione deve definire e documentare i requisiti per la qualità dei dati e garantire che i dati utilizzati per sviluppare e gestire il sistema di IA soddisfino tali requisiti.
A.7.5	Provenienza dei dati	L'organizzazione deve definire e documentare un processo per la registrazione della provenienza dei dati utilizzati nei suoi sistemi di IA lungo il ciclo di vita dei dati e del sistema di IA.
A.7.6	Preparazione dei dati	L'organizzazione deve definire e documentare i criteri di selezione dei dati da elaborare e i metodi di elaborazione degli stessi.
<b>A.8 Informazioni per le parti interessate ai sistemi di IA</b>		
Obiettivo: Garantire che le parti interessate abbiano le informazioni necessarie per comprendere e valutare i rischi e i loro impatti (sia positivi che negativi).		
	Argomento (Topic)	Controllo
A.8.2	Documentazione del sistema e informazioni per gli utilizzatori (users)	L'organizzazione deve determinare e fornire le informazioni necessarie agli utilizzatori del sistema di IA.
A.8.3	Reporting esterno	L'organizzazione deve fornire alle parti interessate la possibilità di segnalare gli impatti negativi del sistema di IA.
A.8.4	Comunicazione degli incidenti	L'organizzazione deve determinare e documentare un piano per la comunicazione degli incidenti agli utilizzatori del sistema di IA.
A.8.5	Informazioni per le parti interessate	L'organizzazione deve determinare e documentare i propri obblighi di comunicazione, alle parti interessate, delle informazioni relative al sistema di IA.
<b>A.9 Utilizzo di sistemi di IA</b>		
Obiettivo: Assicurare che l'organizzazione utilizzi i sistemi di IA in modo responsabile (responsibly) e secondo le politiche dell'organizzazione.		
	Argomento (Topic)	Controllo
A.9.2	Processi per un utilizzo responsabile (responsible) dei sistemi di IA	L'organizzazione deve definire e documentare i processi per l'utilizzo responsabile dei sistemi di IA.
A.9.3	Obiettivi per un utilizzo responsabile (responsible) del sistema di IA	L'organizzazione deve identificare e documentare gli obiettivi per guidare l'utilizzo responsabile dei sistemi di IA.
A.9.4	Uso previsto del sistema di IA	L'organizzazione deve garantire che il sistema di IA sia utilizzato secondo gli usi previsti del sistema stesso e secondo la documentazione a corredo.

Il set documentale di un sistema di gestione per l'IA è quindi piuttosto corposo e assicurarne il controllo richiede un processo accurato ma anche sostenibile.

## Il ruolo della SoA

La norma ISO/IEC 42001 nel req. 6.1.3 chiede di *produrre* una SoA (Statement of Applicability o Dichiarazione di applicabilità), non una informazione documentata quindi.

Per le aziende certificate è la ISO/IEC 42006 degli Organismi di Certificazione a imporre che la SoA diventi una *informazione documentata*. Questo a causa del fatto che i riferimenti della SoA (data e versione) verranno riportati nel certificato in modo da cristallizzare lo stato del sistema di gestione alla data di certificazione. Ogni cambiamento significativo della SoA produrrà una riemissione del certificato per assicurarne l'allineamento alla situazione reale.

Essendo la SoA la raccolta di tutti i controlli messi in atto a fronte dei rischi, ed essendo i rischi legati agli obiettivi di una IA, ne consegue che l'azienda potrebbe avere più di una SoA, una per ciascun sistema IA. Questo porta molte aziende ad avere una sola SoA strutturata come segue:

			Sistema IA1	Sistema IA2	Sistema IA <sub>n</sub>
Controllo Annex A			Giustificazione per inclusione o esclusione	Giustificazione per inclusione o esclusione	Giustificazione per inclusione o esclusione
A.2.2	Politica di IA	L'organizzazione deve documentare una politica per lo sviluppo o l'utilizzo di sistemi di IA.			
A.2.3	Allineamento con altre politiche dell'organizzazione	L'organizzazione deve determinare in quali casi eventuali altre politiche possono essere influenzate o essere applicate agli obiettivi dell'organizzazione in relazione ai sistemi di IA.			
A.2.4	Riesame della politica di IA	La politica di IA deve essere rivista a intervalli pianificati o, se necessario, in più occasioni, per garantirne l'idoneità, l'adeguatezza e l'efficacia.			
A.3.2	Ruoli e responsabilità dell'IA	I ruoli e le responsabilità dell'IA devono essere definiti e assegnati in base alle esigenze dell'organizzazione.			
A.3.3	Reporting dei reclami	L'organizzazione deve definire e mettere in atto un processo per la segnalazione di dubbi sul ruolo dell'organizzazione rispetto a un sistema di IA lungo tutto il suo ciclo di vita.			
A.4.2	Documentazione delle risorse	L'organizzazione deve identificare e documentare le risorse appropriate che sono necessarie per le attività delle fasi del ciclo di vita del sistema di IA e di altre attività relative all'IA rilevanti per l'organizzazione.			
A.4.3	Risorse per i dati	Nell'ambito dell'identificazione delle risorse, l'organizzazione deve documentare le informazioni concernenti quelle relative alle risorse di dati (data resources) utilizzate per il sistema di IA.			

La SoA diventa quindi una informazione documentata obbligatoria per le aziende che intendono certificarsi.

## Possibile integrazione degli standard ISO a supporto delle IA

Oltre allo standard ISO/IEC 42001 possono essere integrati ed applicati in modo trasversale e coordinato anche altri standard, quali la ISO 9001 per la gestione della qualità, ISO/IEC 27001

per la sicurezza delle informazioni, al fine di rafforzare i processi sia sotto il profilo organizzativo che documentale e facilitare il rispetto degli obblighi normativi.

A tal proposito il rapporto tecnico UNI CEI CEN/CLC/TR 18115 fornisce una panoramica sugli standard connessi ai temi della governance dei dati e della qualità dei dati, illustrando i collegamenti tra i numerosi standard e regolamenti, al fine di fornire un quadro informativo di riferimento.

In particolare, la governance dei dati e la qualità dei dati sono elementi interdipendenti, volti a influenzare le politiche organizzative e la gestione dei dati, contribuendo in modo determinante alla qualità dei processi e dei prodotti di dati.

La sezione 6 del report definisce la governance dei dati come “strategia, politiche, strutture decisionali e responsabilità, attraverso le quali gli accordi di governance dell’organizzazione operano sui dati” e specifica che il concetto di governance dei dati (pubblici e privati) include l’ambiente IT, l’ambiente intermedio ed il campo di applicazione specifico dell’IA.

Le questioni legate alla governance devono essere considerate in relazione alle normative e agli standard esistenti, nonché agli standard tecnici in corso di definizione.

Il concetto di qualità dei dati viene affrontato nella sezione 7 del rapporto, che lo definisce come “il grado in cui le caratteristiche dei dati soddisfano esigenze dichiarate e implicite quando utilizzate in condizioni specifiche”. L’insieme di tali caratteristiche - da considerare nelle diverse fasi del ciclo di vita dei dati – costituisce il modello di qualità dei dati, che fornisce un quadro per specificare i requisiti di qualità dei dati e valutare la qualità dei dati.

Il primo modello di qualità dei dati è stato definito dagli standard ISO/IEC 25012:2008 e ISO/IEC 25024:2015 ed è stato importato nello standard ISO/IEC 5259-2.

La qualità dei dati deve essere valutata considerando sia quanto disposto dall’art. 10 dell’AI Act sia i requisiti disposti dagli standard correlati ai dati sull’IA.

Il rapporto indica, inoltre, per ogni caratteristica di qualità dei dati dell’ISO/IEC 25012, la definizione e le relative misure di qualità, tratte dall’ISO/IEC 25024. Tali caratteristiche e relative misure sono importate nell’ISO/IEC 5259-2.

Caratteristica di qualità dei dati	Definizione	Misure di qualità
<b>Accuratezza</b>	i dati hanno attributi che rappresentano correttamente il valore reale	<ul style="list-style-type: none"> <li>• accuratezza sintattica</li> <li>• accuratezza semantica</li> <li>• garanzia di accuratezza</li> <li>• rischio di inaccuratezza del set di dati (in caso di presenza di valori anomali in un set di dati)</li> <li>• accuratezza del modello di dati</li> <li>• accuratezza dei metadati</li> <li>• intervallo di accuratezza dei dati</li> </ul>
<b>Completezza</b>	i dati hanno valori per tutti gli attributi previsti	<ul style="list-style-type: none"> <li>• completezza del record</li> <li>• completezza degli attributi</li> <li>• completezza del file di dati</li> <li>• completezza dei valori vuoti</li> <li>• record vuoti in un file di dati</li> <li>• completezza del modello di dati concettuale</li> <li>• completezza degli attributi del modello di dati concettuale</li> <li>• completezza dei metadati</li> </ul>
<b>Coerenza</b>	i dati hanno attributi coerenti con altri dati	<ul style="list-style-type: none"> <li>• integrità referenziale</li> <li>• coerenza del formato dei dati</li> <li>• rischio di incoerenza dei dati</li> <li>• coerenza dell'architettura</li> <li>• copertura della coerenza dei valori dei dati</li> <li>• coerenza semantica</li> </ul>
<b>Credibilità</b>	i dati hanno attributi che sono considerati veri e credibili dagli utenti	<ul style="list-style-type: none"> <li>• credibilità dei valori</li> <li>• credibilità della fonte</li> <li>• credibilità del dizionario dei dati</li> <li>• credibilità del modello di dati</li> </ul>

Caratteristica di qualità dei dati	Definizione	Misure di qualità
<b>Attualità</b>	i dati hanno attributi che hanno il giusto tempo	<ul style="list-style-type: none"> <li>• frequenza di aggiornamento</li> <li>• tempestività dell'aggiornamento</li> <li>• richiesta di aggiornamento degli elementi</li> </ul>
<b>Accessibilità</b>	i dati sono accessibili a persone che necessitano di tecnologia di supporto o di una configurazione speciale a causa di qualche disabilità	<ul style="list-style-type: none"> <li>• accessibilità dell'utente</li> <li>• accessibilità del dispositivo</li> <li>• accessibilità del formato dei dati</li> </ul>
<b>Conformità</b>	i dati hanno attributi che aderiscono a standard, convenzioni o regolamenti in vigore e regole simili relative alla qualità dei dati	conformità normativa di valore e/o formato, conformità normativa, a causa della tecnologia
<b>Riservatezza</b>	i dati hanno attributi che garantiscono che siano accessibili e interpretabili solo da utenti autorizzati	<ul style="list-style-type: none"> <li>• utilizzo della crittografia</li> <li>• non vulnerabilità</li> </ul>
<b>Efficienza</b>	i dati hanno attributi che possono essere elaborati e possono fornire i livelli di prestazioni previsti	<ul style="list-style-type: none"> <li>• formato efficiente dell'elemento dati</li> <li>• efficienza utilizzabile</li> <li>• efficienza del formato dati</li> <li>• efficienza di elaborazione dati</li> <li>• rischio di spazio sprecato</li> <li>• spazio occupato dalla duplicazione dei record</li> <li>• ritardo temporale dell'aggiornamento dei dati</li> </ul>

Caratteristica di qualità dei dati	Definizione	Misure di qualità
<b>Precisione</b>	i dati hanno attributi che sono esatti o che forniscono valori discriminanti	<ul style="list-style-type: none"> <li>• precisione dei valori dei dati</li> <li>• precisione del formato dati</li> </ul>
<b>Tracciabilità</b>	i dati hanno attributi che forniscono una traccia di controllo dell'accesso ai dati e di eventuali modifiche apportate ai dati	<ul style="list-style-type: none"> <li>• tracciabilità dei valori dei dati</li> <li>• tracciabilità dell'accesso degli utenti</li> <li>• valori dei dati</li> <li>• tracciabilità</li> </ul>
<b>Comprensibilità</b>	i dati hanno attributi che consentono di leggerli e interpretarli da parte degli utenti	<ul style="list-style-type: none"> <li>• comprensibilità dei simboli</li> <li>• comprensibilità semantica</li> <li>• comprensibilità del master</li> <li>• comprensibilità dei valori dei dati</li> <li>• comprensibilità del modello dei dati</li> <li>• comprensibilità della rappresentazione dei dati</li> <li>• comprensibilità dei dati master collegati</li> </ul>
<b>Disponibilità</b>	i dati hanno attributi che consentono di essere rinvenuti da utenti e/o applicazioni autorizzati	<ul style="list-style-type: none"> <li>• rapporto di disponibilità dei dati</li> <li>• probabilità di dati disponibili</li> <li>• disponibilità degli elementi dell'architettura</li> </ul>
<b>Portabilità</b>	i dati hanno attributi che consentono di installarli, sostituirli o spostarli da un sistema all'altro preservando la qualità esistente	<ul style="list-style-type: none"> <li>• rapporto di portabilità dei dati</li> <li>• portabilità dei dati prospettica</li> <li>• portabilità degli elementi dell'architettura</li> </ul>

Caratteristica di qualità dei dati	Definizione	Misure di qualità
<b>Ripristinabilità</b>	i dati hanno attributi che consentono di mantenere e preservare un livello specificato di operazioni e qualità, anche in caso di guasto	<ul style="list-style-type: none"> <li>• rapporto di recuperabilità dei dati</li> <li>• backup periodico</li> <li>• recuperabilità dell'architettura</li> </ul>

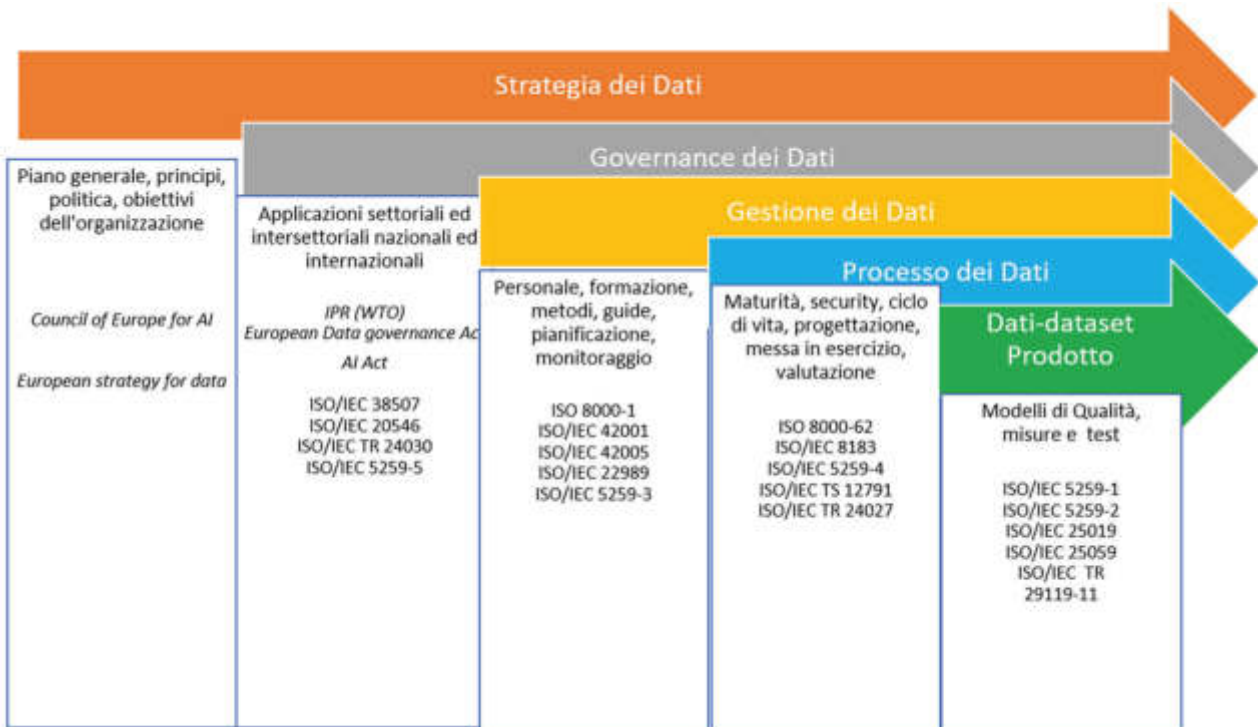
Il rapporto indica ulteriori caratteristiche che si riferiscono solo ai set di dati e le relative misure sono indicate nell'ISO/IEC 5259-2.

Caratteristica di qualità dei dati	Definizione	Misure di qualità
<b>Verificabilità</b>	i dati sono disponibili ai fini della conduzione di audit	<ul style="list-style-type: none"> <li>• record verificati</li> <li>• record verificabili</li> </ul>
<b>Identificabilità</b>	capacità di identificare un'informazione di identificazione personale	rapporto di identificabilità
<b>Bilanciamento</b>	si riferisce alla distribuzione dei campioni, al set di dati di addestramento e ai dati del mondo reale, alla categoria considerata	<ul style="list-style-type: none"> <li>• bilanciamento della luminosità</li> <li>• bilanciamento della risoluzione</li> <li>• bilanciamento delle immagini tra le categorie</li> <li>• bilanciamento del rapporto tra altezza e larghezza del riquadro di delimitazione</li> <li>• bilanciamento dell'area del riquadro di delimitazione della categoria</li> <li>• bilanciamento dell'area del riquadro di delimitazione del campione</li> </ul>

Caratteristica di qualità dei dati	Definizione	Misure di qualità
<b>Diversità</b>	differenza tra campioni, etichette, cluster	<ul style="list-style-type: none"> <li>• ricchezza dell'etichetta</li> <li>• abbondanza relativa dell'etichetta</li> <li>• ricchezza dei componenti</li> </ul>
<b>Efficacia</b>	risoluzioni delle immagini, quantità di immagini, soglia richiesta	<ul style="list-style-type: none"> <li>• efficacia della luminosità</li> <li>• efficacia della risoluzione</li> <li>• efficacia delle dimensioni della categoria</li> <li>• efficacia dell'area del riquadro di delimitazione</li> </ul>
<b>Provenienza</b>	informazioni sul luogo e l'ora di origine, derivazione o generazione di un set di dati, prova del set di dati o un record di proprietà passata e presente del set di dati	ad esempio numero di record con informazioni sulla provenienza rispetto al numero di record
<b>Rilevanza</b>	un set di dati è adatto per un dato contesto	<ul style="list-style-type: none"> <li>• rilevanza delle caratteristiche</li> <li>• rilevanza del record</li> </ul>
<b>Rappresentatività</b>	un campione riflette la popolazione target studiata	rapporto di rappresentatività: ad esempio confronto tra attributi nel campione e attributi nella popolazione
<b>Similarità</b>	il set di dati è rilevante per la classificazione, le attività di clustering, le differenze adeguate	<ul style="list-style-type: none"> <li>• somiglianza del campione</li> <li>• compattezza del campione</li> <li>• indipendenza del campione</li> </ul>

Caratteristica di qualità dei dati	Definizione	Misure di qualità
<b>Tempestività</b>	si riferisce alla latenza tra il tempo tra il fenomeno e la registrazione	tempestività degli elementi di dati

Di seguito una tabella che mappa i riferimenti legali europei con standard essenziali che possono avere un ruolo per la qualità dei dati.



## Come integrare i sistemi di gestione

Immaginiamo una logica di nesting applicabile ai sistemi di gestione generati dall'applicazione delle norme ISO disponibili e certificabili:

- 9001 – processi a supporto dello sviluppo, fornitura e uso dell'IA, in particolare per fornitori e catene collegate, processi legati al ciclo di vita del sw e dei dati, attenzione al cliente e comunicazioni in/out, knowledge ecc.
  - 22301 – continuità dei servizi collegati alle IA da un punto di vista del business, analisi impatti di business sull'azienda e relativi piani per i casi critici legati ad AI Act e tecnologie, violazioni legali e contrattuali, allucinazioni e bias, violazione di principi/obiettivi dichiarati della IA ecc.
    - 20000-1 – processi a supporto della gestione dei servizi IT collegati alle IA, in particolare per quelli di delivery e support (ITIL oriented)
      - 27001 – per la sicurezza delle infrastrutture a supporto delle IA esercite
      - 27701 - per la protezione dei dati personali gestiti a livello di infrastrutture
        - 27017 - per la sicurezza delle informazioni dei servizi in cloud (sistemi IA)
        - 27018 - per la sicurezza dei dati personali in cloud pubblici, in posizione di responsabile del trattamento

## Rapporti tra AI Act, ISO/IEC 42001, norme armonizzate e la legge 132/2025

Il panorama normativo volontario e quello cogente (quindi ISO/IEC 42001 e AI Act) è stato di recente sconvolto dall'approvazione definitiva del DDL 1146, pubblicato nella legge 132/2025. Lo sconvolgimento è dato dalla necessità di dover coordinare più fonti normative, non solo di rango diverso ma anche strutturalmente. Se la legge 132 si riferisce a specifici ambiti (come si vedrà successivamente) scollegati strutturalmente dal Regolamento, quest'ultimo invece

opera su un piano più globale. Piano che prescinde dalle deleghe governative e dai settori specifici di quella legge.

Un punto di contatto ulteriore, anche con riferimento alla ISO/IEC 42001 è dato dall'articolo 40 dell'AI Act, relativo alle norme tecniche (armonizzate). Per razionalizzare ulteriormente, una norma armonizzata è una norma europea che è stata adottata dalle organizzazioni europee di normazione (CEN/CENELEC/ETSI), sulla base di una richiesta fatta dalla Commissione, allo scopo di supportare il diritto derivato dell'unione europea.

Ora, il confine tra legge (europea) e norma (standardizzata) è stato oggetto di discussione sul tavolo delle istituzioni europee per diverso tempo ed è stato anche risolto una decina di anni fa nei seguenti termini: **“quando la Commissione presenta una richiesta di normazione tecnica, non delega alcun tipo di potere all'ente di normazione, bensì si limita a riconoscerne il loro specifico ruolo tecnico in tale processo.”**<sup>11</sup>

Una diversa soluzione, secondo la Corte di Giustizia dell'UE, avrebbe portato a inevitabili ricadute sul mercato interno se, oggettivamente, la norma armonizzata fosse stata l'unica opzione per accedere al mercato in un particolare stato membro.<sup>12</sup>

---

<sup>11</sup> Oever ten Niels, Milan Stefania, “*The Making of International Communication Standards: Towards a Theory of Power in Standardization*”, in *Journal of Standardisation*, pp. 1-27, 2022

<sup>12</sup> Sul punto si esprime la Corte di Giustizia dell'Unione europea (CGUE C-171/11, *Fra.bo*), la quale in *ratio decidendi* dimostrò come la norma armonizzata (volontaria) può diventare “obbligatoria” quando ogni altro mezzo per raggiungere la conformità risulti più lungo e oneroso. Questo è l'unico caso in cui una norma armonizzata assurge al rango di normativa giuridicamente vincolante.

Su questo punto la Corte di Giustizia<sup>13</sup> è decisamente diretta in punto da rapporti da diritto europeo, nazionale e norme tecniche, ritenendo la frizione tra normazione armonizzata e legislazione insanabile.<sup>14</sup>

Su questi aspetti l'Unione Europea ha cercato nel corso degli anni di colmare il divario, andando a snellire i processi di armonizzazione e norme tecniche, ma i lavori sono ancora in corso<sup>15</sup> e, con riferimento proprio al Regolamento AI, è necessario che si metta mano alla logica di co-regolamentazione lasciando la funzione legislativa al solo legislatore (europeo). Relegando la normazione tecnica ad un posto di raccordo e ausilio dove la prima non arriva.<sup>16</sup> Proseguendo sul tema del raccordo tra normazione volontaria, cogente e tecnica, la Commissione, già nel 2022, aveva provveduto a chiedere la redazione di una bozza di

---

<sup>13</sup> Sempre con riferimento a quanto in nota 12, la Corte (al punto 49 delle motivazioni) prosegue in questo modo: *“[il fatto che le raccordature nel settore della fornitura di acqua potabile de quibus] non siano assoggettate ad alcuna norma europea armonizzata non vuol dire che agli Stati membri spetti un potere discrezionale illimitato ai fini dell’elaborazione di norme tecniche nazionali concernenti le accordature medesime. Gli Stati membri sono piuttosto tenuti, nell’ambito della produzione normativa tecnica nazionale, a rispettare gli obblighi derivanti dalla libera circolazione delle merci. Qualora gli Stati membri potessero eludere tale obbligo di rispetto delle libertà fondamentali nell’elaborazione e applicazione di norme tecniche mediante un trasferimento – de facto – dei poteri ad associazioni private, ne deriverebbe un’applicazione non uniforme del diritto dell’Unione. Infatti, negli Stati membri in cui il potere di normazione e di certificazione resta riservato alle autorità in quanto funzione pubblica, essa dovrebbe essere esercitata nel rispetto delle libertà fondamentali. Negli Stati membri, invece, in cui tale compito venga trasferito – de facto – ad un’associazione di diritto privato, le libertà fondamentali resterebbero, a tal riguardo, inefficaci”.*

<sup>14</sup> Si faccia l’esempio del produttore/fornitore/deployer che non vuole conformarsi alle norme armonizzate, di fatto preferendo la dimostrazione di *compliance* con l’AI Act, il quale risulta al momento sguarnito di numerosi accorgimenti tecnici, i quali sono in mano alla Commissione e che saranno elaborati e pubblicati nei prossimi anni.

<sup>15</sup> Una panoramica dei lavori è rinvenibile qui <https://artificialintelligenceact.eu/standard-setting-overview/>.

<sup>16</sup> Veale Michael, Borgesius Zuiderveen J. Frederik, *“Demystifying the Draft EU Artificial Intelligence Act - Analysing the good, the bad, and the unclear elements of the proposed approach”*, in *Computer Law Review International*, pp. 97-112, 2021.

normazione tecnica a supporto di una IA sicura e affidabile. Richiesta che si è poi arenata al *draft* da parte di CEN, CENELEC e ETSI (questo solo come *collaborator*) del 2023.<sup>17</sup>

All'interno dei lavori della Commissione, nei risultati del periodo tra il 2022 e il 2025 si sono menzionati alcuni punti di intervento, specie anche alla luce dell'arresto sui lavori di armonizzazione verso l'AI Act.<sup>18</sup> L'arresto si è poi aggravato anche quanto le aziende, con sede in UE, hanno chiesto, tramite una lettera aperta<sup>19</sup>, di arrestare l'efficacia dell'AI Act fino al completamento della normativa armonizzata e una maggiore certezza in punto di regole, sanzioni e linee guida da parte della Commissione.

Proseguendo sul percorso tracciato ad inizio capitolo, il panorama normativo-legislativo, a livello interno, è stato recentemente inciso dalla legge 132/2025. Il quale nonostante condivida alcuni principi di fondo col Regolamento (ma anche alcuni più di importanza interna, come l'uso dell'IA all'interno delle Pubbliche Amministrazioni), si pone in realtà su segmenti operativi diversi.

Tra i principali temi di primaria importanza:

- Il rapporto tra le Autorità indipendenti (AgiD e ACN) coinvolte;
- Le disposizioni in tema di professioni intellettuali e informativa sull'uso di IA;
- L'introduzione di una nuova fattispecie di reato e la modifica di alcune normative di settore (come in punto di proprietà intellettuale);
- Ulteriori aspetti di raccordo tra IA e attività giudiziaria;
- Rapporti di sinergia in ambito cybersecurity.

Rimangono poi sul tavolo alcuni aspetti di stampo finanziario (come la clausola sull'invarianza finanziaria e alcuni profili lavoristici, come l'Osservatorio sull'IA nel mondo del lavoro), ma

---

<sup>17</sup> Commission implementing decision on a standardisation request to the European Committee for Standardisation and the European Committee for Electrotechnical Standardisation in support of Union policy on artificial intelligence ([https://ec.europa.eu/transparency/documents-register/detail?ref=C\(2023\)3215&lang=en](https://ec.europa.eu/transparency/documents-register/detail?ref=C(2023)3215&lang=en)).

<sup>18</sup> Si faccia riferimento al report seguente: [https://ec.europa.eu/info/law/better-regulation/have-your-say/initiatives/13446-European-standardisation-evaluation\\_en](https://ec.europa.eu/info/law/better-regulation/have-your-say/initiatives/13446-European-standardisation-evaluation_en).

<sup>19</sup> <https://aichampions.eu/>

anche sul versante delle deleghe al governo (per materie davvero importanti come diritto penale, procedura penale, dati e algoritmi) ed in materia sanitaria (ad Agenas per la pianificazione e l'assistenza sanitaria).

Sull'efficacia della legge 132/2025 nel contesto interno è ancora presto per pronunciarsi e sul punto la letteratura deve ancora iniziare a prendere cognizione dello stato dell'arte reale successivo alla sua entrata in vigore.

Concludendo, la situazione in questo momento, nei rapporti tra AI Act, ISO/IEC 42001, norme armonizzate e DDL pare presentare ben più di qualche punto irrisolto e di non immediata risoluzione. La ragione di questa considerazione va ricercata su più livelli, ovvero:

- Tra Unione europea e Stati membri, per i motivi che già sono stati elencati sul presunto carattere squisitamente politico dell'AI Act;
- Tra Unione europea e OEN, analogamente, per la lentezza dei lavori e la mancata *guidance* nel processo di armonizzazione;
- Tra UE e aziende, per il mancato coinvolgimento e dialogo collaborativo;
- Tra azienda e OEN, per i medesimi motivi e in aggiunta ad una componente competitiva;
- Tra legislatore italiano e legislatore europeo, per aver trasposto un Regolamento, che di fatto poneva più interrogativi che risposte, con una legge, che amplifica questi interrogativi ed anzi ne pone ulteriori sia a causa delle disposizioni inserite sia a causa dell'eccesso di delega e di ricorso a fonti secondarie.

Si tratta come si può facilmente immaginare di un dialogo che si innesta per forza di cose su più protagonisti e che necessiterà, nell'immediato futuro, di un cospicuo piano di risoluzione. Per questi motivi, in assenza di una risposta definitiva e forse anche soddisfattiva, si può ora passare ad alcune considerazioni preliminari all'esame del *case study*, di cui si era anticipato nelle pagine precedenti, relativo all'implementazione di più standard di gestione in un'ottica di *nesting*.

### **Considerazioni per una definizione orientata di "Sistema di IA"**

Ricollegandosi alle considerazioni di cui ai precedenti paragrafi, con riferimento alla definizione di Sistema di IA, si può circoscrivere gran parte delle distorsioni operative ed interpretative collegate alle norme di cui in argomento, siano esse volontarie o cogenti.

Il principale motivo di confusione è, probabilmente, dovuto alla mancata comprensione delle destinazioni d'uso dei due documenti, l'AI Act quale regolamento europeo direttamente applicabile negli Stati membri e dunque anche in Italia e la ISO/IEC 42001 quale standard di adozione volontaria.

Quindi due posizioni ontologicamente diverse, non opposte, semmai complementari, in sostanza potremmo dire che sono due facce della stessa medaglia:

- Il Regolamento guarda al Sistema di IA;
- la norma ISO guarda ai processi organizzativi che sono utilizzati per il Sistema AI.

Per fare un esempio estremamente semplice: il Regolamento stabilisce le regole per costruire, fornire e utilizzare un prodotto/servizio, mentre lo standard ISO indica a chi lo produce/eroga/utilizza cosa tenere in considerazione per fa sì che il prodotto/servizio non solo funzioni come atteso, ma che sia anche in linea con il Regolamento.

Una considerazione dettata dall'esperienza è chiara: aziende certificate non necessariamente generano prodotti/servizi adeguati. Tuttavia, anche prodotti/servizi eccellenti non necessariamente implicano aziende certificate. Sono aspetti complementari e sarebbe auspicabile garantirli entrambi per aumentare i margini di sicurezza di qualsiasi prodotto/servizio.

Le differenze sostanziali stanno nella loro natura e nelle conseguenze nel caso di mancata soddisfazione di quanto in esse contenuto.

Il Regolamento prevede sanzioni, di varia natura e grado, capaci di impedire che un Sistema AI possa essere commercializzato e utilizzato se non rispetta le regole. Si tratta di obblighi e non di scelte. Il rispetto delle leggi è definito come compliance, in quanto obblighi cogenti.

Lo standard ISO è per sua natura volontario, in caso di inadeguatezze (non conformità) non si ottiene la certificazione, oppure la si posticipa fino a quando tutti gli elementi non rientrano nei parametri necessari, incluso il rispetto del Regolamento (per quanto applicabile). Il rispetto delle norme ISO è definito come conformità.

Compliance e conformità non sono la stessa cosa, da qui la differenza anche nel resto della letteratura tecnica tra compliance e conformity. Fornendo un po' di contesto, a livello di

normazione tecnica, nella prima versione della ISO/IEC 17021 del 2006<sup>20</sup>, con riferimento agli obiettivi di un audit Stage 2 (la parte dell'audit di certificazione dedicata al funzionamento del sistema di gestione).

Qualche anno più tardi, nella versione del 2011, si troverà la medesima interpretazione<sup>21</sup> di cui al paragrafo precedente.<sup>22</sup> Questo disallineamento continuerà a permanere anche nella versione attuale del 2015, esattamente con la stessa formulazione (vedi note). In termini prettamente pratici potremmo dire che compliance è più vicino a “rispetto della normativa” piuttosto che a “soddisfazione di un requisito”.

Su un versante di sistemi di gestione, la situazione si è complicata ulteriormente con la ISO 19600:2014 (quella che oggi è diventata la ISO 37301:2021), la quale nella definizione di *compliance* ha inteso questa come “*meeting all the organization's compliance requirements*”. Di fatto estendendo il concetto di *legal compliance* a tutte le prescrizioni a cui un'Organizzazione deve conformarsi. L'equivoco terminologico, di cui anche sopra, è stato parzialmente risolto proprio dalla ISO 37301, all'interno delle definizioni.

---

<sup>20</sup> La versione in inglese enunciava “*The client's management system and performance as regards **legal compliance***”, laddove la versione italiana recitava “*il Sistema di gestione del cliente e le prestazioni con riferimento al rispetto delle **prescrizioni legali***”.

<sup>21</sup> Vedi Nota 15

<sup>22</sup> Nella versione inglese si troverà “*A management system **certification audit is not a legal compliance audit***” che in italiano sarebbe stata resa con “*Un audit di **certificazione di Sistema di Gestione non** è un audit di **conformità legale***”.

Ai punti 3.16 e 3.17 si sofferma proprio sulla differenza tra “non conformità” (mancato soddisfacimento di un requisito [della norma]) e “non compliance” (mancato soddisfacimento di un obbligo di compliance). Al punto 3.25 specifica quali siano questi obblighi di compliance, ovvero:

- Requisiti mandatori/cogenti cui l'Organizzazione deve obbligatoriamente conformarsi (***mandatory has to comply with***);
- Requisiti ai quali un'Organizzazione ha deciso volontariamente di conformarsi (***voluntarily chooses to comply with***).

Al di là di questi aspetti sulle differenze concettuali tra *compliance* e conformità, il discorso non ha effetto nei confronti del Regolamento AI Act e della ISO 42001. Vi è infatti concordanza sul fatto che uno sia un requisito cogente e l'altro volontario, a prescindere dal dibattito terminologico di cui al presente capitolo.

### **Chi verifica?**

Un altro punto fondamentale, connesso con quanto visto sopra, è chi si occupa di verificare il rispetto del Regolamento e chi si occupa di verificare la conformità alla ISO.

La verifica del rispetto del regolamento è affidata alle Autorità (ACN e AgID per l'Italia).

La verifica della conformità rispetto agli standard ISO è invece affidata agli organismi di certificazione accreditati. Un organismo di certificazione è una entità indipendente che opera in un contesto regolato da altri standard ISO (nel caso specifico dallo standard ISO/IEC 17021-1 e altri). Questo organismo è a sua volta verificato da una entità nazionale che opera secondo il Regolamento Europeo 765/2008. Questa entità per l'Italia è Accredia, a sua volta soggetta a controlli da una entità Europea (EA) e da una intercontinentale (IAF).

## Sistema AI

La definizione di Sistema AI è sostanzialmente la stessa sia a livello di Regolamento sia a livello di standard. L'unica differenza, che può aiutare nel comprendere l'estrema mutevolezza del concetto di sistema AI è data dalla prima versione dell'AI Act, ossia la bozza del 21 aprile 2021 da parte della Commissione.<sup>23</sup> L'eccessiva mutevolezza si vide poi anche nella definizione proposta dal Consiglio nell'aprile 2022.<sup>24</sup> La differente ampiezza nelle due definizioni va ricercata in una singola causa storica: il lancio di quello che è chiaramente LLM più famoso, ChatGPT, lanciato a novembre 2022.

L'emersione di un *software* talmente *disruptive* da cambiare totalmente le carte in gioco, ChatGPT (come tutti gli LLM) non rientrava infatti né nella versione vecchia della Commissione né in quella del Consiglio. Ed è per questo motivo che nella versione attuale dell'AI Act esiste una parte dedicata alle GPAI, per questi motivi esistono i codici di condotta, per questo motivo c'è voluto più di un passaggio per arrivare alla definizione in vigore attualmente.

---

<sup>23</sup> In tale sede si scriveva, infatti, come Sistema AI fosse *“un software sviluppato con una o più delle tecniche e degli approcci elencati nell'allegato 1, che può, per una determinata serie di obiettivi definiti dall'uomo, generare output quali contenuti, previsioni, raccomandazioni o decisioni che influenzano gli ambienti con cui interagiscono”* (a cui faceva seguito un allegato di approcci e tecniche per lo sviluppo dell'IA);

<sup>24</sup> Ovvero *“un sistema progettato per funzionare con elementi di autonomia e che, sulla base di dati e input forniti da macchine e/o dall'uomo, deduce come raggiungere una determinata serie di obiettivi avvalendosi di approcci di apprendimento automatico e/o basati sulla logica e sulla conoscenza, e produce output generati dal sistema quali contenuti (sistemi di IA generativi), previsioni, raccomandazioni o decisioni, che influenzano gli ambienti con cui il sistema di IA interagisce”*,

Conclusa questa parte introduttiva, si possono ora passare in rassegna le principali definizioni di Sistema AI. Si è altresì inclusa la definizione restituita dalla Convenzione quadro del Consiglio d'Europa sull'intelligenza artificiale e i diritti umani, la democrazia e lo Stato di diritto.

<p>AI ACT art. 3.1</p>	<p>«sistema di IA»: un sistema automatizzato progettato per funzionare con livelli di autonomia variabili e che può presentare adattabilità dopo la diffusione e che, per obiettivi espliciti o impliciti, deduce dall'input che riceve come generare output quali previsioni, contenuti, raccomandazioni o decisioni che possono influenzare ambienti fisici o virtuali;</p>
<p>Legge 132/2025 (DDL 1146)</p>	<p>Art. 2. (Definizioni) 1. Ai fini della presente legge, si intendono per: a) sistema di intelligenza artificiale: il sistema definito dall'articolo 3, punto 1), del regolamento (UE) 2024/1689;</p>
<p>ISO/IEC 42001 (più precisamente ISO/IEC 22989 terminologia e concetti)</p>	<p>3.1.4 sistema di intelligenza artificiale sistema ingegnerizzato che genera output come contenuti, previsioni, raccomandazioni o decisioni per un dato insieme di obiettivi definiti dall'uomo. Nota 1: il sistema ingegnerizzato può utilizzare varie tecniche e approcci legati all'intelligenza artificiale, sviluppare un modello per rappresentare dati, conoscenze, processi, ecc. che possono essere utilizzati per svolgere compiti. Nota 2: i sistemi di IA sono progettati per funzionare con diversi livelli di automazione.</p>

Consiglio d'Europa (CM(2024)52) - Convenzione quadro del Consiglio d'Europa sull'intelligenza artificiale	Art. 2 "Definition of artificial intelligence systems" a machine-based system that for explicit or implicit objectives, infers, from the input it receives, how to generate outputs such as predictions, content, recommendations or decisions that may influence physical or virtual environments. Different artificial intelligence systems vary in their levels of autonomy and adaptiveness after deployment.
---	---

Il Sistema AI è quindi un prodotto/servizio che può rientrare a pieno titolo anche ne "La guida blu all'attuazione della normativa UE sui prodotti 2022" (2022/C 247/01) e nel "New legislative framework" del 2008 che richiama le attività di certificazione accreditata per la conformità: Abbiamo quindi, da un lato Regolamento, Direttive e leggi che impongono determinate caratteristiche di "sicurezza" e dall'altro un sistema di standard ISO che permette alle aziende produttrici/erogatrici/utilizzatrici di predisporre i processi di governo di tali attività in modo da soddisfare sia gli standard ISO sia gli obblighi giuridici.

Ovviamente i sistemi di controllo sono diversi essendo diverse le origini delle fonti di riferimento.

Un Sistema AI, inteso come prodotto/servizio, prevede l'esistenza di un fornitore, cioè di una organizzazione che ne assume le relative responsabilità di produzione/erogazione. Qualsiasi prodotto/servizio deve avere un utilizzatore per essere considerato "operativo" (la regolamentazione per i prodotti/servizio non destinati al "consumo" è diversa incluse le responsabilità derivanti in caso di problemi - responsabilità da prodotto difettoso).

Questi tre ruoli: sviluppatore/produttore, erogatore, utilizzatore sono ben chiari in tutti i documenti citati. Pertanto, non vi sono, in tal senso, potenziali conflitti tra AI Act e ISO/IEC 42001. Sono anzi complementari e non antagoniste.

### **Dove sorgono i problemi?**

Quali siano i problemi endemici interni allo stesso AI Act è stato già visto, ma quali sono invece quelli per le aziende? I problemi, infatti, sorgono nel momento in cui un imprenditore o un amministratore di una azienda privata affronta questi documenti.

La prima causa è la complessità, la seconda è il disallineamento.

Facciamo un esempio per comprendere l'affermazione appena fatta.

Nell'AI Act si parla di "Sistema di gestione della Qualità" (art. 17). Almeno 80.000 aziende in Italia (fonte Accredia, verificabile anche attraverso le CCIAA) sono dotate di un Sistema di Gestione della Qualità, per un totale di oltre 157.000<sup>25</sup> certificati in circolazione (ogni azienda può avere più certificati).

Per queste aziende il termine "Sistema di Gestione della Qualità" riporta allo standard ISO 9001 per cui sono certificate; infatti, l'intestazione della ISO 9001 è proprio: "Sistemi di gestione per la qualità".

Ogni azienda certificata conosce bene il significato di qualità, di sistema di gestione, prodotto/servizio, processi ecc. Ognuna delle aziende certificate viene verificata con cadenza almeno annuale dal proprio organismo di certificazione e ogni 3 anni è tenuta a rinnovare il tutto, pena la perdita del certificato. Ogni azienda certificata e coinvolta nelle attività inerenti all'AI capisce benissimo la terminologia e ha già predisposto quanto necessario.

Proviamo di seguito a collocare le varie parti dell'Art. 17 dell'AI Act rispetto ai requisiti della ISO 9001 (supponendo che questa sia utilizzata per supportare sviluppo/produzione, erogazione e utilizzazione di Sistemi AI):

---

<sup>25</sup> ISO Survey 2024 <https://www.iafcertsearch.org/services/iso-survey>

Art. 17 AI Act	Requisiti equivalenti ISO 9001
<p>1.a) una strategia per la conformità normativa, compresa la conformità alle procedure di valutazione della conformità e alle procedure per la gestione delle modifiche dei sistemi di IA ad alto rischio;</p>	<p>4 Contesto dell'organizzazione 5 Leadership 6.1.1 Azioni per affrontare rischi e opportunità 6.3 Pianificazione delle modifiche</p>
<p>1.b) le tecniche, le procedure e gli interventi sistematici da utilizzare per la progettazione, il controllo della progettazione e la verifica della progettazione del sistema di IA ad alto rischio;</p>	<p>8.2 Requisiti per i prodotti e i servizi 8.3 Progettazione e sviluppo di prodotti e servizi 8.4 Controllo dei processi, prodotti e servizi forniti dall'esterno</p>
<p>1.c) le tecniche, le procedure e gli interventi sistematici da utilizzare per lo sviluppo e per il controllo e la garanzia della qualità del sistema di IA ad alto rischio;</p>	<p>8.2 Requisiti per i prodotti e i servizi 8.4 Controllo dei processi, prodotti e servizi forniti dall'esterno 8.5 Produzione ed erogazione dei servizi 8.7 Controllo degli output non conformi</p>
<p>1.d) le procedure di esame, prova e convalida da effettuare prima, durante e dopo lo sviluppo del sistema di IA ad alto rischio e la frequenza con cui devono essere effettuate;</p>	<p>8.2 Requisiti per i prodotti e i servizi 8.4 Controllo dei processi, prodotti e servizi forniti dall'esterno 8.5 Produzione ed erogazione dei servizi 8.6 Rilascio di prodotti e servizi 8.7 Controllo degli output non conformi</p>

Art. 17 AI Act	Requisiti equivalenti ISO 9001
<p>1.e) le specifiche tecniche, comprese le norme, da applicare e, qualora le pertinenti norme armonizzate non siano applicate integralmente, o non includano tutti i requisiti pertinenti di cui alla sezione 2, i mezzi da usare per garantire che il sistema di IA ad alto rischio sia conforme a tali requisiti;</p>	<p>9.1 Monitoraggio, misurazione, analisi e valutazione 9.2 Audit interno 10.2 Non conformità e azioni correttive</p>
<p>1.f) i sistemi e le procedure per la gestione dei dati, compresa l'acquisizione, la raccolta, l'analisi, l'etichettatura, l'archiviazione, la filtrazione, l'estrazione, l'aggregazione, la conservazione dei dati e qualsiasi altra operazione riguardante i dati effettuata prima e ai fini dell'immissione sul mercato o della messa in servizio di sistemi di IA ad alto rischio;</p>	<p>8.4 Controllo dei processi, prodotti e servizi forniti dall'esterno 8.5 Produzione ed erogazione dei servizi 8.6 Rilascio di prodotti e servizi 8.7 Controllo degli output non conformi</p>
<p>1.g) il sistema di gestione dei rischi di cui all'articolo 9;</p>	<p>6.1.1 Azioni per affrontare rischi e opportunità 6.2 Obiettivi per la qualità e pianificazione per il loro raggiungimento</p>

Art. 17 AI Act	Requisiti equivalenti ISO 9001
1.h) la predisposizione, l'attuazione e la manutenzione di un sistema di monitoraggio successivo all'immissione sul mercato a norma dell'articolo 72;	8.4 Controllo dei processi, prodotti e servizi forniti dall'esterno 8.5 Produzione ed erogazione dei servizi 8.6 Rilascio di prodotti e servizi 8.7 Controllo degli output non conformi 9.1 Monitoraggio, misurazione, analisi e valutazione
1.i) le procedure relative alla segnalazione di un incidente grave a norma dell'articolo 73;	9.1 Monitoraggio, misurazione, analisi e valutazione 9.2 Audit interno 10.2 Non conformità e azioni correttive
1.j) la gestione della comunicazione con le autorità nazionali competenti, altre autorità pertinenti, comprese quelle che forniscono o sostengono l'accesso ai dati, gli organismi notificati, altri operatori, clienti o altre parti interessate;	8.2 Requisiti per i prodotti e i servizi 7.4 Comunicazione 9.1 Monitoraggio, misurazione, analisi e valutazione 10.2 Non conformità e azioni correttive
1.k) i sistemi e le procedure per la conservazione delle registrazioni e di tutte le informazioni e la documentazione pertinenti	7.5 Informazioni documentate
1.l) la gestione delle risorse, comprese le misure relative alla sicurezza dell'approvvigionamento	7 Supporto 8.4 Controllo dei processi, prodotti e servizi forniti dall'esterno

Art. 17 AI Act	Requisiti equivalenti ISO 9001
<p>1.m) un quadro di responsabilità che definisca le responsabilità della dirigenza e di altro personale per quanto riguarda tutti gli aspetti elencati nel presente paragrafo</p>	<p>5.3 Ruoli, responsabilità e autorità nell'organizzazione                      7.1.2 Persone                      7.1.6 Conoscenza organizzativa                      7.2 Competenza                      7.3 Consapevolezza</p>
<p>2.L'attuazione degli aspetti di cui al paragrafo 1 è proporzionata alle dimensioni dell'organizzazione del fornitore. I fornitori rispettano, in ogni caso, il grado di rigore e il livello di protezione necessari per garantire la conformità dei loro sistemi di IA ad alto rischio al presente regolamento.</p>	<p>4.4 Sistema di gestione per la qualità e relativi processi                      6.1.1 Azioni per affrontare rischi e opportunità                      8.2 Requisiti per i prodotti e i servizi                      8.4 Controllo dei processi, prodotti e servizi forniti dall'esterno                      8.7 Controllo degli output non conformi                      9.1 Monitoraggio, misurazione, analisi e valutazione                      9.2 Audit interno                      10.2 Non conformità e azioni correttive</p>

Art. 17 AI Act	Requisiti equivalenti ISO 9001
<p>3.I fornitori di sistemi di IA ad alto rischio soggetti agli obblighi relativi ai sistemi di gestione della qualità o a una funzione equivalente a norma del pertinente diritto settoriale dell'Unione possono includere gli aspetti elencati al paragrafo 1 nell'ambito dei sistemi di gestione della qualità stabiliti a norma di tale diritto.</p>	<p>4.4 Sistema di gestione per la qualità e relativi processi                      6.1.1 Azioni per affrontare rischi e opportunità                      8.2 Requisiti per i prodotti e i servizi                      8.4 Controllo dei processi, prodotti e servizi forniti dall'esterno                      8.7 Controllo degli output non conformi                      9.1 Monitoraggio, misurazione, analisi e valutazione                      9.2 Audit interno                      10.2 Non conformità e azioni correttive</p>
<p>4.Per i fornitori che sono istituti finanziari soggetti a requisiti in materia di governance, dispositivi o processi interni stabiliti a norma del diritto dell'Unione in materia di servizi finanziari, l'obbligo di istituire un sistema di gestione della qualità, ad eccezione del paragrafo 1, lettere g), h) e i), del presente articolo, si considera soddisfatto se sono soddisfatte le regole sui dispositivi o i processi di governance interna a norma del pertinente diritto dell'Unione in materia di servizi finanziari. A tal fine, si tiene conto delle norme armonizzate di cui all'articolo 40.</p>	<p>4.4 Sistema di gestione per la qualità e relativi processi                      6.1.1 Azioni per affrontare rischi e opportunità                      8.2 Requisiti per i prodotti e i servizi                      8.4 Controllo dei processi, prodotti e servizi forniti dall'esterno                      8.7 Controllo degli output non conformi                      9.1 Monitoraggio, misurazione, analisi e valutazione                      9.2 Audit interno                      10.2 Non conformità e azioni correttive</p>

La spiegazione di dettaglio sarebbe lunga e articolata ma ogni organismo di certificazione, accreditato in Italia da Accredia, svolgerebbe esattamente tutte le verifiche necessarie per assicurare il rispetto del Regolamento (almeno per il campione oggetto di certificazione) oltre che per la ISO 9001.

Al netto delle due cause di problemi emerse sopra, sorge spontanea la seguente domanda: c'è bisogno davvero di un nuovo standard? Ovviamente no, ne esiste già uno perfettamente adattabile ed integrabile con altri standard specifici che potrebbero ampliare il grado di sicurezza delle AI: ISO/IEC 27001, ISO/IEC 20000-1, ISO/IEC 42001 ecc.

Tuttavia, a livello Europeo si sta lavorando ad una proposta di norma che possa comunque soddisfare anche questo aspetto, in particolare ci riferiamo alla prEN18286<sup>26</sup>.

### **Certificazione di sistema vs certificazione di prodotto**

Un ulteriore elemento di confusione è la certificazione. Si era già anticipato tale elemento in apertura, qui viene espanso a livello di più sistemi ISO.

La certificazione di un sistema di gestione ISO 9001, ISO/IEC 27001, ISO/IEC 42001 ecc. è garantita dagli organismi di certificazione, sulla base della ISO/IEC 17021-1 e altri standard associati.

La certificazione dei prodotti/servizi (come ad es. per eIDAS) è garantita dagli organismi di certificazione, sulla base della ISO/IEC 17065 ed eventuali altri standard (ad es. ETSI per eIDAS). Peraltro, la certificazione di prodotto/servizio vede sempre una Autorità nazionale responsabile di definire e governare le modalità, ad es. per i servizi relativi al Regolamento eIDAS l'autorità competente è AgiD/ACN e gli organismi di certificazione svolgono il lavoro operativo, disponendo delle competenze e delle risorse necessarie (umane e tecniche) nonché degli accreditamenti necessari (Reg. 765/2008) attraverso Accredia.

Le due certificazioni sono profondamente diverse, anche perché destinate ad ambiti diversi; ad esempio, la ISO/IEC 17021-1 prevede audit a campione rispetto alle attività oggetto di

---

<sup>26</sup> <https://www.cencenelec.eu/news-events/news/2025/brief-news/2025-10-23-ai-standardization/>

certificazione; il campionamento non deve essere però inteso come un fenomeno riduttivo ma risulta invece rappresentativo di una affermazione molto semplice “se il sistema di gestione è efficace e conforme qualsiasi prodotto/servizio sarà in grado di dimostrare tali caratteristiche”. Siamo quindi di fronte ad un elevatissimo rischio per l'organizzazione nel caso in cui non fossero effettivamente rispondenti ai requisiti dichiarati. Il campionamento è quindi uno sprone ad assicurare che tutto quanto sia conforme, non potendo stabilire a priori cosa l'organismo deciderà di verificare.

Nel caso della ISO/IEC 17065 invece la verifica è sistematica, cioè ogni elemento dichiarato o richiesto deve essere dimostrato in ogni sua parte. Ne consegue un'attività molto dettagliata, con molte giornate e con team estremamente focalizzati al prodotto/servizio.

Anche in questo senso si capisce la complementarità delle due certificazioni e quindi dei vantaggi del doppio approccio.

Sarebbe quindi auspicabile una certificazione del Sistema AI (secondo quanto indicato nell'AI Act), nella logica di certificazione accreditata assicurata da un sistema di gestione integrato, anche questo certificato in maniera accreditata, che soddisfi la ISO 9001 e la ISO/IEC 42001, possibilmente con ISO/IEC 27001 e ISO/IEC 20000-1 (magari in momenti diversi ma programmati in un lasso di tempo predefinito). La fiducia che si ripone in un approccio di questo tipo riflette certamente il miglioramento del panorama normativo, questo per almeno una serie di considerazioni che si possono riassumere in questo modo:

- La crisi tra diversi sistemi di gestione renderebbe praticamente identificabile l'obiettivo definitorio sul Sistema AI;
- Il lavoro delle OEN, in questo momento “fermo”, sarebbe valorizzato dal “ponte” tra la normativa europea (vincolante) e la volontaria (questo sistema di gestione integrato ipotetico);
- Non vi sarebbe alcuna usurpazione di funzioni tra soggetti e *regulation*, giacché tutti i partecipanti “giocherebbero” la stessa partita, questa volta però in un'ottica davvero collaborativa;
- Infine, ogni standard ISO andrebbe a coprire le parti richieste dal regolamento, ampliando lo spettro di sicurezza, efficacia e conformità.

## Case study

Si tratta di un mero esercizio speculativo (non esaustivo) per dimostrare come ogni norma citata contribuisca in modo significativo al miglioramento di quanto stabilito in maniera più ristretta dalla ISO/IEC 42001, ampliando però efficacia e garanzie per l'IA e per i processi sottesi al suo sviluppo e utilizzazione.

Ipotizziamo che la IA sia stata sviluppata per un uso/ambito specifico e che il cliente, multinazionale con sede in Italia e siti in tutto il mondo, sia anche l'utilizzatore. L'IA è stata sviluppata in Italia per essere utilizzata nel solo territorio UE (quindi soggetta a regolamenti, direttive e leggi applicabili per l'uso e ambito specifico). L'IA è dotata di Model Card.

La nostra IA "Cerca e seleziona candidati", nome di fantasia che descrive la funzionalità della IA, utilizza un predeterminato set di dati per analizzare i CV dei candidati, identificare quelli più vicini alle esigenze dell'utilizzatore e, nel rispetto dei requisiti cogenti applicabili, estrarre i profili più idonei alle successive fasi di selezione. La nostra IA deve rispettare i principi di base:

- equità e pari opportunità
- responsabilità
- trasparenza e spiegabilità
- sicurezza e privacy
- interrompibilità.

Questi principi sono garantiti al cliente utilizzatore. Pertanto, lo sviluppo e l'uso responsabile devono essere garantiti e nel rispetto di tali principi.

Una delle funzionalità della IA prevede test psicometrici sui candidati per valutarne alcuni parametri personali. L'IA è stata sviluppata nel 2020 e da allora non subisce modifiche rilevanti.

L'IA "gira" in ambiente cloud dell'utilizzatore e non necessita di supporto da parte del produttore, in caso di necessità la IA ha funzionalità specifiche per l'intervento umano, che può non solo interrompere l'IA ma anche chiedere intervento del produttore, ad es. in caso di allucinazioni, bias, situazioni anomale, incidenti legati alla cybersecurity e/o alla privacy ecc. Gli interventi devono essere garantiti nella modalità 5x12 (dal lunedì al venerdì, dalle ore 8:00 alle ore 20:00 – periodi di esercizio della funzione HR del cliente).

Produttore e cliente/utente hanno preconcordato tutti i requisiti sopraelencati e realizzato una Proof of Concept per consolidare lo scenario.

Per la realizzazione della IA il produttore utilizza una delle IA di mercato integrata in una soluzione propria. L'algoritmo è stato concordato con il cliente così come le misurazioni necessarie. I dati di test sono forniti dal cliente (CV parzialmente anonimizzati dei candidati fittizi e di candidati reali, CV del personale interno, CV dei consulenti – per tutti autorizzazioni concesse).

Il produttore ha sviluppato l'IA in un ambiente cloud speculare a quello di esercizio in cui il cliente lo utilizzerà.

Fissati questi assunti possiamo analizzare:

- come i vari standard potrebbero garantire, grazie alle loro caratteristiche specifiche, il rispetto di tutto quanto necessario;
- le conseguenze in termini di AI Act.

## ISO 9001

È la norma che permette di rappresentare i processi di una organizzazione in relazione a prodotti/servizi (per semplificare il concetto).

Tra i requisiti della norma abbiamo quelli riferiti al cliente (e utente nel nostro caso) e più precisamente:

### **8.2.1 Comunicazione con il cliente**

Questo requisito include:

- la fornitura di informazioni relative ai prodotti e servizi, nel nostro caso alla IA “Cerca e seleziona candidati”;
- la gestione delle richieste, contratti o ordini, comprese le modifiche;
- l'ottenimento, dal cliente, di informazioni di ritorno relative ai prodotti e servizi, compresi i reclami del cliente stesso, nel nostro caso alla IA “Cerca e seleziona candidati”;
- la gestione o la tenuta sotto controllo della proprietà del cliente, nel nostro caso la IA opererà nel cloud del cliente possiamo quindi associare questo elemento al periodo di test e validazione che potrebbe essere eseguito nell'ambito cloud del cliente;

- la definizione di specifici requisiti per le azioni di emergenza, quando pertinente, nel nostro caso intervento umano (interrompibilità) in caso di allucinazioni, bias, situazioni anomale, incidenti legati alla cybersecurity e/o alla privacy ecc.

### **8.2.2 Determinazione dei requisiti relativi ai prodotti e servizi**

Questo requisito include:

a) siano definiti i requisiti dei prodotti e servizi, compresi:

1) ogni eventuale requisito cogente applicabile, nel nostro caso AI Act, GDPR, Statuto ei Lavoratori....

2) quelli ritenuti necessari dall'organizzazione, nel nostro caso i principi dell'IA

b) l'organizzazione sia in grado di corrispondere a quanto essa dichiara in relazione ai prodotti e servizi offerti, assumiamo che l'organizzazione abbia esperienza consolidata nella progettane e sviluppi di sistemi IA

### **8.2.3 Riesame dei requisiti relativi ai prodotti e servizi**

L'organizzazione deve assicurare che essa possiede la capacità di soddisfare i requisiti dei prodotti e servizi da offrire ai clienti, nel nostro caso vale quanto detto per il punto b) al precedente requisito.

Prima di impegnarsi a fornire prodotti e servizi al cliente, l'organizzazione deve condurre un riesame che comprenda:

a) i requisiti specificati dal cliente, compresi i requisiti per le attività di consegna e post-consegna, nel nostro caso i requisiti sono preconcordati con il cliente/utente incluse le attività di test/validazione in ambiente cloud del cliente e per l'assistenza successiva;

b) i requisiti non stabiliti dal cliente, ma necessari per l'utilizzo specificato o atteso, quando conosciuto, nel nostro caso questi elementi saranno oggetto di analisi di impatto del IA;

c) i requisiti specificati dall'organizzazione, nel nostro caso vale quanto specificato al punto a);

d) i requisiti cogenti applicabili ai prodotti e ai servizi, nel nostro caso AI Act, GDPR, Statuto ei Lavoratori....

e) i requisiti del contratto o dell'ordine che differiscono da quelli espressi in precedenza, nel nostro caso ogni differenza sarà gestita per mezzo di modifiche (definite nel requisito successivo)

L'organizzazione deve assicurare che siano risolte le differenze fra i requisiti del contratto o dell'ordine e quelli espressi in precedenza, nel nostro caso eventuali differenze saranno trattate come modifiche ((definite nel requisito successivo).

Qualora il cliente non fornisca una dichiarazione documentata dei propri requisiti, i requisiti del cliente devono essere confermati dall'organizzazione prima di essere accettati, nel nostro caso il cliente/utente ha preconcordato i requisiti.

L'organizzazione deve conservare informazioni documentate, per quanto applicabile:

- a) dei risultati del riesame, nel nostro caso ogni riesame è dimostrato da uno specifico documento;
- b) di ogni nuovo requisito per i prodotti e servizi, nel nostro caso qualsiasi nuovo requisito espresso dal cliente sarà trattato come una modifica (definite nel requisito successivo)

#### **8.2.4 Modifiche ai requisiti per i prodotti e servizi**

Quando i requisiti di prodotti e servizi vengono modificati, l'organizzazione deve assicurare che le pertinenti informazioni documentate siano aggiornate e che le persone pertinenti siano rese consapevoli in merito ai requisiti modificati, nel nostro caso ogni modifica implica la ripetizione dell'intero ciclo offerta/contratto/ordine, generando un nuovo progetto avente la somma dei requisiti e chiudendo come superato il progetto basato su requisiti pregressi.

#### **ISO 22301**

Questa norma assicura l'erogazione dei servizi anche a fronte di eventi che possano avere impatti significativi sull'organizzazione.

Nel nostro caso considereremo l'erogazione dei servizi legati agli interventi sulla IA "Cerca e seleziona candidati" per allucinazioni, bias, situazioni anomale, incidenti legati alla cybersecurity e/o alla privacy ecc.

La Business Impact Analysis permetterà, sulla base della valutazione degli impatti della IA, di capire quali possano essere i Single Point of Failure delle attività critiche. Una successiva analisi dei rischi permetterà di individuare i rischi maggiori e di identificare le strategie/procedura opportune di risposta ai vari rischi. In fine si produrrà il Business Continuity Plan relativo e saranno definiti test/esercitazioni per assicurare che l'IA "Cerca e seleziona candidati" possa operare anche a fronte di scenari di impatto.

## ISO/IEC 20000-1

Questa norma garantisce l'erogazione dei servizi IT (interventi sulla IA "Cerca e seleziona candidati") secondo SLA (dal lunedì al venerdì, dalle ore 8:00 alle ore 20:00) concordati con il cliente, garantendo anche i processi sottesi al funzionamento di tali servizi.

Nel nostro caso almeno i seguenti requisiti della norma dovranno essere implementati, per garantire quanto specificato a livello contrattuale e di SLA con il cliente:

Verso il cliente/utente

### **8.3.2 Business relationship management**

### **8.3.3 Service level management**

Verso il fornitore di IA

### **8.3.4.1 Management of external suppliers**

Lato interno a supporto del servizio

### **8.4.1 Budgeting and accounting for services**

### **8.4.2 Demand management**

### **8.4.3 Capacity management**

Lato interno a supporto della progettazione ed erogazione

### **8.2.5 Asset management**

### **8.2.6 Configuration management**

### **8.5.1 Change management**

### **8.5.2 Service design and transition**

Lato interno per le attività di intervento

**8.6.1 Incident management**

**8.6.2 Service request management**

Lato interno a supporto delle attività di intervento

**8.6.3 Problem management**

Lato interno a supporto delle caratteristiche del servizio

**8.7.1 Service availability management**

**8.7.2 Service continuity management**

Trattandosi di elementi complessi ma comunque esplicativi per chi opera nel campo dei servizi ICT, evitiamo in questa sede approfondimenti specifici che impegnerebbero svariate pagine.

ISO/IEC 27001

Questa norma garantisce la protezione delle informazioni in termini di riservatezza, integrità e disponibilità.

Nel nostro caso l'applicazione della information security sarebbe applicabile all'ambiente infrastrutturale del produttore.

ISO/IEC 27701

Questa norma costituisce una specifica applicazione della ISO/IEC 27001 per la protezione dei dati personali (utilizzati per le fasi di addestramento e test dell'IA).

ISO/IEC 27017

Questa norma estende la ISO/IEC 27001 ai servizi erogati in cloud (ambiente di sviluppo, test dell'IA e successive analisi in caso di interventi richiesti da cliente a fronte di situazioni anomale)

ISO/IEC 27018

Questa norma estende la ISO/IEC 27001 e la ISO/IEC 27017 ai cloud pubblici con dati personali dove il produttore è responsabile del trattamento dei dati (dati dei CV utilizzati per addestramento e test dell'IA).

## Conseguenze in termini AI Act

Essendo la IA sviluppata nel 2020, prima dell'uscita dell'AI Act occorre rivolgersi al momento storico attuale, non potendosi parlare più di progettazione ma soffermandosi esclusivamente sul ciclo di vita. Pertanto, l'IA seppure sviluppata nel 2020 deve essere sottoposta a un processo di valutazione del rischio al fine di valutare se si tratti o meno di IA ad alto rischio e devono essere identificati eventuali gap di compliance e conseguenti azioni correttive, che nel caso di sistema ad alto rischio comporteranno d'adozione di tutti gli obblighi previsti dall'AI Act nella sezione II e nell'Allegato III. In ogni caso, l'AI Act prevede per i sistemi ad alto rischio l'obbligo del monitoraggio costante post immissione sul mercato (art 72).

L'AI Act è tassativo, sia nell'art. 6 che nel rimando ai sistemi "automaticamente" ad alto rischio (Annex III), occorre prevedere, già in questo momento:

- *Framework* di gestione dei rischi per tutto il ciclo di vita del sistema di IA;
- Effettuare valutazioni di *data governance*, su tutto il ciclo dei dati (addestramento, validazione e test del dataset);
- Mantenere, aggiornare e revisionare la documentazione tecnica del sistema di IA;
- Implementare, testare e mantenere *logs* del sistema di IA per tutto il suo ciclo di vita;
- Creare e mantenere informative per i *deployer* in modo da rendere tali soggetti responsabili;
- Ideare i sistemi di IA improntando questi su quattro direttive principali: supervisione umana, precisione, robustezza e cybersecurity;
- Implementare un sistema di controllo qualità (non nel senso di cui alla ISO 9001) perché sia mantenuta e consolidata la compliance al Regolamento.

Sul punto, per motivi di adeguatezza del mercato, le aziende avranno fino al 2 agosto 2027 per rendersi "conformi" (leggasi *compliant*) col Regolamento, per quanto riguarda i sistemi di IA di cui al comma 1 dell'articolo 6. Per tutto il resto dell'articolo, l'obbligo scatta al 2 agosto 2026. La precisazione, nonché la differenza, è importante per quanto riguarda i sistemi di cui all'Annex III e la clausola di deroga. Entro il 2 febbraio 2026 la Commissione europea fornirà orientamenti che specificano l'attuazione pratica delle regole di classificazione dei sistemi di IA, fornendo un elenco esaustivo di esempi pratici di casi d'uso di sistemi di IA ad alto rischio e non ad alto rischio. Inoltre, la Commissione europea potrà modificare le condizioni che

legittimano l'esclusione dai sistemi ad alto rischio qualora vi siano prove concrete e affidabili dell'esistenza di sistemi di IA utilizzati in determinati settori che non presentano un rischio significativo di danno.

Per concludere, si tratta di uno scenario ancora molto "fluido" in cui non è possibile dare risposte definitive, ma spesso sarà necessario procedere con un'analisi caso per caso.

## Conclusioni

Si è arrivati alla conclusione di questo contributo, piuttosto denso, sui rapporti tra ISO/IEC 42001, norme armonizzate, AI Act e l. 132/2025 (ex DDL 1146), quali conclusioni possiamo trarre da tutto ciò? A nostro avviso possiamo fissare alcuni punti fondamentali:

1. Nonostante la differenza ontologica, tra ISO e Regolamento europeo, esistono certamente dei punti di contatto che possono portare ad una certa integrazione tra i due ecosistemi. Questi ecosistemi devono per forza di cosa comunicare tra loro, anche per il tramite delle norme armonizzate;
2. Come anticipato nei paragrafi precedenti, la ISO/IEC 42001 non certifica il prodotto ma il sistema; ed esisteranno tanti sistemi quante sono le IA all'interno dell'organizzazione (tenuto conto di settore di applicazione e uso dell'IA nonché dei ruoli rispetto al singolo sistema);
3. Da un punto di vista di legislazione interna, sicuramente un ruolo di primo piano spetterà ad ACN e ad AgID (senza dimenticare del Garante per la protezione dei dati personali) per il corretto sviluppo dei sistemi di IA nell'ambito delle Pubbliche Amministrazioni e dei servizi destinati ai cittadini.

Chiaramente non si tratta di un punto di arrivo, ma di un *checkpoint* di medio periodo sullo stato dell'arte attuale concernente il panorama relativo all'intelligenza artificiale e le norme (cogenti/volontarie/armonizzate) applicabili. Sarebbe errato sottacere come l'estrema velocità di cambiamento dell'intelligenza artificiale non finisca per inficiare anche l'efficacia di questo tipo di contributi, ma se non altro può contribuire all'inserimento e consolidamento di tutta una serie di determinati paletti operativi.

## **Bibliografia**

### **Fonti normative**

1. Regolamento (UE) 2024/1689 del Parlamento Europeo e del Consiglio (Ai Act);
2. Legge 132 del 2025 (Disposizioni e deleghe al Governo in materia di intelligenza artificiale);
3. Regolamento (CE) 765/2008 del Parlamento Europeo e del Consiglio;
4. Consiglio d'Europa (CM(2024)52) - Convenzione quadro del Consiglio d'Europa sull'intelligenza artificiale.

### **Standard e documentazione tecnica**

1. ISO/IEC 42001:2023
2. UNI CEI ISO/IEC 42001:2024
3. ISO/IEC 42006:2025
4. ISO/IEC 42005:2025
5. ISO/IEC 22989:2022
6. ISO/IEC 27001:2022
7. ISO 22301:2019
8. ISO/IEC 20000-1:2018
9. ISO/IEC 27017:2015
10. ISO/IEC 27018:2025
11. ISO 9001:2015
12. ISO/IEC 17065:2012
13. ISO/IEC 17021-1:2015
14. ISO 19600:2014
15. ISO 37301:2021
16. ISO/IEC 25012:2012
17. ISO/IEC 25024:2015
18. ISO/IEC 5259-3:2024
19. ISO/IEC 5259-2:2024
20. ISO/IEC TR 24027:2021
21. ISO/IEC 23053:2022
22. ISO/IEC 5338:2023
23. ISO/IEC 23894:2023
24. UNI CEI CEN/CLC/TR 18115

### Citazioni ulteriori e link

1. Veale Michael, Borgesius Zuiderveen J. Frederik, *“Demystifying the Draft EU Artificial Intelligence Act - Analysing the good, the bad, and the unclear elements of the proposed approach”*, in *Computer Law Review International*, pp. 97-112, 2021;
2. Oever ten Niels, Milan Stefania, *“The Making of International Communication Standards: Towards a Theory of Power in Standardization, in Journal of Standardisation*, pp. 1-27, 2022;
3. Corte di Giustizia dell'Unione europea (CGUE C-171/11, Fra.bo);
4. <https://www.uninfo.it/>;
5. <https://www.uni.com/sistemi-di-gestione-efficaci-e-integrati-una-guida-alla-harmonized-structure/>;
6. <https://msblogs.thesourcemediaassets.com/sites/5/2022/06/Microsoft-RAI-Impact-Assessment-Template.pdf>;
7. <https://artificialintelligenceact.eu/standard-setting-overview/>;
8. [https://ec.europa.eu/transparency/documents-register/detail?ref=C\(2023\)3215&lang=en](https://ec.europa.eu/transparency/documents-register/detail?ref=C(2023)3215&lang=en);
9. [https://ec.europa.eu/info/law/better-regulation/have-your-say/initiatives/13446-European-standardisation-evaluation\\_en](https://ec.europa.eu/info/law/better-regulation/have-your-say/initiatives/13446-European-standardisation-evaluation_en);
10. <https://aichampions.eu/>
11. <https://www.iafcertsearch.org/services/iso-survey>;
12. <https://www.cencenelec.eu/news-events/news/2025/brief-news/2025-10-23-ai-standardization/>.