UNIVERSITA' POLITECNICA DELLE MARCHE

FACOLTA' DI INGEGNERIA

Corso di Laurea magistrale in Ingegneria Elettronica

Sviluppo di interfaccia utente e architettura di comunicazione per il controllo remoto dei prodotti Elica

Development of user interface and communication architecture for remote control of Elica products

Relatore:

Prof. Ennio Gambi

Tesi di Laurea di:

Daniele Alidori

Correlatore:

Ing. Luca Meniconi

A.A. **2021** / **2022**

Sommario

Introduzione

Il presente lavoro di tesi nasce dopo aver affrontato un percorso lavorativo durato circa tre mesi presso Elica S.p.a., azienda leader mondiale nella produzione di cappe ad uso domestico e che ora si sta allargando anche al mercato dei piani ad induzione e forni.

I prodotti Elica hanno da sempre avuto un occhio di riguardo per il valore assegnato alla "user experience": la capacità che un'interfaccia ha di rendere piacevole l'utilizzo dell'elettrodomestico è il valore aggiunto da perseguire. Il "piacere d'uso" di un prodotto non risiede solo nella sua funzionalità ma anche nel modo e nello stile con cui questo assolve al suo compito. Da qui la volontà di sviluppare una nuova architettura in grado di permettere agli elettrodomestici Elica, nel caso particolare la cappa, una integrazione che risulti essere il più semplice possibile all'interno di una Smart Home, garantendo comunque una ottimizzazione di tutta una serie di aspetti legati alla produzione e progettazione, con il fine di abbattere i costi di realizzazione. Tutto il processo di on-boarding della cappa è stato rivisto con il fine di risultare intuitivo e naturale. L'intento è quello di creare una architettura che risulti anche essere il più generale possibile, così da poter essere implementata su una serie di prodotti anche tra loro differenti.

La soluzione proposta è il risultato di un lavoro durato tre mesi svolto all'interno dell'area R&D dell'azienda, collaborando con i dipendenti ed ingegneri del reparto per la definizione delle specifiche e tecnologie, ma anche con il personale e direttori di altri uffici con il fine di avere una visione il più possibile trasversale del progetto. Per raggiungere il risultato è stata necessaria una prima fase di allineamento, di valutazione e studio dello stato dell'arte: questo punto è stato raggiunto studiando la documentazione interna dell'azienda ma anche testando con mano i prodotti e servizi che essa mette a disposizione sul mercato. Successivamente è seguita una seconda fase di engineering, ovvero di definizione delle specifiche hardware della nuova user interface: componenti, dimensioni, posizionamento dei moduli. Questa fase è stata accompagnata da una serie di riunioni con possibili fornitori e dirigenti dell'area marketing, analizzando la situazione sia dal punto di vista ingegneristico ma anche logistico e soprattutto economico. L'ultima parte del progetto si è concentrata invece sulla definizione della nuova architettura di comunicazione tra lo smartphone e la cappa, con il fine di identificare un protocollo alternativo a quello attualmente in uso per semplificare il processo di registrazione della cappa sull'App Elica Connect: è stato effettuato uno studio volto ad indentificare e confrontare le possibili soluzioni applicabili con il fine di identificare la tecnologia che più si adattasse all'obiettivo prefissato. Identificato lo standard da applicare sono seguiti: lo studio della tecnologia stessa, la definizione della modalità di implementazione e lo sviluppo del software necessario alla realizzazione di simulazioni del prodotto finito, così da poter commentare e giudicare il lavoro svolto. L'ultima parte del tirocinio si è concentrata sullo studio ed analisi del processo di certificazione di un prodotto finito; quindi, comprendere come si legge una norma e come si definiscono i test e prove da eseguire.

Nella stesura della tesi si è costantemente inseguito l'obiettivo di dare ad essa uniformità e linearità, cercando di seguire il percorso svolto all'interno dell'azienda così da favorire una lettura logica ed una migliore comprensione. L'elaborato si articolerà seguendo una prima fase descrittiva dell'azienda e del suo laboratorio, cuore di supporto alla ricerca, innovazione e capace di garantire l'accesso al mercato globale. Segue una fase di descrizione del prodotto, dell'architettura attualmente implementata nei dispositivi connessi Elica, una analisi e mappatura delle tecnologie disponibili e consolidate in ambito connectivity ed IoT per poi descrivere lo sviluppo della nuova user interface e della nuova architettura implementata, tenendo conto di eventuali vincoli realizzativi e di costo. Il capitolo descrive poi il processo di certificazione, descrivendo tutti i test propedeutici alla messa in vendita sul mercato del prodotto. Per concludere verrà presentata una panoramica sulla cybersecurity, sulle minacce più comuni che interessano i dispositivi IoT e quelle che sono le soluzioni per la sicurezza applicate da Elica.

1. Storia dell'Azienda

In questo capitolo è contenuta una rapida descrizione della realtà aziendale che ha fatto da sfondo alla stesura di questa tesi. Sarà presentato il gruppo industriale con alcuni numeri di mercato, saranno introdotti gli elettrodomestici prodotti e per finire verrà riportata una panoramica sull'EPL (Elica Propulsion Laboratory) certificato a livello europeo, riportando le prove eseguibili al suo interno e descrivendo il processo che porta alla definizione delle prove da svolgere per certificare un prodotto connesso.

1.1. Elica S.p.a.

Elica (Figura 1), fondata nel 1970 da Ermanno Casoli, è la capofila di un Gruppo attivo nel mercato delle cappe da cucina, piani aspiranti, piani ad induzione e forni ad uso domestico che rappresenta oggi il primo produttore mondiale di cappe aspiranti e leader del mercato europeo in termini di unità vendute. Vanta inoltre una posizione di leadership a livello europeo nella progettazione, produzione e commercializzazione di motori elettrici per elettrodomestici e caldaie da riscaldamento.

Il connubio tra tradizione, qualità, design, innovazione e tecnologia caratterizza da sempre questa azienda che, nel 1972 riuscì ad anticipare le tendenze del mercato, presentando alla Philips di Parigi il primo aspiratore d'aria ad incasso. Da questo momento inizia un processo di evoluzione societaria, organizzativa ed industriale che ha portato Elica a seguire una strategia di crescita per linee esterne con l'obiettivo di estendere la propria attività anche in settori complementari.

Figura 1 - Logo Elica

Elica S.p.a. è oggi un Gruppo quotato (dal 10 Novembre 2006), presieduto da Francesco Casoli e guidato da Andrea Cocci, amministratore delegato, che ha chiuso il 2021 con un Fatturato pari a 541,3 milioni di euro, un EBITDA (in italiano Margine Operativo Lordo, MOL) pari a 38,5 milioni di euro. Le principali Business Unit di Elica Corporation sono:

- Cooking BU: progetta, produce e commercializza cappe da cucina a uso domestico, sia a marchio proprio sia attraverso i brand dei principali produttori internazionali di elettrodomestici e cucine (Whirlpool, Electrolux, Ikea, Bosch-Siemens, Haier, ecc.), piani cottura e, per il mercato asiatico, forni e sterilizzatori;
- Motors BU: progetta, produce e commercializza motori elettrici per il mercato del riscaldamento, della ventilazione e degli elettrodomestici attraverso la società controllata EMC FIME, nata nel 2022.

Con circa 3.200 dipendenti il Gruppo Elica ha una piattaforma produttiva articolata su 7 siti produttivi tra Italia, Polonia, Messico e Cina (Figura 2). [1]

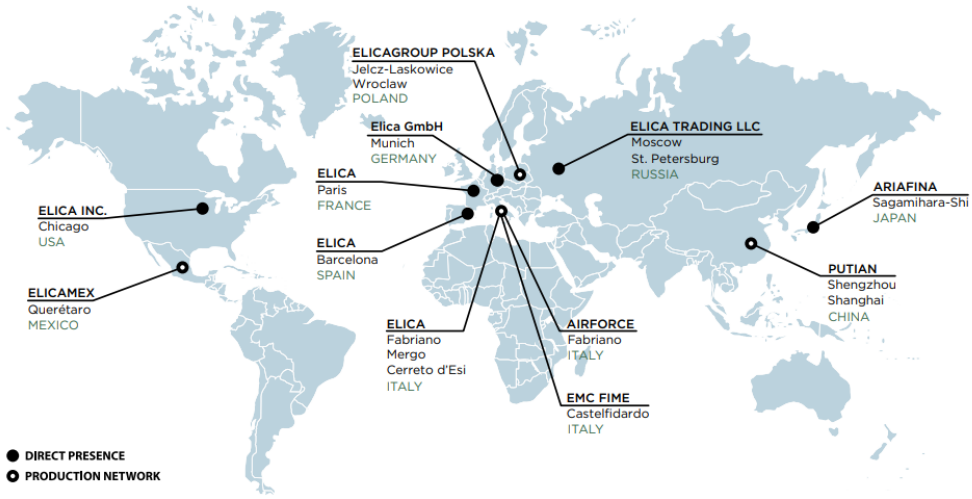


Figura 2 - Posizione siti produttivi

In Europa la Società è presente in Italia, nella Regione Marche, dove hanno sede l'Headquarter (a Fabriano, in provincia di Ancona, dove ha inizio la storia di Elica), gli stabilimenti produttivi e la sede centrale del laboratorio di ricerca e sviluppo. È presente poi in Polonia, con Elica Group Polska, a Jelcz Laskowice, nel polo industriale di Wroclaw, uno dei più importanti dell'Est Europa; in Germania serve direttamente il mercato con Elica GmbH; in Spagna, con un'organizzazione dedicata che consente un efficace presidio del mercato e in Francia grazie alla recente apertura di Elica France nel centro di Parigi.

Elica Corporation è presente in Messico, a Querétaro, con Elicamex, sede produttiva e commerciale per l'America Latina e per il Nord America. La presenza in questo Paese si inserisce nel progetto strategico, portato avanti da Elica Corporation nel corso degli anni, di essere sempre più vicini ai clienti del mercato di riferimento per coglierne le nuove e importanti opportunità di crescita, sia nel business OEM (Original Equipment Manufacturer) che attraverso il lancio e lo sviluppo dei propri marchi.

In Asia Elica Corporation è presente dal 2002, anno della joint venture con Fuji Industrial, prima azienda produttrice di cappe aspiranti in Giappone, del quale dal 2006 Elica detiene il controllo. Dalla JV è nato Ariafina, brand di riferimento per il mercato giapponese delle cappe di alta gamma. Nel 2005 Elica ha aperto uno show room nella principale via della moda di Osaka. Nel 2010 Elica è entrata nel mercato cinese, primo maggior mercato mondiale delle cappe, acquisendo la quota di maggioranza della società cinese Zhejiang Putian Electric Co. Ltd, proprietaria del marchio Puti, con il quale produce e commercializza cappe, piani a gas e sterilizzatori per stoviglie per il mercato locale. Elica Corporation è presente nel più grande mercato mondiale del settore cappe con PUTI, un noto marchio cinese e con il brand Elica, inoltre dispone di una struttura produttiva di qualità e con ampie potenzialità di sviluppo. Lo stabilimento produttivo è situato a Shengzhou, uno dei più affermati distretti industriali cinesi degli elettrodomestici. Nel 2012 la Società ha rafforzato la sua presenza diretta in questo mercato, in cui è attiva attraverso i suoi marchi già dal 1995, acquisendo il 100% della società controllata Elica Trading LLC, che commercializza prodotti con marchi propri, quali Elica, Jet Air e Turboair. Elica Trading LLC, costituita nel 2011 e con sedi a San Pietroburgo e a Mosca, grazie ai suoi magazzini di stoccaggio serve direttamente una fitta rete di distribuzione nel territorio locale. Elica Corporation è in grado oggi di assicurare in questo mercato maggiore efficienza e qualità, oltre che del prodotto anche del servizio offerto ai clienti e ai consumatori, grazie alla gestione diretta di una rete di assistenza tecnica (Figura 3). [1]

Figura 3 - Marchi Elica

Nel 2009 Elica ha aderito all'Associazione World Class Manufacturing (WCM), organizzazione internazionale no-profit che riunisce aziende di diversi settori coinvolte nell'introduzione e sviluppo di un medesimo processo di cambiamento unificato.
Il WCM è un sistema di produzione strutturato e integrato che riguarda l'organizzazione della fabbrica nel suo complesso e ne promuove il miglioramento sistematico e duraturo attraverso la valutazione e la riduzione di ogni tipo di spreco o perdita, applicando metodi rigorosi e standard condivisi e coinvolgendo l'intera organizzazione in una logica di lavoro di team. Elica vuole applicare la logica WCM a tutta la catena del valore aziendale, intraprendendo un percorso di cambiamento che renda il processo logistico–produttivo più snello e veloce, senza sprechi e che tenga sotto stretto controllo la sicurezza dei lavoratori e del prodotto finito.
Per garantire il rispetto dei principi di salvaguardia dell'ambiente e della sicurezza nel luogo di lavoro da parte di ogni dipendente opera una specifica funzione organizzativa, l'Environment Health Safety. L'attenzione alle persone si traduce anche nell'attenzione alla sicurezza e alla salute. L'obiettivo è "la sicurezza prima di tutto".
La vision ambientale della Società è assicurare processi e prodotti rispettosi dell'ambiente nel corso di tutto il ciclo di vita, adoperandosi per ridurre il consumo di fonti di energia non rinnovabili e la produzione di rifiuti.
La Società rispetta tutte le normative vigenti in materia ambientale e risponde alle normative internazionali a carattere volontario. Elica è certificata UNI EN ISO 14001 per il SGA - Sistema di Gestione Ambientale e si è dotata di specifiche linee guida e procedure per la gestione di sostanze chimiche, prevedendo misure preventive e informative per la sicurezza degli operatori e dell'ambiente.
Nel 2011 Elica ha inaugurato il primo impianto fotovoltaico del Gruppo, presso lo stabilimento di Castelfidardo (AN). L'impianto è in grado di soddisfare il 35% del fabbisogno di energia elettrica dello stabilimento, consentendo una produzione annua di energia pari a 1.240.000 KWh e evitando l'emissione annua di 765 tons di CO_2, pari a 76.500 alberi, a 6,6 mln di km percorsi mediamente da un'auto in un anno o al consumo energetico annuale di 128 appartamenti di 100 mq. Presso l'Headquarter di Fabriano il Leaf Meter, misuratore della sostenibilità, permette di misurare in diretta il trend di produzione energetica e di mappare la tendenza dei consumi energetici dello stabilimento. [1]

1.2. Fondazione Ermanno Casoli

Lo sviluppo tecnologico ed i risultati ottenuti nei cinquanta anni di attività dell'azienda sono il frutto di un ambiente di lavoro in cui le persone si sentono libere di esprimersi, di dialogare, di collaborare e di conseguenza innovare. Un esempio dell'attenzione dell'azienda nei confronti dei lavoratori è rappresentato dalla Fondazione Ermanno Casoli (FEC).

La Fondazione Ermanno Casoli, nata nel 2007 in memoria di Ermanno Casoli, promuove iniziative in cui l'arte contemporanea diventa uno strumento didattico e metodologico capace di migliorare gli ambienti di lavoro e di innescare processi innovativi, ponendosi come obiettivo quello di favorire il rapporto tra il mondo dell'arte e quello delle aziende. Pioniera nell'indagare le potenzialità del dialogo fra arte e industria, la FEC si è affermata in Italia come modello di riferimento all'avanguardia nel campo della formazione aziendale attraverso l'arte contemporanea, proponendo attività sempre più strutturate e specializzate, in grado di far interagire questi due mondi nel rispetto dei reciproci obiettivi.

Alla base delle attività della FEC c'è la convinzione che l'arte contemporanea, in quanto attivatrice di pensiero, contribuisca a rompere i paradigmi tradizionali del sapere comune, permettendo alle persone che si avvicinano ad essa di prendere confidenza con uno stato mentale ed emotivo che porta al manifestarsi di una possibilità inattesa. Questo rende l'arte contemporanea uno strumento particolarmente adatto a creare contesti esperienziali aperti e innovativi. La FEC promuove progetti che fanno dialogare arte e organizzazioni aziendali affinché si possano innescare originali processi di innovazione che stimolano la creatività e rafforzano il lavoro di squadra.

Le opere d'arte che compongono la Elica Corporate Collection sono il frutto dell'interazione tra dipendenti ed artisti di fama internazionale. Questa particolare quanto specifica raccolta di opere è stata inserita nel volume Global Corporate Collection *(2015)*, dedicato alle 100 più belle collezioni d'arte aziendale nel mondo. Tutte le attività promosse dalla FEC trovano in Elica l'incubatore ideale in cui sperimentarne processi e risultati, affinché possano essere successivamente applicati in altri contesti. [2]

Un'originale modalità di interazione tra arte e impresa che porta l'arte contemporanea nel vivo dei sistemi produttivi è la *FEC for Factories*. Gli artisti vengono invitati a confrontarsi con le fasi che precedono la realizzazione di un prodotto industriale, condividendo il percorso progettuale con designer, ingegneri, specialisti del marketing, prototipisti e operai specializzati. In questo modo si incentiva la creatività e la possibilità di inventare nuovi linguaggi, processi produttivi e sistemi di comunicazione.

Particolare attenzione va anche rivolta al progetto E-STRAORDINARIO, il progetto che dal 2008 porta l'arte contemporanea nel mondo dell'impresa quale strumento didattico e metodologico rivolto alla formazione aziendale. Attraverso un ciclo di workshop artisti di fama internazionale lavorano alla realizzazione di un'opera d'arte con i dipendenti di un'azienda, coadiuvati da un formatore manageriale e da un curatore d'arte contemporanea. Le opere prodotte nel corso di queste attività di formazione vanno a costituire un "museo diffuso" che coinvolge tutte le imprese che negli anni hanno collaborato con la FEC. E-STRAORDINARIO ha ottenuto il patrocinio del Ministero per i Beni e le Attività Culturali e il Premio Cultura + Impresa 2014.

Il progetto trova poi numerose varianti ed applicazioni, tra cui E-STRAORDINARIO FOR KIDS, dedicato ai ragazzi e alle loro famiglie, nato per i figli dei dipendenti di Elica, poi sperimentato anche in altri contesti. Come per E-STRAORDINARIO, si tratta di una serie di workshop che fanno entrare attivamente i partecipanti nel processo creativo dell'artista, nella convinzione che l'arte contemporanea possa svolgere un ruolo importante nella formazione delle giovani generazioni.

1.3. I prodotti Elica

Esperienza di oltre cinquant'anni nel settore, grande attenzione al design, ricercatezza dei migliori materiali e tecnologie avanzate sono gli elementi che contraddistinguono Elica sul mercato e che hanno consentito al Gruppo di rivoluzionare l'immagine tradizionale delle cappe aspiranti da cucina: non più semplici accessori ma elementi d'arredo e oggetti sofisticati dal design unico e ricercato.

"Quando il mondo dell'aria incontra il design, l'innovazione e la tecnologia, nasce Elica"

Figura 4 - Cappa Nuage

Tecnologia e design sono i punti cardine di Elica che ha fatto dell'innovazione l'elemento principe del proprio posizionamento con l'obiettivo di offrire ai propri clienti prodotti in grado di rispondere a qualsiasi necessità. Il design è internazionale e nasce dalla mente del designer Fabrizio Crisà, capace di creare vere e proprie opere d'arte dal design unico; negli anni ha saputo interpretare i valori del gruppo sviluppando soluzioni all'avanguardia e nuove forme. Ne è un esempio la cappa Nuage: il suo stile e la sua forma la rendono un tutt'uno con la parete, dal quale sembra fuoriuscire (Figura 4). Elica è presente sul mercato con diverse tipologie di prodotti in grado di soddisfare le esigenze di svariati tipi di clientela a cui si rivolgono. Al momento è possibile scegliere tra oltre cento modelli di cappe, distinte in: cappe da parete, incasso, isola, angolo, soffitto e le più particolari chiamate "a scomparsa", ovvero l'elettrodomestico è integrato all'interno del bancone e nel momento in cui è richiesto il suo utilizzo con un movimento fluido e silenzioso la cappa emerge, per poi rientrare subito dopo l'uso facendo riacquisire spazio utile (Figura 5).

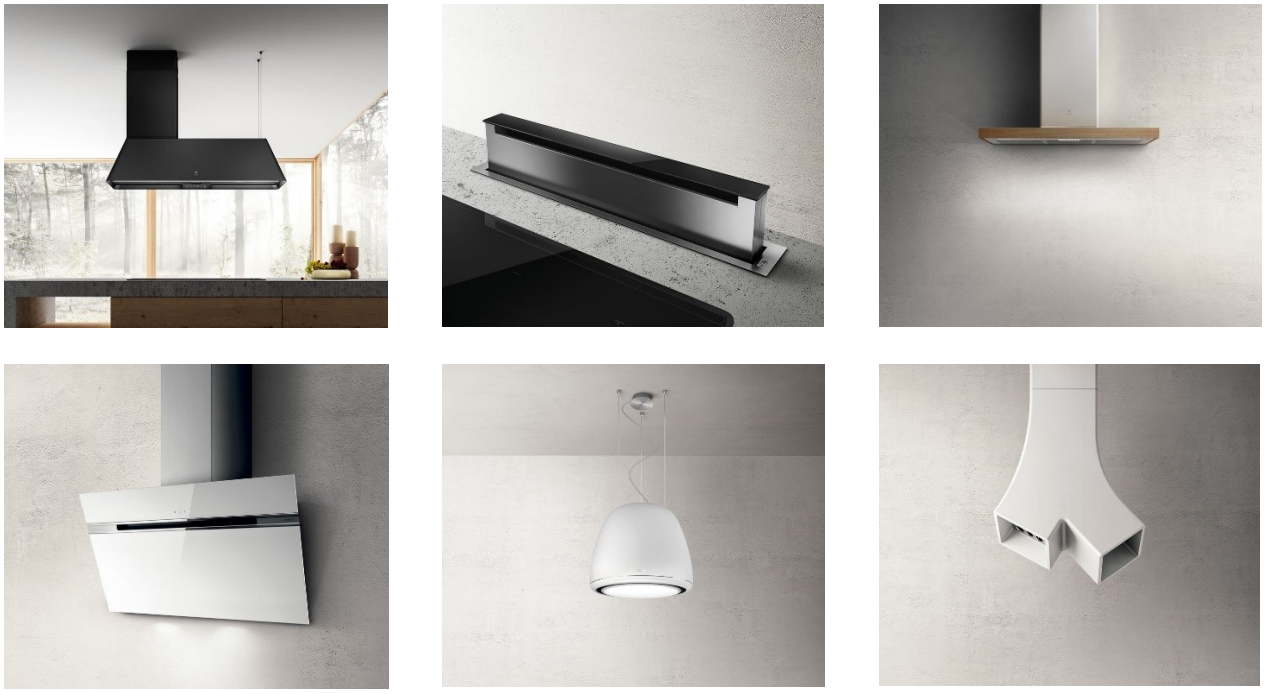


Figura 5 - Esempi di cappe Elica

Il design innovativo dei prodotti è stato riconosciuto anche dal mercato, vincendo in più occasioni numerosi premi, oltre 180, tra cui il Design Awards, Reddot Awards, Iconic Awards e Compasso D'oro ADI.

Oltre all'alta gamma, è importante evidenziare come Elica produca cappe sia con il proprio marchio che per azienda esterne destinate a tutti i settori ed a tutte le fasce di mercato. Alla base di ogni prodotto sono sempre tenuti considerazione altri aspetti fondamentali: efficienza, innovazione e tecnologia.

- Efficienza. Tutte le cappe Elica sono progettate e realizzate tenendo sempre in considerazione due fondamentali concetti: efficienza e silenziosità. La continua ricerca Elica in questi ambiti ha portato all'introduzione di un nuovo sistema di aspirazione, denominato *Optimized Aspiration System*, che permette di avere ottime prestazioni in termini di aspirazione dei fumi e dei vapori, con una ridotta emissione di rumore;

- Tecnologia. La ricerca negli ultimi anni ha condotto ad un notevole sviluppo tecnologico del prodotto che sempre più diventa strumento multifunzionale al servizio dell'utente. Tecnologie che permettono alla cappa di accendersi, spegnersi e regolarsi automaticamente, di fornirci informazioni sulla temperatura interna ed esterna, accendere e regolare le luci in maniera automatica o in grado di garantire tutti i comandi da remoto utilizzando l'applicazione Elica Connect o il telecomando fornito in dotazione;

- Innovazione. L'obiettivo che l'azienda si pone è quello di rendere semplice ed efficiente l'impiego della più avanzata tecnologia. Secondo questa filosofia sono state sviluppate le interfacce utente quali: slider, pulsantiera meccanica, pulsantiera soft ligth e touch control. Elica ha brevettato sistemi di aspirazione che riducono notevolmente il rumore senza penalizzare l'efficienza di aspirazione, ideato e realizzato oggetti che si inseriscono armoniosamente in qualsiasi cucina, incrementato la resistenza dei suoi prodotti grazie a tecnologie e materiali innovativi.

Con il fine di mantenere una continua innovazione, negli ultimi anni Elica ha deciso di andare ad unire due elettrodomestici che sono normalmente separati in cucina: il piano cottura e la cappa, ridefinendo così i semplici gesti quotidiani, in un perfetto connubio tra tecnologia, funzionalità ed estetica. Quello che hanno creato con il piano aspirante Nikola Tesla (e versioni successive) è qualcosa di unico e straordinario, dal design elegante a cura di Fabrizio Crisà (Figura 6). Il piano esiste sia nella versione a gas o induzione, ed oltre a quattro zone cottura presenta il sistema aspirante al centro del piano in grado di garantire un'elevata captazione dei fumi, nettamente superiore alla loro velocità di salita. Le varie versioni si differenziano principalmente dal punto di vista estetico: dimensioni, User Interface (touch, manopole) e design del sistema aspirante.

Figura 6 - Piano aspirante Nikola Tesla

Novità del Salone Internazionale del Mobile Eurocucina 2022 è il “LHOV” (Figura 7). Il prodotto rappresenta una rivoluzione perché integra piano cottura, cappa e forno, riaffermando la leadership di Elica nel segmento Cooking a 360 gradi. Una categoria di prodotto del tutto inedita, compatto, potente, automatizzato, che esprime a pieno la spinta all’innovazione anche verso la sostenibilità. La linea "LHOV" permette una gestione ottimale dello spazio domestico e dà nuova forma all’esperienza di cottura.

Figura 7 - LHOV

1.4. Il reparto R&D

Il reparto di ricerca e sviluppo, anche noto come R&D (dall’inglese Research and Development) si occupa di tramutare le specifiche e le esigenze che arrivano dal mercato, in prodotti finiti, rispettando i criteri di costo, qualità, prestazioni ed affidabilità richiesti dalla direzione aziendale ed in linea con il marchio Elica.

L’area R&D della Business Unit Cooking è strutturata come riportato nel grafico (Figura 8).

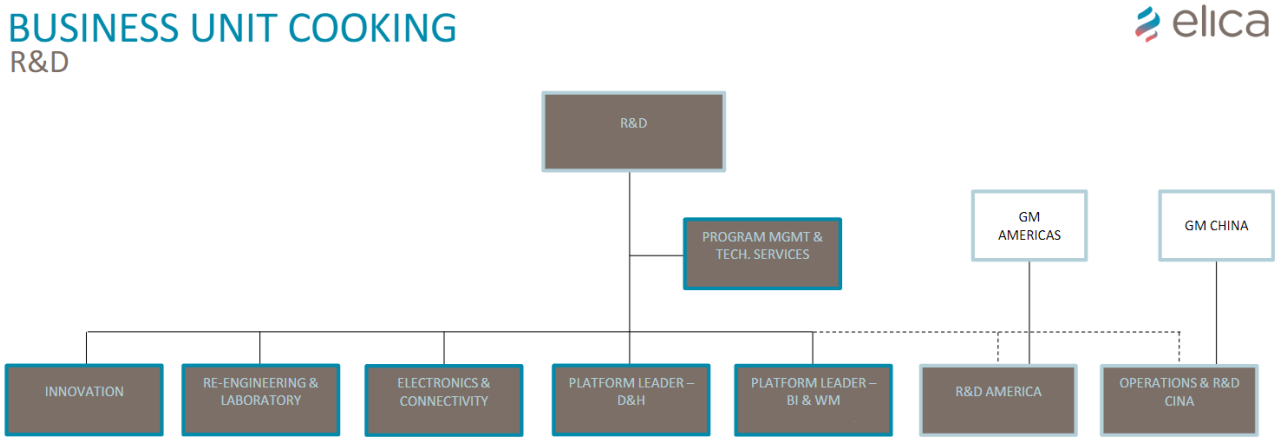


Figura 8 - Organigramma R&D

Nella figura si riporta uno schema di principio di come è organizzato il reparto R&D, senza scendere nei dettagli in quanto soggetto a segreto aziendale. Come è possibile vedere dal grafico, al di sotto della direzione ricerca e sviluppo sono indicati i seguenti reparti:

- Innovation: sviluppo e test di nuove tecnologie da applicare a futuri prodotti. Viene analizzata l'effettiva praticità, fattibilità ed implementabilità della soluzione proposta;
- Re-engineering & Laboratory: reingegnerizzazione di prodotto e test di conformità a normative e capitolati di prova interni di prodotti finiti e singoli componenti (il Laboratorio è descritto nel dettaglio all'interno del paragrafo successivo);
- Electronics & Connectivity: sviluppo elettronica, parti elettriche (cablaggi, lampade, connettori, schemi elettrici, ecc.), sviluppo e definizione architettura piattaforma connessa;
- Platform Leader – Decorative&Hobs: figura di riferimento per tutte le cappe definite "decorative" e piani ad induzione. Segue tutti i relativi progetti e lavora a stretto contatto anche con il reparto marketing;
- Platform Leader – Built In I & Wall Mounted: figura di riferimento per tutte le cappe incassate (nascoste nei mobili) o montate a parete. Segue tutti i relativi progetti e lavora a stretto contatto anche con il reparto marketing;
- R&D America: Equivalente del reparto R&D Europa ma che cura tutti gli aspetti legati a richieste specifiche del mercato ME;
- Operations: figura che in azienda supervisiona e ottimizza tutti i processi aziendali (chiamati operations) necessari per realizzare e consegnare al cliente un prodotto;
- R&D Cina: Equivalente del reparto R&D Europa ma che cura tutti gli aspetti legati a richieste specifiche del mercato cinese;

Questo lavoro di tesi è stato svolto nell'area R&D sotto la supervisione dell'Electronics & Connectivity Manager Luca Meniconi.

1.5. Elica Propulsion Laboratory

La necessità di un laboratorio interno nasce con l'intento di perseguire una missione composta da tre obiettivi principali:

1. Verificare sicurezza, affidabilità, efficienza energetica, prestazioni e compatibilità elettromagnetica di prodotti finiti e materiali;
2. Garantire accesso al Mercato Globale;
3. Supportare ricerca e innovazione.

EPL alias di Elica Propulsion Laboratory è nato nel 1988 come laboratorio aziendale per il test di cappe da cucina.
Dal 2006 intraprende un percorso di crescita continua ottenendo innumerevoli accreditamenti nell'ambito della certificazione di prodotto sino a diventare nel 2012 un laboratorio ILAC MRA (International Laboratory Accreditation Cooperation Mutual Recognition Arrangement) con Accredia. ILAC MRA è un accordo firmato da Accredia stessa grazie al quale l'accreditamento rilasciato in Italia ha pieno riconoscimento all'interno di tutte le economie mondiali. [3] EPL (Figura 9) è un ente interno all'azienda in grado di certificare la conformità alle normative in termini di sicurezza, prestazioni ed EMC sia per i prodotti Elica che per quelli di eventuali clienti esterni all'azienda. Tutto ciò comporta un rigido sistema di gestione delle attività, delle tarature degli strumenti e dei test report. Questi ultimi sono a tutti gli effetti dei documenti formali, che attestano la conformità o meno di un prodotto finito a determinate prestazioni o capitolati di prova. EPL possiede nel suo staff numerosi professionisti del settore elettrodomestico, che si occupano di tutto l'iter di validazione e certificazione di un prodotto finito, in particolare si hanno competenze su: compatibilità elettromagnetica, sicurezza, fluidodinamica, efficienza energetica applicata all'elettrodomestico, affidabilità componenti e chimica dei materiali.

EPL
Elica Propulsion Laboratory

Figura 9 - Logo EPL

Il laboratorio è a tutti gli effetti un'azienda dentro l'azienda con una sua precisa struttura ed un sistema di qualità interno da rispettare. Inoltre, dato che EPL non certifica solo prodotti Elica c'è una dichiarazione formale dell'amministratore delegato che attesta la completa autonomia del laboratorio, in questo modo si vogliono evitare eventuali ingerenze e pressioni volte a condizionare l'esito dei test.

L'EPL, come anticipato, è in grado di rilasciare certificazioni sia per i suoi prodotti sia prodotti terzi valide a livello globale. Tra queste evidenziamo i principali mercati in cui Elica opera:

- Europa. Il laboratorio EPL possiede il certificato di accreditamento fornito da Accredia per il soddisfacimento dei requisiti della norma ISO/IEC 17025 (recepita in Italia come UNI CEI EN ISO/IEC 17025:2018);
- Cina (CQC, China Quality Certification). Il CQC è sotto il controllo del China Certification & Inspection Group, che è approvato dall'Amministrazione generale statale per la supervisione della qualità e l'ispezione e la quarantena e dall'Amministrazione di certificazione e accreditamento della Repubblica popolare cinese;
- Nordamerica (UL, Underwriters Laboratories). Il marchio UL, simbolo di sicurezza del prodotto in Nordamerica, indica che UL o un laboratorio accreditato ha testato dei campioni rappresentativi di un prodotto, valutandoli idonei agli standard applicabili o ad altri requisiti, in relazione ai loro potenziali rischi di incendio, shock elettrico e pericoli meccanici.

Oggi, con una nuova sede inaugurata nel 2017 e una superfice di oltre 1800mq e 23 persone, EPL è diventata una struttura unica nel suo genere in grado di coniugare la mentalità dinamica ed aperta propria di un Laboratorio Industriale e di Ricerca & Innovazione, con il rigore e l'autorevolezza di un Laboratorio di Certificazione.

Elica Propulsion Laboratory è il partner per lo sviluppo e la certificazione dei prodotti Elica e dei client terzi (Whirlpool, Samsung, Electrolux, Bosch, Ariston Thermo, UL) con più di 300 test incentrati su: sicurezza prodotti e materiali, compatibilità elettromagnetica (EMC), misurazioni ed analisi acustiche, performance, affidabilità, prove imballo ed attività di testing personalizzabili.

L'EPL è in grado di verificare la conformità con le norme di sicurezza internazionale EN-IEC-UL e rilasciare certificazioni in collaborazione con UL International ed altri enti di certificazione, in base al mercato in questione (Figura 10):

- Certificazione UL e cULs per gli USA e Canada. UL & CSA Standards (Safety), FCC Directive, Energy Star;
- CE Certification per il mercato Europeo. Low Voltage & RED Directives (Safety), EMC Directive, Energy Labeling & Ecodesign Directives
- CB Certification. Il "passaporto" for Worldwide Market ad eccezione di USA e Canada.

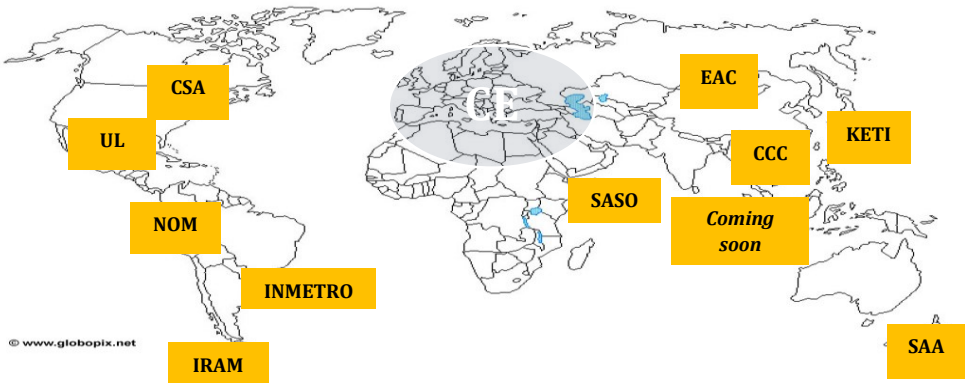


Figura 10 - Certificazioni zone del mondo

Il laboratorio è in grado di eseguire test su tutti gli elettrodomestici che Elica produce: cappe, piani ad induzione e blower&fans. [3]

La nuova struttura del laboratorio è provvista delle seguenti aree:

- Impianto di condizionamento (in grado di garantire una temperatura tra i 20°C e i 25°C);
- Impianto di ventilazione per test vista, grassi e odori;
- Tensione stabilizzata a 120 V @ 50 Hz;
- Tensione stabilizzata a 220 V @ 50 Hz;
- Tensione stabilizzata a 380 V @ 50 Hz;
- Impianto di aria compressa;
- Impianto di distribuzione gas per prove normative;
- Impianto di distribuzione acqua;
- Rete LAN;
- Impianto per la riduzione della durezza dell'acqua;
- Sistema antintrusione;
- Sistema antincendio;
- Sistema di rilevamento fughe gas metano;
- Camera climatica per prove di temperatura;
- Forno ventilato;
- Camera riverberante per prove di rumore;
- Camera climatica per prove di nebbia salina;
- Area test per EMC;
- Impianto per test imballo.

Le principali analisi e verifiche che l'EPL esegue sui prodotti sono divise in base alle aree che compongono il laboratorio stesso.

1.5.1. Compatibilità elettromagnetica

Questa area si occupa delle verifiche e delle analisi di compatibilità elettromagnetica (EMC) su elettrodomestici, componenti elettrici ed elettronici, motori elettrici e strumenti musicali in conformità alle norme EN-IEC-CISPR-FCC oltre ad eseguire verifiche ed analisi in accordo alla direttiva RED. Più in generale si occupa dell'analisi e dell'ottimizzazione degli effetti indesiderati prodotti dalla generazione, trasmissione e ricezione non intenzionali di energia elettromagnetica, con l'obiettivo di garantire il corretto funzionamento nel medesimo ambiente di diversi altri apparati che coinvolgono a loro volta fenomeni elettromagnetici durante il loro funzionamento.

Vengono eseguite principalmente due tipi di misure: misure di emissione e misure di immunità.

Misure di emissione [3]

Figura 11 - Antenna loop per la misura della potenza irradiata

- Emissione di corrente armonica in accordo alla IEC 61000-3-2 con alimentazione mono-fase fino 16 A;
- Flicker in accordo alla IEC 61000-3-3 con alimentazione mono-fase fino 16 A (emissione disturbi come fluttuazioni di corrente, frequenza ed ampiezza della tensione);
- Misura del campo Elettromagnetico emesso (EMF) in accordo alla IEC 62233;
- Emissioni Condotte banda [0,009 ÷ 30] MHz 3-fasi fino a 32 A;
- Disturbi condotti banda [30 ÷ 300] MHz;
- Misura dell'intensità del campo magnetico mediante -3D-Loop Antenna [0,009 ÷ 30] MHz (Figura 11).

Misure di immunità [3]

Figura 12 - Camera schermata

- Prove di immunità ad impulsi lenti ad alta energia in accordo a CISPR 14-2 e IEC 61000-4-5;
- Prove di immunità a transitori/treni di impulsi elettrici veloci in accordo a CISPR 14-2 e IEC 61000-4-4;
- Prove di immunità a cadute e brevi interruzioni di tensione in accordo a CISPR 14-2 e IEC 61000-4-11;
- Immunità a disturbi condotti indotti da campi radio frequenza (RF) in accordo a CISPR 14-2 e IEC 61000-4-6;
- Immunità alle scariche elettrostatiche test in accordo a CISPR 14-2 e IEC 61000-4-2;
- Immunità Ring wave test in accordo a IEC 61000-4-12.

La maggior parte delle prove di immunità viene svolta all'interno della camera schermata (Figura 12).

1.5.2. Misurazione ed analisi acustiche

L'analisi acustica consente di esaminare in dettaglio le emissioni sonore di apparecchiature in funzionamento. Lo scopo può essere la risoluzione di problemi di rumorosità, la certificazione della potenza acustica o la ricerca di quegli accorgimenti che rendano più "gradevole" il rumore percepito.

Il laboratorio, con il fine di eseguire misure di Olografia acustica, ovvero l'identificazione e misura di sorgenti acustiche, oppure analisi vibro acustiche, può contare sulla camera riverberante più grande d'Europa (Figura 13) e una camera silente, interconnessa con la riverberante (Figura 14). [3]

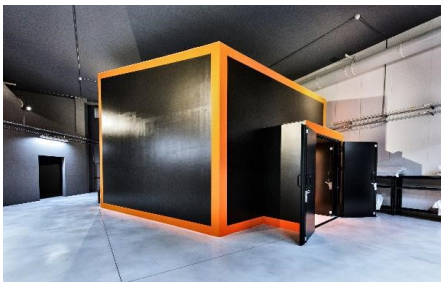


Figura 13 - Camera riverberante

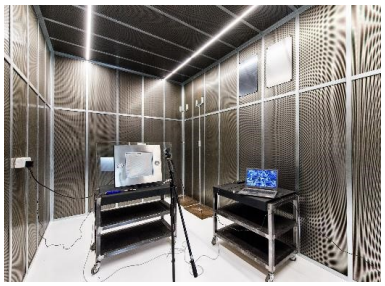


Figura 14 - Camera silente

1.5.3. Test specifici sviluppati internamente

Il laboratorio EPL esegue test che non sono necessari ai fini della conformità di un prodotto ma non meno importanti. Queste verifiche hanno generalmente il fine di stabilire se un elettrodomestico raggiunge quei requisiti di qualità e performance attese. Alcuni esempi di queste analisi sono: test di affidabilità su componenti e prodotti, test di invecchiamento accelerati in camera climatica, analisi quantitative e qualitative per la valutazione della captazione di prodotti aspiranti o visualizzazione grafica dell'andamento dei vettori di velocità del flusso aspirato (quest'ultimo test necessario per poter definire il parametro della portata per quanto riguarda le capacità di aspirazione della cappa ad esempio). [3]

1.5.4. Prove imballo

Una delle missioni dell'imballaggio è quella di preservare l'integrità del prodotto, dal produttore all'utilizzatore.
La necessità di proteggere adeguatamente un prodotto e la contemporanea necessità di essere conformi al decreto Ronchi del 1997, che obbliga il produttore ad utilizzare imballi a più basso impatto ambientale possibile (attraverso un minor utilizzo di materie prime), da sole giustificano l'esigenza di un'attenta analisi degli stessi.
Le principali prove che vengono eseguire sugli imballi sono:

- Prove imballo su oggetti peso 300kg max ed ingombro massimo 1x2x2 m (LxPxH);
- Test di impatto secondo ISO 2244 e ISO 2248;
- Clamp test;
- Test di vibrazione secondo ISO 2247 & ASTM 4728D;
- Test di compressione in accordo ISO 2874;
- Analisi della qualità del cartone:
    - ECT – Edges Compression Test FEFCO n°8;
    - COBB – assorbimento acqua FEFCO n°7;
    - Spessore;
    - Grammatura. [3]

1.5.5. Prove affidabilità

L'affidabilità ha un ruolo fondamentale nella soddisfazione del cliente, con profondi impatti sulla sicurezza di numerosi prodotti rilasciati sul mercato. Alcune prove eseguite sono:

- Prove vita accelerate in camera climatica o forno;
- Salt spray test;
- Tenuta colle;

- Analisi vernici e serigrafie;
- Azionamenti meccanici;
- Prove vita prodotto finito. [3]

1.5.6. Certificazione prodotto connesso

Il laboratorio svolge quindi un ruolo di assoluta importanza all'interno dell'azienda, senza il suo supporto non sarebbe infatti possibile commercializzare i prodotti. Di seguito è brevemente descritto il processo che porta alla definizione delle prove da effettuare con il fine di certificare un prodotto connesso come ad esempio la cappa trattata all'interno di questa tesi.

La certificazione di prodotto è l'attestazione che un apparecchio, prima di essere immesso sul mercato, sia stato sottoposto da un organismo accreditato di terza parte, indipendente rispetto a chi vende e produce, alle verifiche necessarie per accertare la conformità ai requisiti previsti dalle direttive Europee e Internazionali.
La certificazione può essere cogente o volontaria. Nel primo caso è un requisito obbligatorio previsto dalla legge e il prodotto non può essere commercializzato se prima non viene sottoposto da un organismo notificato a tutte le verifiche necessarie. Rientrano in questo ambito i prodotti più complessi quali le apparecchiature a gas, i dispositivi medici, le attrezzature sotto pressione, alcuni prodotti da costruzione. Nel caso della certificazione volontaria è invece il fabbricante che spontaneamente decide di far verificare i suoi prodotti da un organismo di terza parte, al fine di avere un'ulteriore garanzia della qualità dei propri prodotti e offrire al mercato uno strumento di selezione, trasparente e immediato, nella fase di acquisto.

Per quanto riguarda la cappa connessa la certificazione è cogente e la direttiva che istituisce un quadro normativo per la messa a disposizione sul mercato e la messa in servizio delle apparecchiature radio nell'Unione è la DIRETTIVA 2014/53/UE DEL PARLAMENTO EUROPEO E DEL CONSIGLIO del 16 aprile 2014 concernente l'armonizzazione delle legislazioni degli Stati membri relative alla messa a disposizione sul mercato di apparecchiature radio e che abroga la direttiva 1999/5/CE. La direttiva fornisce inoltre una definizione di apparecchiatura radio, descrivendola come un prodotto elettrico o elettronico che emette e/o riceve intenzionalmente onde radio a fini di radiocomunicazione e/o radio determinazione o un prodotto elettrico o elettronico che deve essere completato con un accessorio, come un'antenna, per poter emettere e/o ricevere intenzionalmente onde radio a fini di radiocomunicazione e/o radio determinazione.

Vengono inoltre fissati quelli che sono i requisiti essenziali, riportati di seguito.

Articolo 3

Requisiti essenziali

1. Le apparecchiature radio sono fabbricate in modo da garantire:

> *a) la protezione della salute e della sicurezza di persone e di animali domestici e beni, compresi gli obiettivi riguardanti i requisiti di sicurezza previsti dalla direttiva 2014/35/UE, ma senza applicazione di limiti minimi di tensione;*
>
> *b) un adeguato livello di compatibilità elettromagnetica ai sensi della direttiva 2014/30/UE.*

2. Le apparecchiature radio sono fabbricate in modo da utilizzare efficacemente lo spettro radio e supportare l'uso efficiente dello spettro radio stesso al fine di evitare interferenze dannose. [4]

Le direttive non sono mai specifiche, ma indicano in maniera molto generica quali sono i requisiti che il prodotto finale deve soddisfare. Possiamo concentrarci principalmente sui punti 3.1b e 3.2, rispettivamente legati alla compatibilità elettromagnetica e all'uso dello spettro radio.

Per un generico produttore è difficile capire da queste descrizioni come rispettare i requisiti e proprio per questo sono realizzate delle linee guida che forniscono tutte le informazioni e riferimenti agli standard armonizzati necessari al soddisfacimento dei requisiti stessi.

Le norme armonizzate sono le norme in cui viene descritto come verificare i requisiti fissati dalle direttive in materia di sicurezza, salute e tutela dell'ambiente. La dicitura "norma armonizzata" è sinonimo di "standard armonizzato". Le norme tecniche armonizzate vengono elaborate dagli Organismi di Normazione Europei: CENELEC (Comité européen de normalisation en électronique et en électrotechnique) per i prodotti del comparto elettrico/elettronico, ETSI (European Telecommunications Standards Institute) per i prodotti nel settore delle telecomunicazioni, CEN (Comité européen de normalisation) per i prodotti degli altri settori. Le norme armonizzate determinano l'idoneità di un certo metodo di verifica a presumere la conformità del prodotto alla direttiva. Tali norme sono dette "armonizzate", quando i loro riferimenti sono pubblicati sulla Gazzetta Ufficiale delle Comunità Europee (GUCE) in relazione a una direttiva. L'applicazione completa delle norme armonizzate permette al produttore di porre il prodotto sul mercato senza sottoporre preventivamente il dossier tecnico di fabbricazione a un organismo notificato. Questo permette di effettuare, autonomamente, la certificazione CE dei prodotti e la redazione della dichiarazione di conformità UE**.** Il produttore idoneamente attrezzato, come nel nostro caso, può eseguire le prove nei propri laboratori altrimenti può rivolgersi ad un laboratorio di fiducia.

Dato che il prodotto è un dispositivo connesso, l'organo di riferimento è l'ETSI e fornisce una guida (ETSI EG 203 367) per l'applicazione degli standard armonizzati che coprono gli articoli 3.1b e 3.2 della direttiva 2014/53/EU RED per dispositivi non radio ma che integrano apparati radio; la cappa connessa è un prodotto di questo tipo, si parte infatti da un elettrodomestico non radio in cui viene inserito un modulo Wi-Fi. [4]

All'interno della linea guida sono presentate diverse combinazioni di prodotto radio e non radio ma nel nostro caso andiamo ad analizzare lo scenario #1 (Figura 15), situazione in cui i due prodotti che generalmente sono in vendita sul mercato distintamente sono stati uniti in un unico prodotto, uno dentro l'altro.

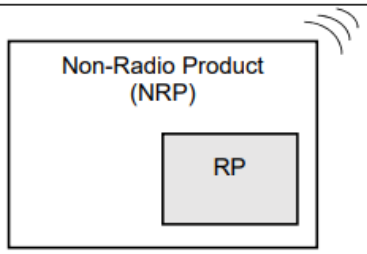
Scenario #	Equipment under the RED [i.1]	Conformity Assessment Procedure(s) (CAP) available	Reference available to demonstrate conformity with articles 3.1b and 3.2 of the RED [i.1]
1		RED CAP (for the RP) EMC DIRECTIVE CAP (for the NRP) Δ (for the combination) (see note)	ETSI EG 203 367

Figura 15 - Estratto ETSI EG 203 367

La tabella permette di capire come riuscire a rispettare i due requisiti della normativa RED: è infatti sufficiente affidarsi alla linea guida per soddisfare la direttiva.

Per quanto riguarda il punto 3.1b la linea guida dice di eseguire tutti test di EMC richiesti per quella particolare categoria di prodotto. Il rispetto dei requisiti EMC per prodotti non radio che installano al loro interno dispositivi radio in accordo al punto 3.1b è ottenuto sulla base dello standard Europeo ETSI EN 303 446-1. Questo documento basato sulla linea guida ETSI EG 203 367 contiene le misurazioni, limiti di emissione e criteri di valutazione delle performance che sono necessari per la valutazione di prodotti non radio che installano dispositivi radio. Al suo interno sono quindi riportate tutte le prove da eseguire e le normative ETSI e CENELEC di riferimento. È compito del laboratorio svolgere tutte le prove richieste.

Queste normative seguono una struttura fissa e facilmente comprensibile, contenendo al loro interno definizioni, setup di misura, caratteristiche ambientali in cui eseguire la prova ed i criteri di valutazione. Quest'ultimi sono organizzati per categorie di prodotto, è quindi necessario identificare il DUT (Device Under Test) all'interno di questa classificazione con il fine di poter stabilire se i risultati raggiunti con le prove sono soddisfacenti o meno. Generalmente le norme coprono tutti i tipi di prodotto, quindi un fornitore riesce ad inserire in maniera univoca il proprio dispositivo all'interno di una categoria o, se necessario, sono presenti categorie e limiti creati ad hoc per prodotti molto specifici e particolari. Nell'eventualità in cui il DUT sia un nuovo progetto ed estremamente particolare se non è possibile inserirlo in una categoria è sempre possibile andare ad utilizzare come riferimento la norma generica, che impone dei limiti minimi di sicurezza ed affidabilità. Naturalmente i limiti generici possono risultare non adatti al prodotto in questione, proprio per questo sono state create categorie con limiti specifici, che possono poi essere superiori o inferiori in base al contesto applicativo finale. Alla fine dei test viene compilato un Dossier riepilogativo in cui sono riportate le prove fatte e per ognuna di queste vengono indicate: setup di misura, condizioni ambientali, descrizione della prova, risultati ed infine l'esito.

La possibilità di potersi basare su normative ben descritte che non lasciano spazio a dubbi o libere interpretazioni garantisce la ripetibilità delle operazioni e il raggiungimento di un risultato oggettivo e valido.

Per il punto 3.2 invece la linea guida riporta che se il modulo radio utilizzato è installato rispettando una serie di requisiti (distanza da piani metallici ad esempio) allora per esso è valida la certificazione fatta dal costruttore; quindi, non è necessario ripetere prove legate alle sue emissioni. Tuttavia, l'azienda Elica ed il laboratorio EPL impongono un controllo, anche se non necessario ai fini della messa sul mercato, sulla banda di trasmissione occupata e sulla presenza di eventuali armoniche, sia sopra che sotto la banda di utilizzo, dato che l'individuazione di possibili componenti fuoribanda anche a frequenze molto minori dei 2,44 GHz potrebbe andare a disturbare il microcontrollore installato sulla Main Board, che lavora a frequenze dell'ordine dei MHz.

2. La cappa

In questo capitolo sono racchiusi i concetti base legati all'elettrodomestico cappa e come questo sia in grado di integrarsi in un ecosistema smart home. Partendo da una breve presentazione del prodotto in tutte le sue componenti si passerà poi attraverso i principi secondo cui scegliere la tipologia di aspirazione più adatta alle proprie esigenze e una breve introduzione sulla smart home. Verranno poi descritti gli attuali metodi di interfacciamento con la cappa e come effettivamente il comando richiesto da User Interface o App Elica Connect viene trasportato ed elaborato dall'elettronica a bordo dell'elettrodomestico (protocollo One-Wire).

2.1. Struttura dell'elettrodomestico

La cappa è essenziale per respirare aria pulita in cucina. La sua funzione principale consiste nel migliorare la qualità dell'aria, eliminando i fumi della combustione, i cattivi odori e i vapori della cottura, dannosi sia per le persone che per mobili e pareti. La cappa è quindi un prezioso alleato al proprio benessere e scegliendola ci si deve assicurare che garantisca:

- una performance di aspirazione adeguata alle proprie necessità e al proprio ambiente, così da ottenere il giusto ricambio dell'aria e un minore consumo di energia elettrica;
- una fonte di luce efficace per rendere più confortevole la preparazione dei cibi;
- un design in linea con i propri gusti e le proprie esigenze;
- una buona usabilità e silenziosità.

Una cappa da cucina in genere è composta dalle seguenti parti:

- Camino: rappresenta il collegamento verso l'esterno che permette di espellere l'aria aspirata. La sua presenza non è necessaria nella versione filtrante, dato che l'aria viene reimmessa nell'ambiente;
- AGR o Assieme Gruppo Motore: è l'assieme che viene installato sulla cappa e contiene al suo interno il motore elettrico (necessario per l'aspirazione), board elettriche, cablaggi, supporti, case metallico e connettori. Nelle immagini di seguito è riportato il CAD 3D sia del motore sia dell'AGR finale che viene installato nell'elettrodomestico (Figura 16).

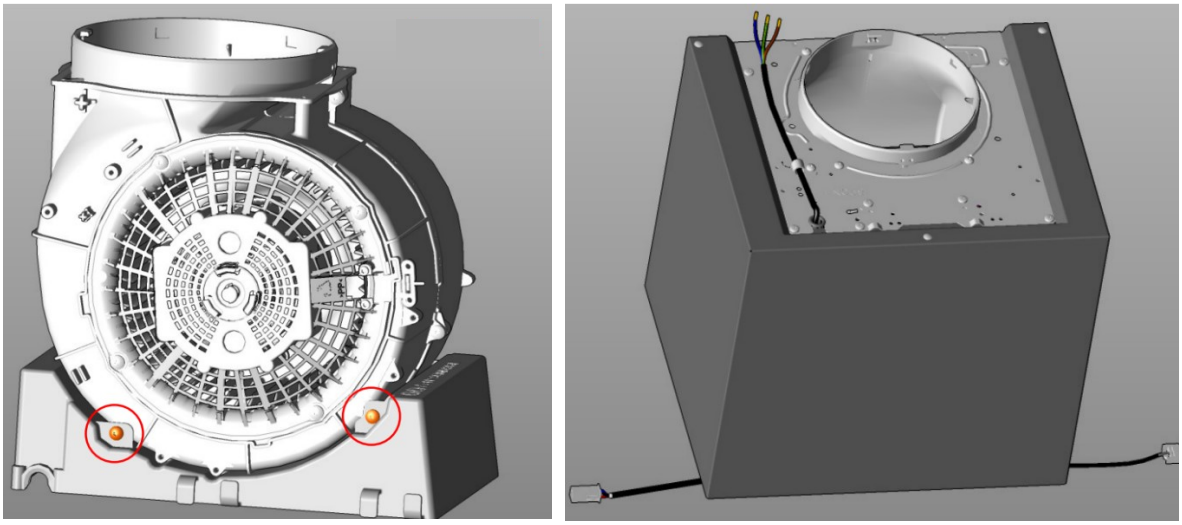


Figura 16 - AGR

- Comandi: sono la UI (User Interface, Figura 17) a pannello o pulsantiera con la quale l'utente si interfaccia con la cappa. Esistono molteplici possibilità sulla base del tipo di cappa e della sua estetica. Slider con selezione lineare della velocità, slider elettronici, pulsantiere meccaniche, pulsantiere Soft Touch, pulsantiere Light Soft retroilluminate, fino al Touch Screen per la gestione elettronica del prodotto. Ad ogni prodotto il comando più adatto.

Figura 17 - Esempi User Interface

Oltre a quelli presenti sul prodotto la cappa è controllabile anche da remoto utilizzando il telecomando. Ma da cosa nasce la necessità di un ulteriore nuovo tipo di comando? La risposta è nell'impegno di Elica di garantire all'utente la miglior esperienza possibile con i propri prodotti; quindi, poter utilizzare lo smartphone o la voce può risultare estremamente comodo in svariate occasioni. Proprio per questo nasce la necessità di dover progettare una cappa in grado di essere controllata da remoto tramite l'utilizzo dell'app di proprietà Elica Connect o attraverso la propria voce grazie alla Skill Elica integrata nei sistemi Amazon Alexa. La cappa entra quindi a far parte dell'ecosistema Smart-home, garantendo un'esperienza di cucina del tutto nuova.

- Filtri: esistono diversi tipi di filtri installabili in una cappa. Filtro antigrasso (Figura 18), sempre presente e posto immediatamente all'ingresso del prodotto, ha il compito di proteggere tutto l'interno della cappa filtrando dall'aria aspirata le particelle di grasso più pesanti. Tali filtri possono essere realizzati in carta o materiale sintetico (da sostituire ciclicamente), in alluminio, griglie filtro in alluminio (GFA) e griglie filtro in inox (GFI). Ad eccezione dei primi tutti gli altri sono facilmente smontabili dalla cappa e lavabili sia a mano con sapone liquido da cucina che in lavastoviglie.

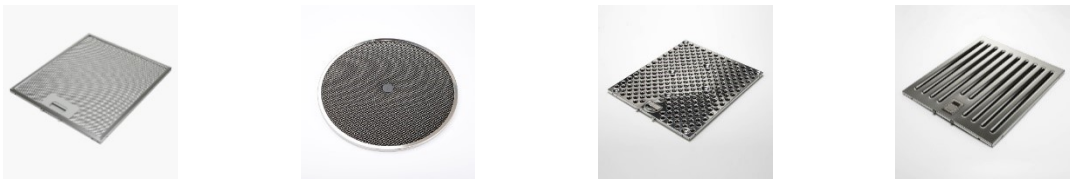


Figura 18 - Vari esempi di filtri antigrasso

I filtri a carboni attivi hanno una struttura estremamente porosa e una grande area superficiale che dona loro un'importante capacità adsorbente. Hanno lo scopo di purificare e depurare l'aria dagli odori, i fumi e i vapori prodotti giorno dopo giorno dalle varie attività in cucina. Sono generalmente utilizzati nelle cappe filtranti proprio per purificare al massimo l'aria prima di farla ricircolare nell'ambiente e vanno sostituiti ciclicamente ogni 3-4 mesi circa, in base all'utilizzo. Elica propone in aggiunta una tecnologia innovativa, il Filtro carbone rigenerabile HP (High Performance). Questo particolare filtro garantisce un'elevata efficacia, ma contrariamente alla versione tradizionale il suo

ciclo di vita è estremamente più lungo. Non va infatti sostituito, ma può essere facilmente rigenerato e riapplicato sulla cappa. Ha una durata di tre anni e può essere lavato in lavastoviglie (ad una temperatura consigliata di 65 °C) ed una asciugatura in forno a 100 °C per dieci minuti. A questi si aggiunge anche il Filtro Ceramico, rigenerabile con il solo passaggio in forno a 200°C per 45 minuti ogni 2/3 mesi, capace di garantire fino a 5 anni di utilizzo.

Figura 19 – In ordine da sinistra: filtro carbone usa e getta, rigenerabile e ceramico

- Illuminazione: sorgenti luminose, sia sul piano da lavoro che luci ambienti per il fattore estetico, in grado di garantire l'illuminazione necessaria sopra al piano cottura. La maggior parte dei modelli sono dotati della sola luce principale, generalmente una barra led o un piano luminoso, ma in alcuni casi, soprattutto nelle cappe dal design più ricercato, oltre alla luce principale spesso è anche installata una luce ambiente, utilizzabile per illuminare direttamente la stanza o comunque come elemento d'arredo. [5]

2.2. Installazione in ambiente domestico

Ogni modello di cappa non contiene al suo interno tutti i filtri appena descritti; infatti, ad eccezione del filtro grassi sempre presente i filtri odori sono installati nelle sole versioni filtranti del prodotto. Le cappe sono infatti divise in due categorie: cappe aspiranti e cappe filtranti.

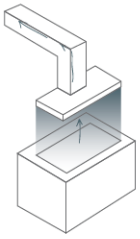


Figura 20 - Cappa aspirante

Cappa aspirante
Nel primo caso la cappa è solitamente posizionata al di sopra del piano di cottura ed aspira l'aria grazie all'azione di un ventilatore elettrico posto al suo interno. L'aria aspirata, satura di vapori e di odori, passa attraverso un sistema di filtri antigrasso che la purifica. Dopo essere stata filtrata, l'aria aspirata viene convogliata all'interno del tubo collegato al camino che la porta all'esterno. Grazie alla loro azione, le cappe aspiranti catturano l'aria viziata e la eliminano definitivamente, contribuendo attivamente a diminuire l'inquinamento domestico (Figura 20).

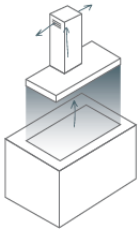


Figura 21 - Cappa filtrante

Cappa filtrante
Nel secondo caso, la cappa filtrante è un elettrodomestico che si installa in una cucina in cui non è presente uno scarico verso l'esterno. Al contrario della cappa aspirante, che aspira l'aria viziata e la convoglia all'esterno, la cappa filtrante, come suggerisce il suo nome, preleva, filtra e purifica l'aria così da trattenere gli odori, i fumi e i grassi che si sprigionano in cucina durante la preparazione dei pasti e restituisce aria pulita nello stesso ambiente. Una volta purificata dalle sostanze più nocive, l'aria raccolta dalla cappa filtrante viene reimmessa nello stesso ambiente (Figura 21). [5]

Ricollegandosi al concetto di installazione della cappa, solitamente intesa come prodotto montato a parete, la possibilità di poter scegliere tra cappe aspiranti e filtranti permette una maggiore libertà nel suo posizionamento all'interno della stanza. Possiamo infatti distinguere quattro casi principali:

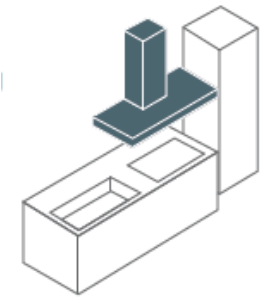


Figura 22 - Cappa a parete

A parete
La cucina è posizionata contro la parete con il piano cottura adiacente al muro. Anche la cappa è quindi installata a parete (Figura 22). Per applicazioni di questo tipo sono adatte sia le classiche cappe T-Shape (aspiranti) oppure le verticali/hand free (filtranti).

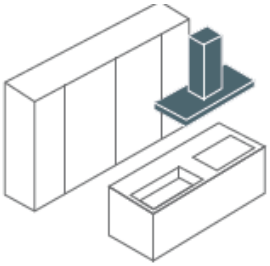


Figura 23 - Cappa a isola

A isola
La cucina è posizionata al centro della stanza con il piano cottura distante dal muro. La cappa è quindi da installare appesa al soffitto. Per applicazioni di questo tipo sono adatte le isole (generalmente riprendono la forma delle T-Shape, quindi aspiranti) o modelli filtranti e dal design moderno come le Ceiling e le sospese (Figura 23).

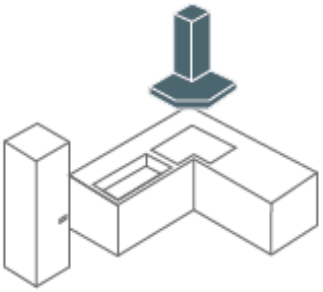


Figura 24 - Cappa ad angolo

Ad angolo
La cucina si estende lungo due pareti della stanza e il piano di cottura è posizionato a ridosso dell'angolo. La cappa è da installare tra le pareti adiacenti. È presente una apposita linea dedicata a questo scenario, linea che conta però su pochi prodotti data la domanda relativamente bassa (Figura 24).

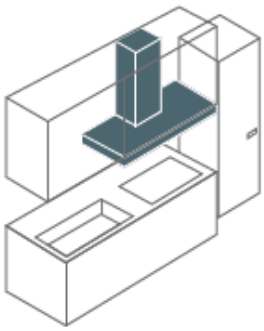


Figura 25 - Cappa ad incasso

Ad incasso
Il piano di cottura è posizionato sotto a un pensile all'interno del quale viene installata la cappa. Le Built-in sono la linea di cappe prodotte per queste applicazioni (Figura 25). [5]

Le installazioni appena descritte sono da considerarsi valide per la cappa standard, come intesa nell'ideale comune. Prodotti come i piani aspiranti invece o le cappe a scomparsa richiedono una progettazione dietro al loro acquisto, con il fine di realizzare anticipatamente le tubature necessarie. Prodotti di questo tipo non

sono un semplice elettrodomestico da aggiungere alla propria cucina, bensì sono il punto di partenza dal quale progettare intorno tutto il resto.

Nel momento in cui si decide di acquistare una cappa, oltre alla scelta del modello filtrante o aspirante e del tipo di installazione da effettuare un parametro molto importante che deve guidare la scelta di un prodotto è l'aspirazione. La potenza di aspirazione necessaria dipende normalmente dalle dimensioni della cucina e dal modo di cucinare. Utilizzando un semplice calcolo è possibile definire quale debba essere la portata adeguata del prodotto da installare. Basterà moltiplicare il volume della stanza per dieci e ottenere in questo modo la portata ideale per quell'ambiente. La cappa, infatti, per garantire un buon ricambio o ricircolo dell'aria, deve essere in grado di cambiare l'aria contenuta nella stanza circa dieci volte in un'ora. Ad esempio, per una cucina di dimensioni 5 x 3 m e di altezza 2,5 m si deve svolgere il seguente calcolo:

$$(5 \times 3 \times 2{,}5) \times 10 = 375$$

Quindi qualsiasi prodotto la cui portata massima risulterà superiore a 375 m^3/h potrà garantire un'areazione del locale piena ed efficace. Tuttavia, è importante non dimenticare comunque le proprie abitudini culinarie, alcune linee guida standard possono infatti essere:

1. Per chi abitualmente prepara pasti rapidi e ha una cucina di dimensioni ridotte, il modello da preferire è quello con una portata fino a 200 – 300 m^3/h;
2. Per una famiglia composta da tre/quattro persone, con una cucina di medie dimensioni e alimentazione di tipo misto, il modello da preferire è quello con una portata pari a 300 – 400 m^3/h;
3. Per famiglie numerose, per gli appassionati di arte culinaria o per riunire numerosi amici in un'ampia cucina nella quale sperimentare ricette esotiche, la portata di aspirazione della cappa dovrà almeno essere di almeno 400 m^3/h. [5]

I valori di portata di una cappa sono calcolati sulla base della norma internazionale IEC 61591. Questa norma la si applica a tutti gli estrattori di fumo per cucina che incorporano ventole per l'estrazione dell'aria ma è anche valida per tutte quelle cappe che hanno il motore esterno; quindi, che sono separate dal dispositivo in casa ma che comunque sono comandate da quest'ultimo. Il documento definisce le performance che l'elettrodomestico deve raggiungere e come misurarle. La portata, ad esempio, deve essere testata in condizioni di utilizzo reali; quindi, non direttamente all'uscita del camino (uscita libera) ma al termine di una tubatura lunga complessivamente 2 metri che al centro presenta una curvatura di 90° (Figura 26). In questo modo non c'è più differenza tra i risultati di laboratorio e quelli nella cucina reale, in quanto la misurazione è effettuata in condizioni che si avvicinano davvero all'utilizzo pratico, inclusa anche la perdita di potenza causata da un condotto di uscita standard.

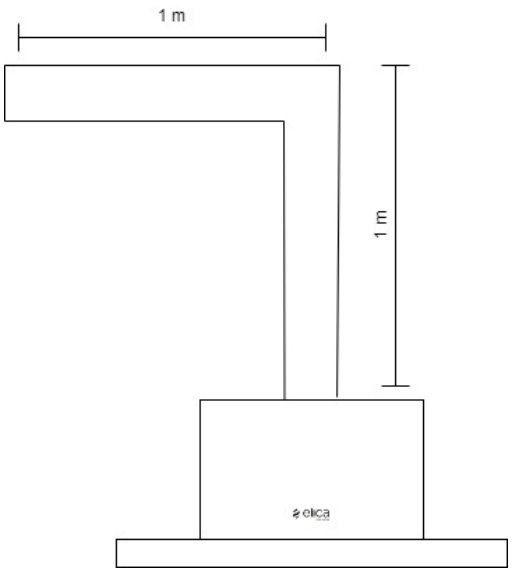


Figura 26 - Setup prove di aspirazione

L'efficace aspirazione dei fumi della cottura è garantita sia da una corretta installazione del prodotto, evitando quindi che il camino faccia troppa strada prima di raggiungere l'esterno o che questo presenti troppe curve e restringimenti, sia dal corretto utilizzo dell'elettrodomestico stesso. È buona norma accendere la cappa alla prima velocità nel momento in cui si inizia la cottura, aumentando l'aspirazione nel momento in cui si verifica la maggior produzione di fumo e odori. A cottura conclusa, tornare alla velocità più bassa mantenendo la cappa accesa per altri 5 – 10 minuti. Nelle cappe designate al segmento medio o alto è implementata una modalità di funzionamento automatica, che in base alle misurazioni di un sensore di temperatura installato nella cappa (e collegato alla User Interface) riesce a regolare in maniera autonoma la portanza di aspirazione necessario in grado di garantire la velocità più adatta in quel momento; di base la logica è molto semplice: maggiore è il calore rilevato, quindi sono accesi più fuochi o stanno entrando nella cappa vapori molto caldi, maggiore dovrà essere la velocità di aspirazione. Con la nuova cappa sviluppata in questa tesi invece si ha anche una

evoluzione sotto questo punto di vista, sostituendo questa soluzione con un sensing module molto più complesso formato da NTC (sensore di temperatura), VOC (sensore per la qualità dell'aria) e sensore di umidità. In questo modo l'entità della misurazione risulta essere più completa e corretta, garantendo una migliore gestione della modalità di aspirazione automatica.

2.3. Metodi di interfacciamento con il prodotto

Come anticipato in precedenza, la cappa può essere controllata in tre modi: interagendo direttamente con il prodotto tramite l'interfaccia, mediante l'utilizzo dei comandi remoti associati all'App Elica Connect ed Alexa oppure utilizzando il telecomando fornito in dotazione ma comunque acquistabile anche esternamente a parte. Qualunque sia la modalità di interazione scelta, il comando richiesto deve essere in grado di raggiungere la Main Board, cuore dell'elettrodomestico sulla quale risiede il microcontrollore, e per fare ciò ad essa sono collegati due moduli:

- User Interface, è l'interfaccia fisica presente sul dispositivo ed attraverso la pressione dei pulsanti o lo sfioramento del pannello, a seconda della soluzione presente, è possibile andare ad interagire con la cappa. Nel caso della Superplat (Figura 27) la User Interface è composta da sette pulsanti capacitivi, ed è rappresentata di seguito.

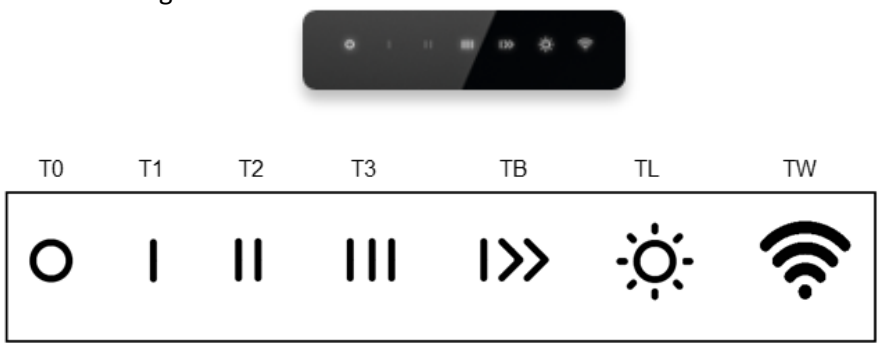


Figura 27 – User Interface Superplat

I pulsanti sono così organizzati:

  - T0: motore off/stand-by;
  - T1 – TB: cinque velocità per le ventole, di cui una "boost" che può essere attivata solo per una durata di tempo limitata attraverso una seconda pressione del pulsante TB;
  - TL: Accensione e spegnimento luce principale, una volta accesa la luce, tramite successive pressioni è possibile regolarne l'intensità fino a spegnerla;
  - TW: pulsante per abilitare la connectivity, utilizzato sia per l'on-boarding sull'App Elica Connect sia per connettere la cappa alla rete Wi-Fi (ma solo dopo aver configurato correttamente la cappa sul proprio dispositivo mobile).
    Il pulsante permette infatti di andare ad attivare o mettere in stand-by il "Core" Wi-Fi, secondo nodo connesso alla Main Board.

  La pressione di un pulsante ed esecuzione dell'azione richiesta è confermata dall'accensione di un led posto al di sotto del pulsante stesso.

- Scheda "Core" Wi-Fi Module, che contiene al suo interno l'ESP32, generico modulo MCU Wi-Fi + Bluetooth. Completano l'ESP32 due core CPU con una frequenza di clock aggiustabile tra gli 80 MHz e 240 MHz. La memoria Flash da 4MB presente al suo interno permette di andare a memorizzare alcune informazioni importanti come il codice identificativo della cappa (CUID), la password per la

connessione al broker MQTT ed il proprio indirizzo MAC, informazioni necessarie per garantire il corretto funzionamento del dispositivo. L'interazione con questo modulo verrà descritta nel paragrafo successivo. [6]

2.3.1. Studio del protocollo One-Wire bus

Le due board scambiano messaggi e dati con la Main Board utilizzando un protocollo UART One-wire Half duplex NRZ unipolare e sono cablati come riportato di seguito (Figura 28).

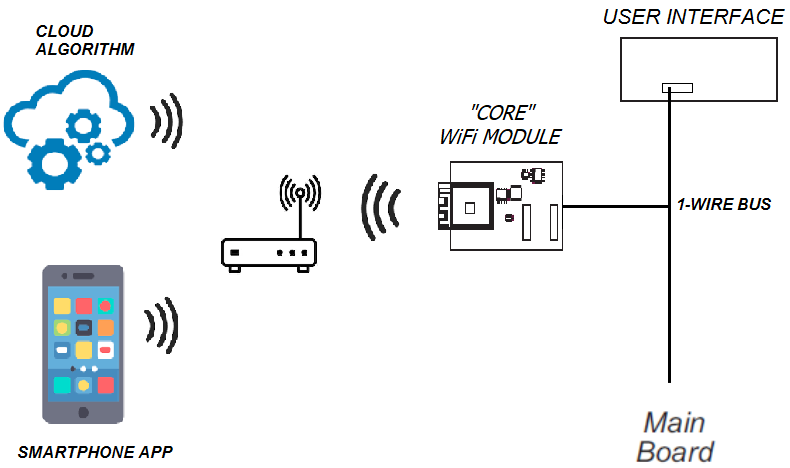


Figura 28 - Schema 1-Wire bus

Volendo entrare più nel dettaglio del protocollo, il collegamento tra le schede è realizzato mediante un cavo ad 8 fili che termina su un connettore Lumberg MICS 08. La configurazione dei pin comprende l'alimentazione a 12 V, la massa, l'on/off del modulo Wi-Fi e solamente il pin 8 è quello utilizzato come bus di comunicazione. La stringa binaria che viene trasmessa è rappresentata nel seguente modo: 1 è un DC bias a 5 V, 0 invece è l'assenza del segnale. [7] Come evidenziato nell'immagine sopra (Figura 30), il canale di comunicazione è condiviso tra le due board connesse alla Main, proprio per questo è utilizzata una struttura "Round Robin", in cui i vari nodi connessi allo stesso bus si alternano per trasmettere. Con il fine di garantire una corretta esecuzione viene nominato un nodo ID=1 (generalmente la Main Board) che si occupa si rilevare tutti gli altri nodi attivi connessi (fino ad un massimo di sette) per poi associargli un ID (compreso quindi tra 2 e 7, nel nostro caso saranno utilizzati solo ID=2 e ID=3 dato che sono soltanto due le schede connesse alla Main attraverso questo bus). Il suo compito è quello di riservare un certo intervallo di tempo ad ognuno per farlo comunicare (Figura 29).

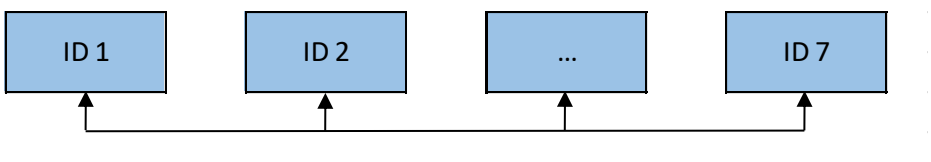


Figura 29 - ID Value 1-Wire bus

L'intervallo ha solitamente una durata di 10 ms, ma può essere aggiustato sulla base dei requisiti hardware. In questo slot temporale il nodo master (ID=1) trasmette un Token in modalità broadcast e quindi ricevuto da tutti, composto da due byte all'interno del quale, tra le varie informazioni, viene indicato l'ID di chi deve trasmettere. Segue quindi la trasmissione del messaggio da parte del nodo interessato utilizzando un particolare pacchetto contenente il destinatario e l'operazione che si vuole eseguire (eseguire un'azione,

richiedere informazioni o ACK). Il terzo ed ultimo messaggio trasmesso è un ack del ricevitore o un codice di errore, a conferma della corretta/errata ricezione del pacchetto. L'eventuale azione da eseguire può essere svolta in qualsiasi momento dal ricevitore, ma l'effettiva trasmissione di una risposta ad una richiesta può essere fornita solamente nell'intervallo di tempo dedicato all'ID interessato. [7]

Basandoci sulla configurazione della cappa, possiamo fare un esempio per nodo con il fine di chiarire lo scambio dei messaggi eseguito.

Per l'User Interface possiamo analizzare il caso in cui l'utente vada a variare la velocità della cappa premendo il pulsante T3 sulla User Interface (Figura 30).

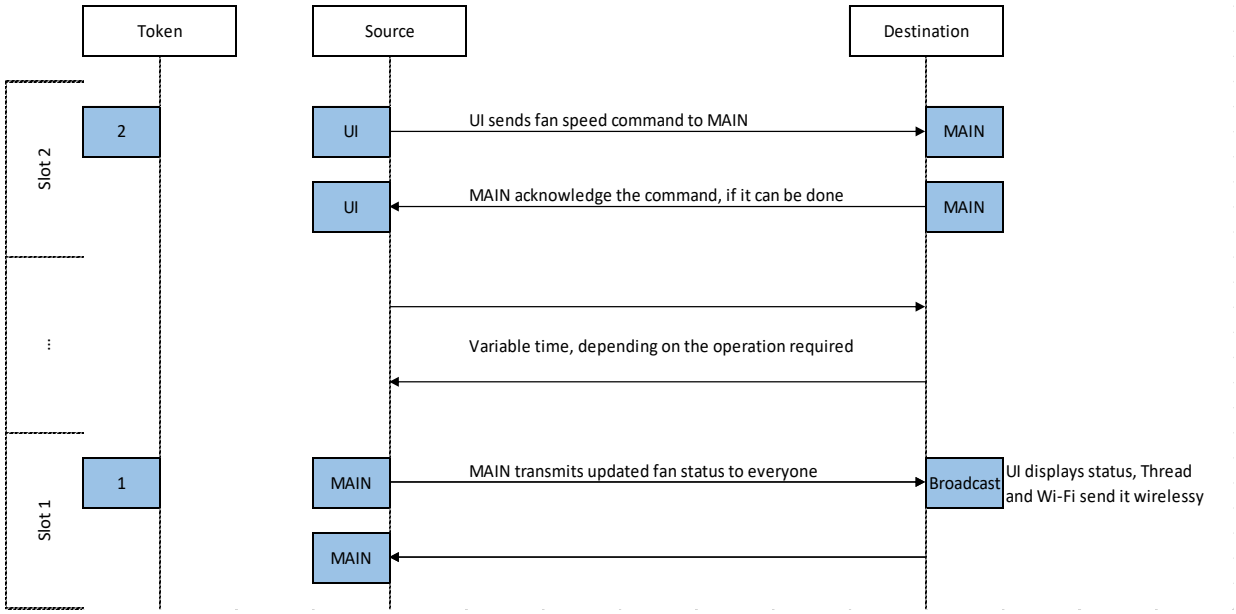


Figura 30 - Esempio di comunicazione

L'UI trasmette la richiesta di variare la velocità della ventola di aspirazione e la Main risponde con un ACK a conferma della corretta ricezione. Segue un certo intervallo di tempo in cui effettivamente la Main board va a variare il PWM trasmesso alla scheda del motore elettrico per regolarne la velocità e ad operazione conclusa, in corrispondenza dell'intervallo temporale associato ad ID=1, la scheda comunica a tutti la variazione della velocità della cappa. In questo modo il modulo Wi-Fi può andare a comunicare al Database la variazione di velocità così da garantire un aggiornamento Real-time anche dell'App. Allo stesso modo il messaggio trasmesso dalla Main viene ricevuto anche dalla UI, che può quindi andare a variare eventuali led luminosi, ad esempio spegnendo il led al di sotto di T2 (velocità di partenza) ed accendendo quello al di sotto di T3 (velocità impostata da User in precedenza). Tutto il processo che porta all'aggiornamento del led richiede un tempo minimo, da 30 ms a qualche decimo di secondo; quindi, per l'utente l'accensione del led e la variazione della velocità sono istantanee. Per quanto riguarda invece l'aggiornamento dell'App la modifica può subire dei ricardi a seconda della qualità della rete internet, ma in generale, in presenza di una connessione discreta, il tutto è istantaneo.

Volendo analizzare una trasmissione che riguarda direttamente il nodo Wi-Fi invece viene descritto il seguente caso (Figura 31):

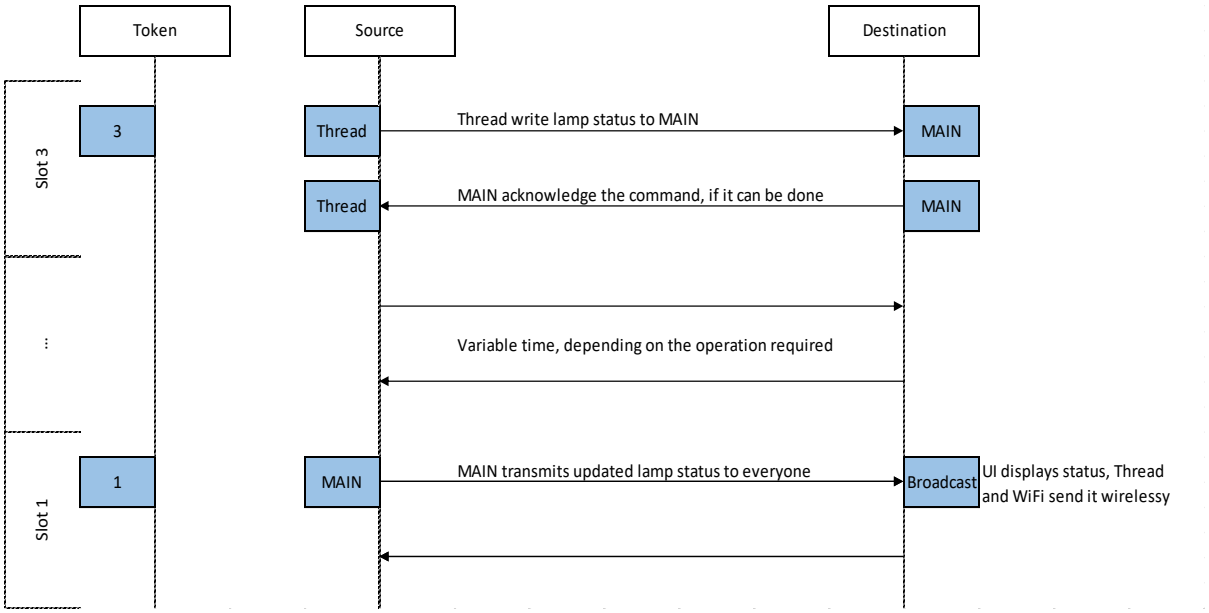


Figura 31 - Esempio di comunicazione

In questo caso l'utente ha deciso di accendere la luce della cappa da App. Trascurando in questa fase la comunicazione tra App e modulo Wi-Fi sulla cappa (aspetto che verrà analizzato nel capitolo successivo) quest'ultimo deve trasmettere alla scheda Main la variazione richiesta. In corrispondenza dello slot temporale a lui associato invia la richiesta di, ad esempio "accensione luce", alla scheda principale e come in precedenza riceve un ACK di conferma ricezione. La Main board va quindi ad accendere la luce e quando possibile trasmette la variazione in maniera broadcast, così che l'User Interface possa andare ad accendere il corrisponde LED al di sotto del pulsante luce (TL).

3. Protocolli ed architettura di rete

In questo capitolo è riportata una descrizione dei vari protocolli di comunicazione utilizzati durante tutte le fasi di utilizzo della cappa: dalla prima programmazione del modulo Wi-Fi, passando per la registrazione sull'App fino alla comunicazione App – Dispositivo vera e propria. Successivamente verrà descritta l'attuale Architettura di rete utilizzata da Elica per i suoi prodotti connessi e come i protocolli descritti in precedenza vengano effettivamente utilizzati.

3.1. Studio ed analisi dei protocolli utilizzati

Attualmente sono disponibili diversi standard e protocolli che possono essere utilizzati in un ecosistema Smart Home e

3.1.1. HTTP

L'Hypertext Transfer Protocol (HTTP) è un protocollo a livello applicativo usato come principale sistema per la trasmissione d'informazioni sul web.
L'HTTP lavora con un'architettura di tipo client/server: il client esegue una richiesta e il server restituisce la risposta mandata da un altro host. Nell'uso comune il client corrisponde al browser ed il server la macchina su cui risiede il sito web. Ci sono quindi due tipi di messaggi HTTP: messaggi richiesta (detti HTTP requests) e messaggi risposta (detti HTTP responses). [8]

HTTP differisce da altri protocolli di livello 7 come FTP, per il fatto che le connessioni vengono generalmente chiuse una volta che una particolare richiesta (o una serie di richieste correlate) è stata soddisfatta. Questo comportamento rende il protocollo HTTP ideale per il World Wide Web, in cui le pagine molto spesso contengono dei collegamenti (*link*) a pagine ospitate da altri server diminuendo così il numero di connessioni attive limitandole a quelle effettivamente necessarie con aumento quindi di efficienza (minor carico e occupazione) sia sul client che sul server. Talvolta però pone problemi agli sviluppatori di contenuti web, perché la natura senza stato (*stateless*) della sessione di navigazione costringe ad utilizzare dei metodi alternativi - tipicamente basati sui cookie - per conservare lo stato dell'utente.

Il messaggio di richiesta è composto da quattro parti:

1. Riga di richiesta (request line);
2. Sezione header (informazioni aggiuntive);
3. Riga vuota (CRLF: i 2 caratteri carriage return e line feed);
4. Body (corpo del messaggio).

La riga di richiesta è composta da metodo, URI e versione del protocollo. Il metodo di richiesta, per la versione 1.1 (utilizzata da Elica), può essere uno dei seguenti:

- GET;
- POST;
- HEAD;
- PUT;
- DELETE;
- PATCH;
- TRACE;
- OPTIONS;
- CONNECT.

L'URI, Uniform Resource Identifier (identificatore univoco di risorsa), indica l'oggetto della richiesta, ad esempio la pagina web che si intende ottenere.

I metodi HTTP più comuni sono GET, HEAD e POST. Il metodo GET è usato per ottenere il contenuto della risorsa indicata come URI (come può essere il contenuto di una pagina HTML o come nel nostro caso le informazioni contenute in una specifica risorsa). HEAD è analogo a GET, ma restituisce solo i campi dell'header, ad esempio per verificare la data di modifica del file.

Il metodo POST è usato di norma per inviare informazioni al server (ad esempio i dati di un form o nel nostro caso per scrivere e aggiornare parametri in una particolare risorsa). In questo caso l'URI indica che cosa si sta inviando e il body ne indica il contenuto.

Gli header di richiesta più comuni sono:

- Host: nome del server a cui si riferisce l'URL. È obbligatorio nelle richieste conformi HTTP/1.1 perché permette l'uso dei *virtual host* basati sui nomi.
- User-Agent: identificazione del tipo di client: tipo browser, produttore, versione...
- Cookie: utilizzati dalle applicazioni web per archiviare e recuperare informazioni a lungo termine sul lato client. Spesso usati per memorizzare un token di autenticazione o per tracciare le attività dell'utente.

Il messaggio di risposta è di tipo testuale ed è composto da quattro parti:

- Riga di stato (*status-line*);
- Sezione header;
- Riga vuota (CRLF: i 2 caratteri carriage return e line feed);
- Body (contenuto della risposta).

La riga di stato riporta un codice a tre cifre catalogato nel seguente modo:

- 1xx: Informational (messaggi informativi);
- 2xx: Successful (la richiesta è stata soddisfatta);
- 3xx: Redirection (non c'è risposta immediata, ma la richiesta è sensata e viene detto come ottenere la risposta);
- 4xx: Client error (la richiesta non può essere soddisfatta perché sbagliata);
- 5xx: Server error (la richiesta non può essere soddisfatta per un problema interno del server).

I codici di risposta più comuni sono:

- 200 OK. Il server ha fornito correttamente il contenuto nella sezione body;
- 301 Moved Permanently. La risorsa che abbiamo richiesto non è raggiungibile perché è stata spostata in modo permanente;
- 302 Found. La risorsa è raggiungibile con un altro URI indicato nel header Location. Di norma i browser eseguono la richiesta all'URI indicato in modo automatico senza interazione dell'utente.
- 400 Bad Request. La risorsa richiesta non è comprensibile al server;
- 404 Not Found. La risorsa richiesta non è stata trovata e non se ne conosce l'ubicazione. Di solito avviene quando l'URI è stato indicato in modo incorretto, oppure è stato rimosso il contenuto dal server;
- 500 Internal Server Error. Il server non è in grado di rispondere alla richiesta per un suo problema interno;
- 502 Bad Gateway. Il server web che agisce come reverse proxy non ha ottenuto una risposta valida dal server di upstream;
- 505 HTTP Version Not Supported. La versione di http non è supportata. [8]

Gli header della risposta più comuni sono:

- Server. Indica il tipo e la versione del server. Può essere visto come l'equivalente dell'header di richiesta User-Agent;
- Content-Type. Indica il tipo di contenuto restituito. La codifica di tali tipi (detti Media type) è registrata presso lo IANA (Internet Assigned Number Authority); essi sono detti tipi MIME (Multimedia Internet Mail Extensions), la cui codifica è descritta nel documento RFC 1521. Alcuni usuali tipi MIME incontrati in una risposta HTTP sono:
    - text/html Documento HTML;
    - text/plain Documento di testo non formattato;
    - text/xml Documento XML;
    - image/jpeg Immagine di formato JPEG;

Il client può chiedere al server, nel messaggio di richiesta, di utilizzare due tipi di comunicazione: "non persistente" ovvero per ogni richiesta e relativa risposta viene stabilita una connessione TCP dedicata oppure "persistente", cioè ogni richiesta e relativa risposta è trasferita utilizzando la stessa connessione TCP. È il comportamento predefinito di HTTP 1.1.

Da un lato, le connessioni non persistenti introducono una latenza aggiuntiva rispetto a quelle persistenti di almeno 3 Round Trip Time (RTT). Infatti, al termine di ogni risposta da parte del server si rendono necessari

- 1.5 o 2 RTT per la chiusura della connessione corrente, con la sua stretta di mano conclusiva a tre o quattro passaggi di FIN ed ACK (*three-* o *four-way handshake*).
- 1.5 RTT per l'apertura della nuova connessione, per i tre passaggi di SYN e ACK.

D'altro canto, le connessioni persistenti precludono il parallelismo nelle comunicazioni, giacché il client che abbia diverse richieste da inviare allo stesso server è costretto ad evaderle sequenzialmente, una dopo l'altra. Per queste ragioni, i browser solitamente sfruttano le complementarità prestazionali delle due politiche di comunicazione per massimizzare la loro efficienza: solitamente aprono con ogni server diverse connessioni TCP in parallelo, su cui comunicano con strategia persistente. [8]

3.1.2. HTTPS

In telecomunicazioni e informatica l'HyperText Transfer Protocol over Secure Socket Layer (HTTPS,anche noto come HTTP over TLS) è un protocollo per la comunicazione sicura attraverso una rete di computer utilizzato su Internet. La porta utilizzata generalmente è la 443. Consiste nella comunicazione tramite il protocollo HTTP (Hypertext Transfer Protocol) all'interno di una connessione criptata, tramite crittografia asimmetrica, dal Transport Layer Security (TLS) fornendo come requisiti chiave:

1. un'autenticazione del sito web visitato;
2. protezione della privacy (riservatezza o confidenzialità);
3. integrità dei dati scambiati tra le parti comunicanti. [9]

Nel suo popolare funzionamento su Internet, HTTPS fornisce la sicurezza del sito web e del server web associato con cui una delle parti sta comunicando, proteggendo la comunicazione dagli attacchi noti tramite la tecnica del man in the middle. Inoltre, HTTPS fornisce una cifratura bidirezionale delle comunicazioni tra un client e un server, che protegge la stessa contro le possibili operazioni di eavesdropping, (*azione mediante il quale viene ascoltata segretamente la conversazione privata tra le parti senza il loro consenso*) e tampering (*letteralmente manomissione o alterazione della comunicazione*) falsificandone i contenuti. In pratica, tale meccanismo fornisce una garanzia soddisfacente del fatto che si sta

comunicando esattamente con il sito web voluto (al contrario di un sito falso), oltre a garantire che i contenuti delle comunicazioni tra l'utente e il sito web non possano essere intercettate o alterate da terzi.

Nei browser web, la URI (*Uniform Resource Identifier*) che si riferisce a tale tecnologia ha nome di schema *https* ed è in tutto e per tutto analoga alle URI *http*. Tuttavia, HTTPS segnala al browser di usare il livello di cifratura aggiuntivo TLS per proteggere il traffico internet. TLS è particolarmente adatto al protocollo HTTP, dato che può fornire una qualche protezione, anche se tra le parti comunicanti solo una è autenticata. Questo è il caso di HTTP nelle transazioni su internet, dove tipicamente è il server l'unica parte ad essere autenticata, mentre il client esamina il certificato del server.

Come anticipato, alla base del funzionamento di HTTPS, sopra il *Transport Layer Security* risiede interamente il protocollo HTTP; per questo motivo quest'ultimo può essere criptato del tutto. La cifratura del protocollo HTTP include:

- la richiesta URL (la pagina web che è stata richiesta);
- i parametri di query;
- le intestazioni della connessione (headers);
- i cookies (i quali spesso contengono le informazioni sull'identità dell'utente). [9]

Tuttavia, poiché gli indirizzi IP dei siti web e i numeri di porta fanno parte dei protocolli sottostanti del TCP/IP, HTTPS non può proteggere la loro divulgazione. In pratica, significa che anche se un web server è correttamente configurato, gli eavesdropper possono dedurre l'indirizzo IP e il numero di porta del web server con cui si sta comunicando, oltre alla quantità dei dati trasferiti e la durata della comunicazione (lunghezza della sessione), ma non il contenuto della comunicazione.

I browser web sanno come fidarsi dei siti web HTTPS basati su certificati di autorità che vengono preinstallati nel loro software. Le autorità di certificazione CA (come Symantec, Comodo, GoDaddy e GlobalSign) sono fidate per i creatori di browser web, per fornire certificati validi ai fini della comunicazione. Pertanto, un utente dovrebbe fidarsi di una connessione HTTPS verso un sito web se e solo se tutti i punti seguenti sono verificati:

- L'utente si fida del fatto che il software del browser implementa correttamente il protocollo HTTPS con dei certificati di autorità correttamente preinstallati;
- L'utente si fida dell'autorità di certificazione che garantisce solo siti web legittimi;
- Il sito web fornisce un certificato valido, che significa che è stato firmato da un'autorità di fiducia;
- Il certificato identifica correttamente il sito web (ad esempio quando il browser visita "https://example.com", il certificato ricevuto è appropriatamente quello relativo a "example.com" e non di qualche altra entità);
- L'utente si fida del fatto che il livello di crittografia del protocollo (SSL/TLS) è sufficientemente sicuro contro le possibili operazioni degli eavesdropper.

HTTPS è particolarmente importante attraverso le reti insicure (come i punti di accesso WiFi pubblici), dato che chiunque sulla stessa rete locale può effettuare uno sniffing di pacchetti e scoprire informazioni sensibili e non protette da HTTPS. Oltre a ciò, molti vengono pagati per impegnarsi nel fare packet injection ("iniezione di pacchetti") all'interno di reti wireless allo scopo di fornire un servizio per le pubblicità delle proprie pagine web, mentre altri lo fanno liberamente. Tuttavia, questa operazione può essere sfruttata malignamente in molti modi, come iniettare dei malware su pagine web e rubare informazioni private agli utenti.

Nonostante siano divulgate più informazioni riguardo alla sorveglianza globale di massa e al furto di informazioni personali da parte degli hacker, l'uso di HTTPS per la sicurezza su tutti i siti web sta diventando sempre più importante, a prescindere dal tipo di connessione ad Internet usata. Mentre i metadati delle pagine individuali che un utente visita non sono informazioni sensibili, quando queste informazioni sono combinate insieme possono svelare molto sull'identità dell'utente e comprometterne la privacy stessa.

La maggior parte dei browser visualizza un messaggio di warning se riceve un certificato non valido dal server che funge come autorità di certificazione. I browser meno recenti, quando si connettevano ad un sito web con un certificato non valido, mostravano all'utente un messaggio di dialogo che chiedeva loro se volessero proseguire con la navigazione. I browser più recenti invece, visualizzano un messaggio di warning che copre l'intera finestra, mostrando per bene all'utente le informazioni di sicurezza del sito visitato sulla barra degli indirizzi del browser. Nei browser moderni la validazione estesa dei certificati mostra la barra degli indirizzi con un colore verde. Inoltre, la maggior parte dei browser visualizza un messaggio di warning all'utente quando esso sta visitando un sito che contiene un misto di contenuti criptati e non criptati.

La sicurezza di HTTPS è garantita dal protocollo TLS sottostante, che in pratica utilizza chiavi private e pubbliche a lungo termine per generare chiavi di sessione a breve termine. Queste chiavi sono utilizzate successivamente per cifrare il flusso dei dati scambiati tra client e server. I certificati definiti dallo standard X.509 sono utilizzati per autenticare il server (a volte anche il client). Di conseguenza, le autorità certificative e i certificati a chiave pubblica sono necessari al fine di verificare il rapporto che sussiste tra il certificato e il suo proprietario, oltre a generare la firma e gestire la validità dei certificati.

3.1.3. MQTT

MQTT (MQ Telemetry Transport) è un protocollo di rete leggero, publish-subscribe, machine to machine. È progettato per le connessioni con sedi remote che dispongono di dispositivi con vincoli di risorse o larghezza di banda di rete limitata. Deve essere eseguito su un protocollo di trasporto che fornisca connessioni ordinate, senza perdita di dati e bidirezionali, in genere TCP/IP. È uno standard OASIS aperto e una raccomandazione ISO (ISO/IEC 20922).

Il protocollo MQTT definisce due tipi di entità di rete: un broker di messaggi e un numero di client. Un broker MQTT è un server che riceve tutti i messaggi dai client e quindi instrada i messaggi ai client di destinazione appropriati. Un client MQTT è qualsiasi dispositivo (da un microcontrollore fino a un server a tutti gli effetti) che esegue una libreria MQTT e si connette a un broker MQTT su una rete.

Il broker MQTT è un software in esecuzione su un computer (in esecuzione in locale o nel cloud) e potrebbe essere autocostruito o ospitato da una terza parte. Il broker funge da ufficio postale. I client MQTT non utilizzano un indirizzo di connessione diretta del destinatario previsto, ma utilizzano la riga dell'oggetto denominata topic. Chiunque si iscriva riceve una copia di tutti i messaggi relativi a quell'argomento. Più client possono sottoscrivere un topic da un singolo broker (funzionalità uno a molti) e un singolo client può registrare abbonamenti ad argomenti con più broker (molti a uno).

Ogni cliente può sia produrre che ricevere dati sia pubblicando che iscrivendosi, ovvero i dispositivi possono pubblicare i dati dei sensori ed essere comunque in grado di ricevere le informazioni di configurazione o i comandi di controllo (MQTT è un protocollo di comunicazione bidirezionale). Questo aiuta sia nella condivisione dei dati, nella gestione e nel controllo dei dispositivi. Un client non può trasmettere gli stessi dati a una serie di topic e deve pubblicare più messaggi al broker, ognuno con un singolo argomento fornito. [9]

Con l'architettura del broker MQTT, i dispositivi client e l'applicazione server vengono disaccoppiati. In questo modo, i client vengono tenuti all'oscuro delle reciproche informazioni. MQTT utilizza la crittografia TLS con connessioni protette da nome utente e password. Facoltativamente, la connessione può richiedere la certificazione, sotto forma di un file di certificato fornito da un client e che deve corrispondere alla copia del server.

I principali vantaggi del broker MQTT sono:

1. Elimina le connessioni client vulnerabili e non sicure
2. Può facilmente scalare da un singolo dispositivo a migliaia
3. Gestisce e tiene traccia di tutti gli stati di connessione client, incluse le credenziali di sicurezza e i certificati

4. Riduzione dello sforzo di rete senza compromettere la sicurezza (rete cellulare o satellitare)

Se un broker riceve un messaggio su un topic per il quale non esistono sottoscrittori correnti, il broker elimina il messaggio a meno che l'autore del messaggio non abbia designato il messaggio come messaggio da mantenere. Un messaggio mantenuto è un normale messaggio MQTT con il "Retained flag" impostato a 1. Il broker memorizza l'ultimo messaggio conservato e il QoS corrispondente per l'argomento selezionato. Ogni client che sottoscrive un topic che corrisponde al topic del messaggio conservato riceve il messaggio mantenuto immediatamente dopo la sottoscrizione. Da notare però che il broker memorizza un solo messaggio conservato per topic. Ciò consente ai nuovi abbonati a un argomento di ricevere il valore più recente anziché attendere il prossimo aggiornamento da un publisher.

Quando un client si connette per la prima volta al broker, può impostare un messaggio predefinito da inviare ai sottoscrittori se il broker rileva che il client si è disconnesso inaspettatamente dal broker (Will message).

I client interagiscono solo con un broker, ma un sistema può contenere diversi server broker che scambiano dati in base agli argomenti dei loro attuali abbonati.

MQTT si basa sul protocollo TCP per la trasmissione dei dati. Una variante, MQTT-SN, viene utilizzata su altri trasporti come UDP o Bluetooth.

MQTT invia le credenziali di connessione in formato testo normale e non include alcuna misura per la sicurezza o l'autenticazione. Questo può essere fornito utilizzando TLS per crittografare e proteggere le informazioni trasferite da intercettazione, modifica o falsificazione (MQTTS). La porta MQTT non crittografata predefinita è 1883. La porta crittografata è 8883.

Il cosiddetto Quality of Service (QoS) è tra le funzionalità più importanti del protocollo MQTT. *La qualità del servizio* a cui si fa riferimento è intesa come il grado di accuratezza nella consegna dei messaggi MQTT tra i publisher e il broker e il broker e i client, ovvero l'accuratezza che definisce la garanzia dell'effettiva, avvenuta consegna di tali messaggi.
Esistono tre livelli di servizio QoS:

- *Al massimo una volta* (livello 0);
- *Almeno una volta* (livello 1);
- *Esattamente una volta* (livello 2);

Il QoS MQTT riguarda sostanzialmente le due fasi della consegna di un messaggio inviato da un client mittente e riceuto da un client sottoscrittore:

- l'invio dal mittente al broker;
- l'invio dal broker a destinatario finale. [9]

Nella prima fase il mittente decide il livello di QoS associato al messaggio e lo invia al broker; nella seconda, il broker a sua volta gira tale messaggio a tutti i client che abbiano una sottoscrizione per tale messaggio utilizzando il medesimo livello QoS. Questo parametro è molto importante perché concede al mittente la possibilità di scegliere il livello di servizio in base alla qualità della rete e alla logica applicativa. Più precisamente le caratteristiche associate a ciascun livello sono le seguenti:

- QoS 0 (At most one, Al massimo uno). Il livello minimo per è zero. Si tratta di un livello concepito per le massime prestazioni col minor sforzo: in questo scenario non c'è alcuna garanzia di consegna. Il mittente invia al broker *e* non attende alcuna risposta né provvede a un eventuale re-invio;
- QoS (At least one = Almeno uno) 1. In questo scenario il mittente (che sia quello che invia l'iniziale messaggio al broker, o esso sia il broker stesso che gira un messaggio al ricevente finale) mantiene in memoria il messaggio finché non riceve dal destinatario la conferma di avvenuta ricezione. In caso non lo riceva entro un tempo congruo, lo invia nuovamente, una seconda volta, e attende nuovamente risposta, e così via. Usando QoS 1 potrebbero dunque verificarsi consegne molteplici del medesimo messaggio. Quando infatti il broker riceve un messaggio marchiato con QoS 1 provvede subito a girarlo ai sottoscrittori di tale messaggio e poi risponde al mittente; se il tempo tra l'invio e la ricezione del pacchetto di conferma è troppo lunga (per esempio in reti congestionate), il

mittente invia nuovamente il messaggio, scatenando nuovamente tutta la catena e causando un invio duplicato;

- QoS 2 (Exactly one = Esattamente uno). Questa è la modalità più lenta ma anche più affidabile: in sostanza il processo prevede un doppio rimbalzo tra mittente e destinatario al fine di confermare al mittente l'effettiva presa in carico del messaggio e quindi l'annullamento di un eventuale re-invio. Questo garantisce che il messaggio arrivi esattamente una e una sola volta, ma ovviamente è più oneroso (minimamente) per i sistemi, per la rete e per i timing. [9]

Non è possibile stabilire quale sia il migliore a priori ma dipende dallo scenario di applicazione del protocollo MQTT, il quale è concepito sì per comunicazioni leggere e rapide, ma la sua configurazione in termini di QoS va calibrata con attenzione in base all'ambito di utilizzo. Nel caso in esame di questa tesi verrà utilizzato un QoS = 1 in quanto non critici.

3.1.3.1. MQTTS: descrizione topic utilizzati

I topic utilizzati sono i seguenti, organizzati in due gruppi: il primo gruppo, a sinistra, sono i topic su cui il Backend pubblica ed il dispositivo è client, il secondo gruppo, a destra, è invece l'opposto dato che il dispositivo pubblica ed il Backend è client. All'interno del Backend risiede il Services, codice che esegue tutte le operazioni associate alla pubblicazione di messaggi sui vari topic disponibili. [10]

Backend publish / Device Subscribe

- v1/device/CUID/connected;
- v1/device/ CUID /time;
- v1/device/ CUID /sync;
- v1/device/ CUID /op/configuration;
- v1/device/ CUID /op/mode;
- v1/device/ CUID /op/reset;
- v1/device/CUID/op/update.

Backend subscribe / Device publish

- v1/devices/CUID/connect;
- v1/devices/CUID/disconnect (will message);
- v1/devices/CUID/status;
- v1/devices/CUID/ping;
- v1/devices/CUID/ack.

Per un maggiore dettaglio verranno ora analizzati singolarmente i vari topic. Per la categoria Backend publish / Device Subscribe sono:

v1/device/CUID/connected (Tabella 1)

Il messaggio *connected* è pubblicato dal Backend in risposta al messaggio *connect* per notificare il dispositivo della connessione completata con successo. Il payload è vuoto. Solo dopo la ricezione di questo messaggio il prodotto inizierà ad operare con il cloud. Oltre a questo suo primario obiettivo dopo il messaggio *connected* il server utilizza subito altri topic: *time, sync, configuration*.

Topic	Qos	Backend	Device
v1/device/CUID/connected	1	Publish	Subscribe

Tabella 1- Topic "connected"

[Payload vuoto]

v1/device/CUID/time (Tabella 2)

Il messaggio time è pubblicato dal backend e sottoscritto dal device per ricevere il timestamp di sincronizzazione RTC dal server. Il messaggio time è ricevuto in seguito alla pubblicazione (periodica) del messaggio ping da parte del dispositivo.

Topic	**Qos**	**Backend**	**Device**
v1/device/CUID/time	1	Publish	Subscribe

Campo	**Lunghezza**	**Descrizione**
timestamp	4	Intero, Data e ora GMT
checksum	1	checksum

Tabella 2- Topic "time"

v1/device/CUID/sync (Tabella 3)

Il messaggio sync è pubblicato dal Backend e sottoscritto dal dispositivo per richiedere lo stato completo del device. Il payload è vuoto. Dopo la ricezione di questo messaggio il dispositivo deve inoltrare un messaggio status integrale (tutti i campi devono essere presenti, altrimenti in genere il messaggio status contiene il valore dei soli parametri che sono cambiati rispetto all'ultima trasmissione).

Topic	**Qos**	**Backend**	**Device**
v1/device/CUID/sync	1	Publish	Subscribe

Tabella 3- Topic "sync"

[Payload vuoto]

v1/device/CUID/op/configuration

Il topic è sottoscritto solo dai dispositivi che supportano la Device Configuration, ovvero la possibilità di impostare dei parametri ambientali con il fine di definire il comportamento del dispositivo, ovvero di configurarlo.
Il messaggio configuration è pubblicato dal Backend e sottoscritto dal dispositivo per essere notificato della modifica della configurazione generata da un'operazione richiesta dalla App attraverso la REST API. Questa operazione viene svolta al termine dell'associazione tra dispositivo e App.

La cappa non è un dispositivo configurabile, di conseguenza, non utilizza questo topic.

V1/device/CUID/op/mode (Tabella 4)

Il messaggio mode è pubblicato dal Backend e sottoscritto dal dispositivo per essere notificato del cambiamento alla modalità operativa di funzionamento generato da un'operazione richiesta dalla App attraverso la REST API.

Topic	Qos	Backend	Device
v1/device/CUID/op/mode	1	Publish	Subscribe

Campo	Lunghezza	Descrizione
operationId	4	Intero
timeout	4	Intero, secondi GMT
payload dinamico		Sequenza chiave-valore: • la chiave ha dimensione 2 byte; • il valore ha dimensione 2 byte se la corrispondente chiave è > 255, altrimenti 1 byte.
checksum	1	checksum

Tabella 4- Topic "mode"

Il campo *operationId* è l'identificativa operazione generato dal server per la correlazione dell'operazione con il messaggio ack (si veda in seguito). Il campo timeout informa il dispositivo se la nuova modalità operativa è da protrarsi indefinitamente (0) o a scadenza. Questa feature è utilizzata nel caso in cui il mode da impostare è scaturito dallo scheduling della programmazione del device. Per ragioni di "sicurezza", infatti, un dispositivo programmato potrebbe perdere la connessione e dunque il device deve prevedere una modalità di default "sicura" nel caso in cui il successivo comando schedulato non dovesse arrivare.

v1/device/CUID/op/reset

Inizialmente introdotto per permettere di effettuare il reset anche da remoto nell'applicazione finale si è deciso di non utilizzare questa features. L'unico modo di effettuare il reset è quello di interagire direttamente con l'User Interface sulla cappa.

v1/device/CUID/op/update (Tabella 5)

Il messaggio update è pubblicato dal Backend e sottoscritto dal device per essere notificato di una nuova versione del firmware disponibile. Il dispositivo deve avviare l'update.

Topic	Qos	Backend	Device
v1/device/CUID/op/update	1	Publish	Subscribe

Campo	Lunghezza	Descrizione
operationId	4	Intero
moduleCount	1	Intero, numero dei moduli da aggiornare
moduleId	1	Intero
moduleVersion	2	Intero
moduleSize	4	Intero
moduleCRC	4	Intero
moduleURL	64	Caratteri con codifica UTF-8 e terminato con un carattere nullo
checksum	1	checksum

Tabella 5- Topic "update"

Il campo *operationId* è l'identificativa operazione generato dal server per la correlazione dell'operazione con il messaggio ack (si veda in seguito).

Il pacchetto permette di specificare multiple versioni firmware da aggiornare nel caso di device costituito da più moduli (hardware) aggiornabili.

moduleCount è il numero di moduli firmware da aggiornare sul device. I successivi campi *moduleId…moduleURL* (in grigio in tabella) saranno ripetuti n volte con n=*moduleCount*.
- *moduleId* è l'identificativo numerico del modulo;
- *moduleVersion* è la versione firmware a cui aggiornare il modulo moduleId;
- *moduleSize* è la dimensione in bytes del download;
- *moduleCRC* è il codice CRC da verificare dopo il download;
- *moduleURL* è la URL di download.

L'endpoint di download del firmware supporta il trasferimento per range di bytes (chunks).

I topic del gruppo Backend subscribe / Device publish sono invece:

v1/devices/CUID/connect (Tabella 6)

Il messaggio connect è pubblicato dal dispositivo subito dopo l'avvenuta connessione MQTT al broker. Lo scopo del messaggio è notificare a livello applicativo la connessione al backend. Per i dispositivi, il messaggio ha inoltre lo scopo di comunicare:

- La versione firmware correntemente installata, necessaria al meccanismo di aggiornamento automatico del firmware;
- L'identificativo e la versione del protocollo di comunicazione utilizzato, necessario al cloud per l'encoding, il decoding e la validazione dei dynamic payload fragments dei messaggi.

Topic	**Qos**	**Backend**	**Device**
v1/devices/CUID/connect	1	Subscribe	Publish

Campo	**Lunghezza**	**Descrizione**
bundleId	1	Intero
moduleCount	1	Intero
moduleId(i)	1	Intero
moduleVersion(i)	2	Intero
dataModelVersion	1	Intero
checksum	1	checksum

Tabella 6- Topic "connect"

Il pacchetto permette di specificare multiple versioni di moduli nel caso di firmware costituito da più moduli (hardware).

- *bundleId* Identifica una specifica configurazione schede prodotto (per le cappe wifi = 1);
- *moduleCount* è il mumero di moduli (con firmware aggiornabile) presenti sul device. I successivi campi *moduleId* e *moduleVersion* (in grigio in tabella) saranno ripetuti n volte con n=*moduleCount*;
- *moduleId* è l'identificativo numerico del modulo;
- *moduleVersion* è la versione firmware corrente del modulo *moduleId* (*).

Il modulo "core", che esiste per definizione per ogni device IOT, è identificato con il valore 0, per cui, di norma avremo *moduleCount*=1 e *moduleId*=0; per eventuali moduli aggiuntivi si consiglia l'assegnamento di *moduleId* sequenziali (e.g. 1, 2, etc.)

- *dataModelVersion,* data model ID del Core cioè il primo byte della Ident Table del Core.

v1/devices/CUID/disconnect (will message) (Tabella 7)

È necessario un Will Message (Payload vuoto) in quanto la disconnessione deve essere notificata al Backend.

Topic	**Qos**	**Backend**	**Device**
v1/device/CUID/sync	1	Subscribe	Publish

Tabella 7- Topic "disconnect"

[Payload vuoto]

v1/devices/CUID/status (Tabella 8)

Il messaggio status è pubblicato dal dispositivo ad ogni variazione dello stato limitatamente agli attributi oggetto della variazione o, integralmente su esplicita richiesta attraverso il messaggio *sync*. Per evitare di incorrere in un'alta frequenza di pubblicazioni il dispositivo dovrebbe comunque implementare un meccanismo che limiti la frequenza con un intervallo minimo tra una pubblicazione e l'altra (e.g. 1 secondo).

Topic	**Qos**	**Backend**	**Device**
v1/devices/CUID/status	1	Subscribe	Publish

Campo	**Lunghezza**	**Descrizione**
timestamp	4	Intero, GMT
wifiLevel	1	Intero
pingTime	2	Intero
Payload dinamico		Sequenza chiave-valore: • la chiave ha dimensione 2 byte; • il valore ha dimensione 2 byte se la corrispondente chiave è > 255, altrimenti 1 byte.
checksum	1	checksum

Tabella 8- Topic "status"

- wifiLevel, livello del segnale Wi-Fi ricevuto dal modulo presente sulla cappa;

- pingTime, il tempo medio di risposta del server.

v1/devices/CUID/ping (Tabella 9)

Il messaggio *ping* è pubblicato dal dispositivo ad intervalli regolari. Lo scopo del messaggio di ping è:

1. Fungere da keep-alive a livello applicativo;

2. Attivare eventulalmente il messaggio time inviato dal Backend al dispositivo per sincronizzare il real time clock (RTC) del device. È alla ricezione di questo messaggio che il device calcola e aggiorna il pingTime ovvero il tempo medio di risposta del server;
3. Attivare eventulalmente il messaggio mode inviato dal Backend al device per impostare la modalità operativa in seguito allo scheduling della programmazione del device;
4. Attivare eventualmente il messaggio update inviato dal Backend al device per avviare una procedura di aggiornamento del firmware. Il firmware attualmente in uso dal dispositivo, comunicato nel messaggio connect, è comparato con la versione corrente rilevata dal Backend e, solo in caso di versione differente (upgrade), verrà attivato un update. L'invio del messaggio update ha precedenza ed esclude l'invio dei messaggi time e mode.

Dunque, al messaggio ping potranno seguire:

- Il solo messaggio time;
- Il solo messaggio mode;
- Il messaggio time seguito dal messaggio mode;
- il solo messaggio update;
- Nessun messaggio.

Topic	**Qos**	**Backend**	**Device**
v1/devices/CUID/ping	1	Subscribe	Publish

Tabella 9- Topic "ping"

[Payload vuoto

v1/devices/CUID/ack (Tabella 10)

Il messaggio *ack* rappresenta un acknowledge a livello applicativo ed è pubblicato originalmente dal dispositivo in risposta ad ognuna delle quattro operazioni di controllo remoto (da Cloud) del device (e.g. *op/configuration, op/mode, op/reset, op/update*). Se il controllo è attivato da interfaccia fisica del device il messaggio ack NON è inviato: il Backend sarà notificato attraverso altri messaggi (e.g. status, disconncted).

Topic	**Qos**	**Backend**	**Device**
v1/devices/CUID/ack	1	Subscribe	Publish

Campo	**Lunghezza**	**Descrizione**
operationId	4	Intero
operationType		Intero, possibili valori: • 0 configuration; • 1 mode; • 2 reset; • 3 update.
ackCode		Intero, possibili codici: • 0 Succes; • 1 Critical Error; • 2 Retryable Error.
errorCode		Intero, la codifica degli errori è libera (non definita da standard) e viene utilizzata per le operazioni di debug
checksum		checksum

Tabella 10- Topic "ack"

operationId deve avere lo stesso valore inviato al client attraverso il messaggio di controllo remoto (e.g. /op/#) e serve per correlare operazione richiesta ed esito.

L'obiettivo del messaggio *ack* è comunicare con la massima affidabilità attuabile (reliability) l'esito dell'operazione (completata con successo o no) e dunque il dispositivo deve "ritardare" il suo invio in relazione con il tipo di operazione richiesta (*operationType*). Nello specifico:

- configuration. Dopo aver effettivamente salvato la configurazione in memoria locale;
- mode. Dopo aver effettivamente commutato la modalità operativa;
- reset. Dopo aver effettivamente effettuato il reset, comunque prima di un eventuale reboot (nel caso di hard reset);
- update. Dopo aver completato i download, il controllo del CRC, il salvataggio dei dati e qualsiasi altra operazione interna, comunque prima del reboot.

ackCode ha valore 0 per l'esito positivo, 1 e 2 per l'esito negativo. A seconda del tipo di errore avremo:

- Critical Error. Un Critical Error è un errore irreversibile che decreta l'operazione fallita;
- Retryable Error. Un Retryable Error è un errore probabilmente reversibile in un futuro prossimo. In caso di errori di questo tipo, il client (inteso come user, e.g. la App) potrebbe implementare una politica di retry entro un numero massimo di tentativi.

errorCode è un codice numerico liberamente utilizzabile dal dispositivo a scopo di debug. Per convenzione è posto a zero in caso di successo dell'operazione. L'esito di un'operazione è dunque generalizzato: non definisce *ackCode* specifici e si limita a 0 (success) e 1-2 (error). È a cura del dispositivo specificare un eventuale *errorCode* pertinente. Quest'ultimo potrebbe comunque essere utile a livello di App se si volessero presentare all'utente informazioni dettagliate riguardanti l'esito negativo.

Ack e *status* sono messaggi indipendenti. Se l'operazione dovesse comportare una modifica dello stato del dispositivo (e.g. /op/configuration e op/mode), il device stesso comunicherà la variazione attraverso il messaggio status. Per convenzione è considerato opportuno l'invio dello status prima *dell'ack*. [10]

3.2. Presentazione dell'attuale architettura di rete

Con il fine di fornire una breve panoramica iniziale, l'architettura implementata è la seguente (Figura 32): in alto a sinistra sono rappresentate le App installate sugli smartphone degli utenti mentre in alto a destra i dispositivi dotati di connettività venduti. Subito sotto è rappresentato il Cloud, che funge da intermediario tra App/Device e Backend/Broker MQTT (VerneMQ), presenti entrambi sulla stessa macchina. Infine, in basso, una terza macchina che contiene il Database MySQL. I servizi sono eseguiti su AWS. [10]

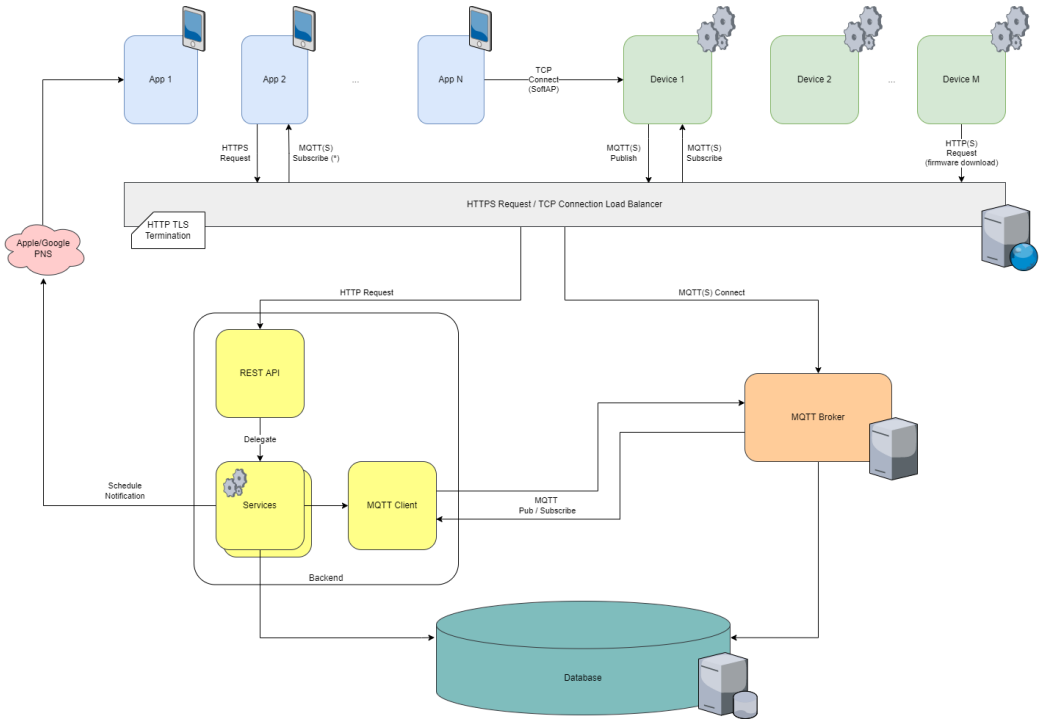


Figura 32 - Architettura di rete

3.2.1. Descrizione On-Boarding cappa su App Elica Connect

Analizzando lo schema dall'alto verso il basso per prima cosa si incontra l'On-Boarding della cappa, ovvero la registrazione del prodotto all'interno dell'App Elica Connect.

L'applicazione è scaricabile dai principali store Google Play o Apple Store gratuitamente e, una volta installata, è sufficiente registrarsi ed effettuare il log-in per poter iniziare ad utilizzare tutte le funzionalità messe a disposizione. Naturalmente, come anticipato, è prima necessario registrare il prodotto e solo a quel punto sarà possibile monitorarlo e comandarlo da remoto.

Per fare ciò l'utente seguendo una procedura guidata nell'applicazione indica l'elettrodomestico in suo possesso e viene portato ad una schermata in cui è richiesto di scansionare il QR code di configurazione presente sulla cappa. Scansionando il codice l'App entra in possesso del CUID (Connectivity Unique ID, 12 caratteri alfanumerici maiuscoli) e del MAC della cappa. Questi due valori sono memorizzati all'interno della Flash del modulo Wi-Fi installato nell'elettrodomestico. A questo punto, come indicato nell'App, è necessario interagire con la cappa per accendere il modulo Wi-Fi attraverso l'apposito pulsante; tramite questa azione la cappa entra in modalità softAP (ovvero si utilizza un software per creare una rete Wi-Fi alla quale un utente

può connettersi per trasferire dati) ed espone una rete protetta con autenticazione WPA2 con SSID "ELICA_CUIDH" (con CUIDH vengono intesi i primi quattro caratteri del CUID, con CUIDL si intendono invece gli ultimi 8 caratteri) e password "CUIDL". Avendo scansionato in precedenza il QR code l'applicazione è a conoscenza del CUID, e riconosce quindi la presenza della rete Wi-Fi attivata dalla cappa e di conseguenza riesce a connettersi ad essa.

Volendo fare un passo indietro per quanto riguarda il modulo Wi-Fi e la sua capacità di esporre una rete con un certo SSID e password, è necessario descrivere il firmware presente sul modulo stesso. Il core Wi-Fi può essere visto come una macchina a stati (Figura 33), ed il passaggio da uno stato all'altro varia il comportamento che questo ha e l'interazione che l'operatore o l'utente può avere con esso. Si parte dallo "stato 0", ovvero il modulo Wi-Fi appena prodotto e senza nessun dato memorizzato. Il produttore a questo punto lo porta allo "stato 1" andando a memorizzare nella flash il firmware da eseguire. A questo punto il modulo apre un SoftAP, ovvero un Access Point attivato da un software, e connettendosi a questa rete è possibile scrivere nella memoria del modulo l'username (CUID) e password con cui esso potrà poi accedere al broker MQTT. Fatta questa operazione viene stampata l'etichetta di configurazione che verrà sia utilizzata in stabilimento ma anche a casa dall'utente che vuole collegare la cappa all'App. Il core Wi-Fi si trova ora nello "stato 2". Durante la produzione della cappa avviene il passaggio allo "stato 3": trovandosi nello "stato 2" quando alimentato il modulo espone una rete (sempre protetta con WPA2) con SSID "ELICA_TEST" e password prestabilita quindi l'operatore con un'apposita App è in grado di eseguire il collaudo e caricare nel Database il CUID della cappa, garantendogli quindi la possibilità di essere inserita nella lista delle cappe collaudate e cioè abilitate alla connessione al broker MQTT. Senza questo passaggio la cappa non sarà in grado di accedere al broker e quindi non potrà essere controllata da remoto. Il collaudo permette al modulo di passare allo "stato 3", stato che permette alla cappa di interagire correttamente con l'App Elica Connect.

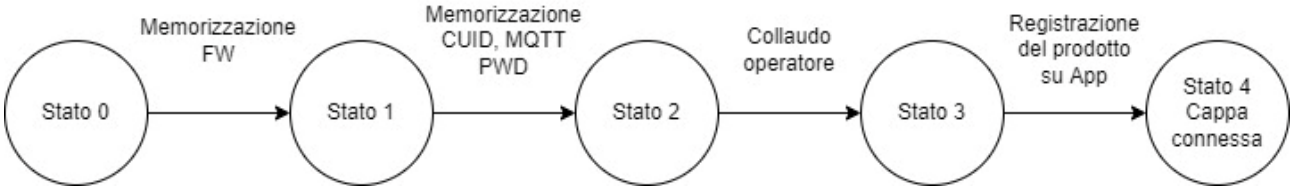


Figura 33 - Macchina a stati modulo Wi-Fi

Tornando al processo di registrazione sull'App, stabilita la connessione tra smartphone ed Access Point (AP) viene aperto un canale TCP utilizzato per comunicare attraverso il protocollo HTTP. Non c'è TLS, quindi su questa comunicazione non c'è cifratura. A questo punto inizia uno scambio di messaggi con il fine di permettere alla cappa di connettersi alla rete Wi-Fi presente in casa. Più nel dettaglio i messaggi scambiati sono i seguenti: l'App richiede le informazioni del dispositivo tramite il metodo GET (*GET /device info)* e riceve una risposta con il metodo POST (*POST /appliance parameters*) che fornisce in risposta un JSON contenente tutte le informazioni utili della cappa all'App come ad esempio CUID, MAC, PRF, Numero Seriale, WIFI STATUS (in questo momento SoftAP, ma può variare) Regione (EU o US, i due mercati di Elica) ed eventuali errori rilevati (Figura 34). A questo punto inizia lo scambio di messaggi che permetterà poi al modulo Wi-Fi e quindi alla cappa di connettersi ad internet. [11]

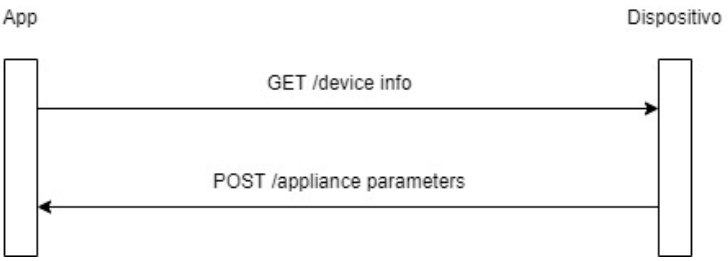


Figura 34 - Comunicazione App-Dispositivo

Tramite il primo GET (*GET /ssid list*) l'App va a richiedere quelle che sono le reti Wi-Fi rilevate dal modulo con i relativi SSID e RSSI. In questo modo sull'applicazione vengono riportate tutte le reti a cui la cappa può connettersi ed un simbolo per la rappresentazione dell'intensità del segnale. L'utente a questo punto seleziona la rete a cui far connettere il dispositivo e digita la password. Con la pressione del bottone "Invia" presente sullo schermo viene fatta una POST (*POST /ntwk parameters*); questo metodo permette di trasmettere alla cappa la password appena inserita e l'SSID selezionato. Ricevuti questi dati il modulo può connettersi al router. Una volta connesso ad internet il dispositivo si connette al cloud e si autentica al Broker MQTT. Durante questo processo l'App può richiedere più volte lo stato del dispositivo (*GET /device info)* così da poter aggiornare di volta in volta la schermata visualizzata: "Connessione alla rete Wi-Fi in corso", "Connesso alla rete Wi-Fi", "Connessione al cloud in corso" o "Dispositivo connesso" (Figura 35). Segue un'ultima fase in cui l'utente può dare un nickname al proprio elettrodomestico e termina la procedura di registrazione. È ora possibile trovare la cappa nella sezione "I miei prodotti", pagina a cui si accede per monitorare o controllare da remoto i dispositivi connessi. [11]

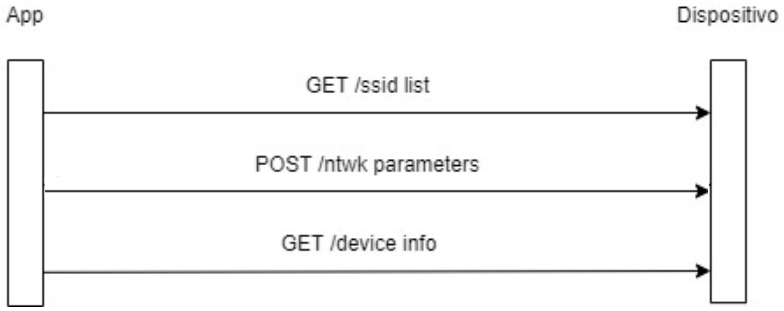


Figura 35 - Comunicazione App-Dispositivo

Una volta che il dispositivo è connesso al Cloud deve iscriversi a tutti i topic del broker MQTT necessari al suo funzionamento mentre nel frattempo l'App si scollega dalla rete della cappa ed interagisce autonomamente sul Cloud. Come descritto nei paragrafi precedenti l'apparato ha una lista di argomenti a cui registrarsi. Utilizzando un programma come Wireshark è possibile riuscire ad intercettare i pacchetti MQTT trasmessi, riuscendo quindi a visualizzare tutte le iscrizioni che il prodotto connesso effettua. Una schermata del software è riportata qui di seguito. Ai fini della comprensione della tabella l'IP della cappa è il 192.168.137.70 mentre l'IP del Cloud/Backend, dove risiede il broker MQTT, è 3.66.58.207 Figura 36). Per ottenere le informazioni in chiaro è stato momentaneamente disabilitato sia il TLS che l'MQTTS così da avere una trasmissione in chiaro ed intercettabile.

No.	Time	Source	Destination	Protocol	Length	Info
1432	2022-07-25 09:40:05,572817	192.168.137.70	3.66.58.207	MQTT	149	Connect Command
1434	2022-07-25 09:40:05,643057	3.66.58.207	192.168.137.70	MQTT	58	Connect Ack
1465	2022-07-25 09:40:07,253312	192.168.137.70	3.66.58.207	MQTT	93	Subscribe Request (id=2) [v1/device/OH1KXKYTEOEE/connected]
1468	2022-07-25 09:40:07,309422	3.66.58.207	192.168.137.70	MQTT	59	Subscribe Ack (id=2)
1472	2022-07-25 09:40:08,574910	192.168.137.70	3.66.58.207	MQTT	88	Subscribe Request (id=3) [v1/device/OH1KXKYTEOEE/sync]
1473	2022-07-25 09:40:08,628788	3.66.58.207	192.168.137.70	MQTT	59	Subscribe Ack (id=3)
1476	2022-07-25 09:40:09,503334	192.168.137.70	3.66.58.207	MQTT	88	Subscribe Request (id=4) [v1/device/OH1KXKYTEOEE/time]
1477	2022-07-25 09:40:09,637745	3.66.58.207	192.168.137.70	MQTT	59	Subscribe Ack (id=4)
1479	2022-07-25 09:40:10,479381	192.168.137.70	3.66.58.207	MQTT	100	Subscribe Request (id=5) [v1/device/OH1KXKYTEOEE/op/configuration]
1480	2022-07-25 09:40:10,527572	3.66.58.207	192.168.137.70	MQTT	59	Subscribe Ack (id=5)
1484	2022-07-25 09:40:11,510341	192.168.137.70	3.66.58.207	MQTT	91	Subscribe Request (id=6) [v1/device/OH1KXKYTEOEE/op/mode]
1485	2022-07-25 09:40:11,758008	3.66.58.207	192.168.137.70	MQTT	59	Subscribe Ack (id=6)
1487	2022-07-25 09:40:12,658253	192.168.137.70	3.66.58.207	MQTT	92	Subscribe Request (id=7) [v1/device/OH1KXKYTEOEE/op/reset]
1488	2022-07-25 09:40:12,789254	3.66.58.207	192.168.137.70	MQTT	59	Subscribe Ack (id=7)
1521	2022-07-25 09:40:14,874886	192.168.137.70	3.66.58.207	MQTT	93	Subscribe Request (id=8) [v1/device/OH1KXKYTEOEE/op/update]
1522	2022-07-25 09:40:14,948868	3.66.58.207	192.168.137.70	MQTT	59	Subscribe Ack (id=8)

Figura 36 - Log Wireshark

Si può notare nell'immagine come il dispositivo richieda la subscribe a tutti i topic necessari, che sono in totale sette:

- *v1/device/CUID/connected;*
- *v1/device/ CUID /sync;*

- *v1/device/ CUID /time;*
- *v1/device/ CUID /op/configuration;*
- *v1/device/ CUID /op/mode;*
- *v1/device/ CUID /op/reset;*
- *v1/device/CUID/op/update.*

Per una descrizione dettagliata dei singoli topic si rimanda al paragrafo precedente.

Terminate queste operazioni di subscribe, come descritto in precedenza, il dispositivo pubblica un messaggio sul topic *v1/device/CUID/connect* con lo scopo di notificare a livello applicativo la connessione al backend (Figura 37).

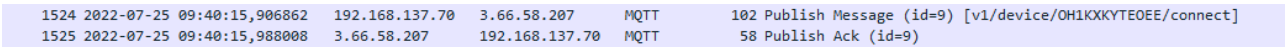


Figura 37 - Log Wireshark

Nel frattempo, prima di collegarsi alla cappa, l'App ha comunicato con il Cloud e ha condiviso i parametri ottenuti dalla scansione del QR code per far sì che quest'ultimo possa iscriversi a tutti i topic utilizzati dalla cappa. Quando la cappa si connette anch'essa al Cloud l'App si scollega dalla rete SoftAP per ricollegarsi ad una rete con accesso ad Internet (o dati mobili) così da poter interagire con il Cloud. Quando la cappa pubblica il messaggio su *v1/device/CUID/connect* il Cloud, riconoscendo che il CUID in questione è associato ad un particolare utente, fa proseguire la procedura di registrazione sull'App avanzando sulla schermata di inserimento del nickname.

3.2.2. Descrizione della comunicazione App – Cappa

Dopo una prima fase di configurazione l'utente può utilizzare l'App Elica Connect per comandare i propri dispositivi. Come anticipato nel paragrafo precedente è necessario registrarsi ed inserire delle credenziali che saranno poi usate per il log-in. Questa operazione è necessaria perché ad ogni utente, cioè ad ogni coppia di credenziali e-mail e password, viene associato un codice identificativo denominato UserID; questo sarà utilizzato nelle successive operazioni per distinguere tra loro i vari clienti.

Nel momento in cui la persona apre l'App si interfaccia al Cloud e fa una richiesta HTTPS *GET /devices* per ottenere la lista dei dispositivi posseduti dall'utente. L'identificazione di quelli effettivamente associati al particolare utente avviene proprio attraverso il ClientID descritto in precedenza, di conseguenza solo i CUID e tutte le varie info dei dispositivi memorizzate nel database associare a quel preciso ClientID saranno restituite sotto una semplice *HTTPS response*. È importante evidenziare che a differenza della comunicazione tra App e Cappa in fase di configurazione basata su HTTP ora invece è implementata sia crittografia che autenticazione grazie all'utilizzo del TLS e di certificati digitali. Sulla base dei CUID ricevuti l'App si va ad inscrivere al topic *device/CUID/statusjson,* uno per ogni dispositivo registrato. Questo topic verrà utilizzato dal Cloud per comunicare all'App eventuali variazioni legate a comandi imposti non direttamente da App ma manualmente da User Interface. In questo modo l'App sarà sempre sincronizzata ed aggiornata in Real-Time con lo stato effettivo della cappa.

Di seguito (Figura 38) è riportata una schematizzazione dei messaggi scambiati tra i vari attori che partecipano a questa prima fase di utilizzo dell'applicazione: Utente, App, Cloud e Broker MQTT.

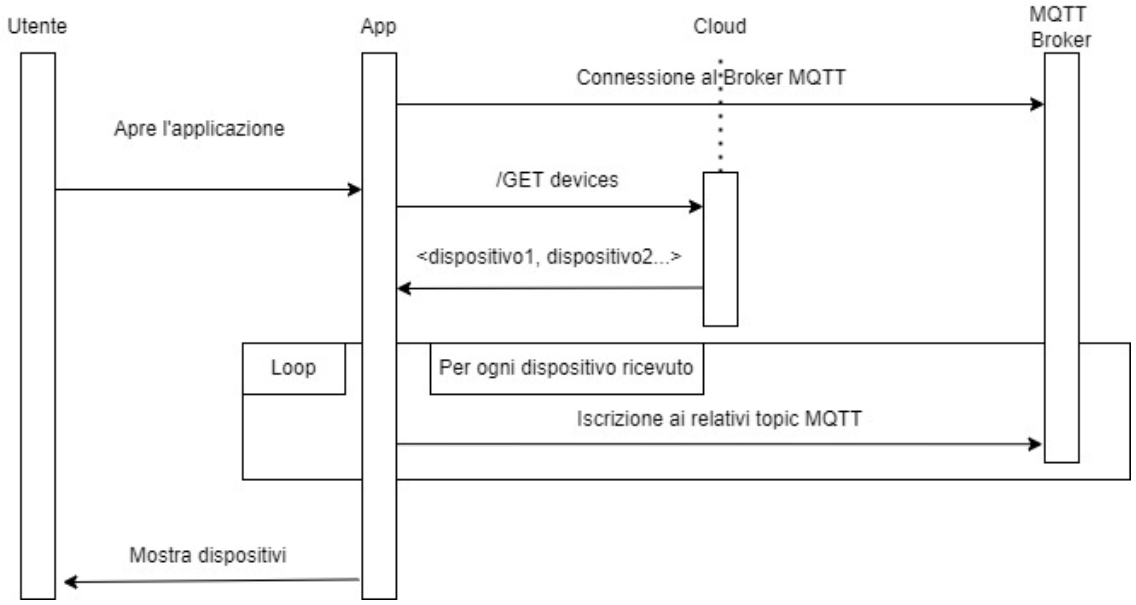


Figura 38 - Comunicazione Utente-App-Cloud

Lo scambio di messaggi precedenti permette di avere la sezione "I miei prodotti" aggiornata con tutti i dispositivi in proprio possesso. Nel momento in cui si vuole imporre un comando utilizzando l'App, ad esempio di accendere la luce, si va a generare un traffico di dati che ora verrà descritto nel dettaglio. Per prima cosa l'utente interagisce con il display e definisce il comando; questo viene inviato al Cloud utilizzando il metodo HTTPS POST */device/CUID/commands (Figura 39)* che permette di andare ad inviare dati alla risorsa, ovvero coppie chiave-valore in cui la chiave rappresenta cosa il comando va a modificare (esempio "luce cappa") mentre il valore rappresenta il comportamento che questa deve assumere (riprendendo l'esempio della "luce cappa", il valore va da 0 a 64 e rappresenta il valore dell'intensità luminosa 0% - 100%, trasmettere 0 significa quindi luce spenta, 64 significa invece intensità massima) . Segue un ACK di conferma recezione. [11]

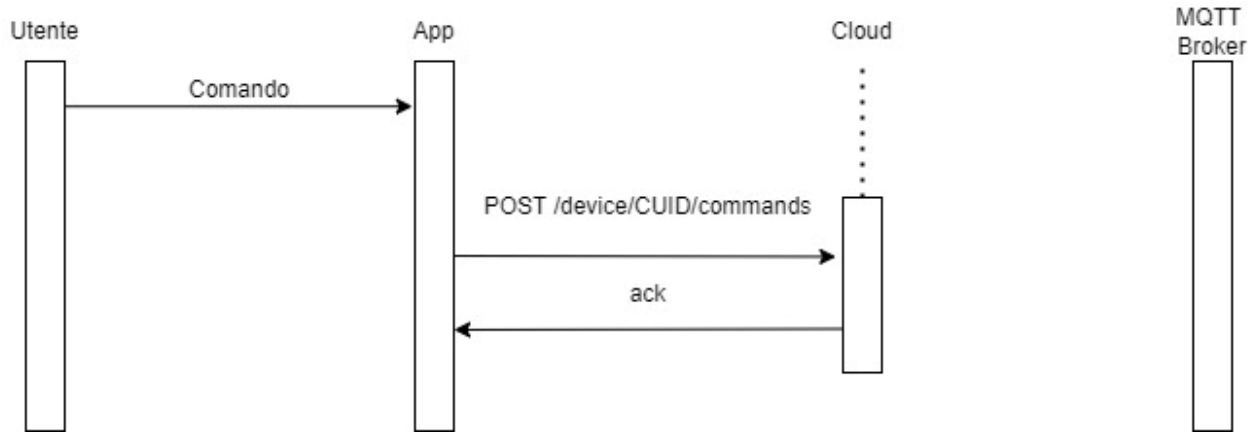


Figura 39 - Comunicazione Utente-App-Cloud

A questo punto si abbandona l'HTTPS in favore dell'utilizzo dell'MQTTS. Sulla base del metodo POST ricevuto il Backend va a pubblicare sul Broker MQTT utilizzando il topic *v1/device/CUID/op/mode* un messaggio in cui il payload dinamico conterrà la coppia chiave – valore della "luce cappa" impostata da App. Come descritto nel paragrafo precedente legato al funzionamento del protocollo MQTT il Broker inoltra il messaggio appena

ricevuto a tutti i client iscritti al topic su cui il messaggio è stato appena pubblicato; quindi, quest'ultimo viene trasmesso al dispositivo e viene ricevuto dal modulo Wi-Fi installato nel prodotto. La conferma di ricezione avviene pubblicando un messaggio con payload vuoto sul topic *v1/device/CUID/ack,* messaggio che con la stessa logica del precedente viene poi consegnato al Cloud dal Broker. Il modulo Wi-Fi presente nella cappa, sfruttando il protocollo One-Wire descritto nel capitolo precedente, trasmette alla scheda Main il comando richiesto da remoto, la scheda quindi attua la variazione e quando possibile comunica a tutti i nodi ad essa connessi le modifiche apportate. In questo caso la board va ad accendere la "luce cappa" e poi successivamente ne comunica a tutti l'accensione. Il modulo Wi-Fi a questo punto riceve l'effettiva variazione dello stato della cappa, ovvero si è passati da avere la "luca cappa" spenta ad accesa, quindi pubblica un messaggio sul topic *v1/device/CUID/status* contenente nel payload le coppie chiave – valore legate ai soli attributi che sono cambiati (Figura 40). [11]

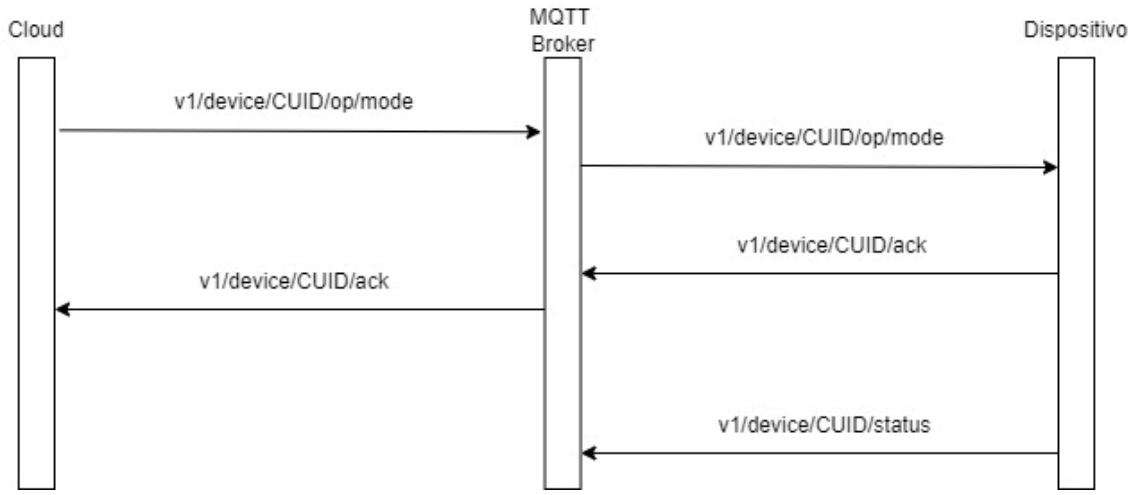


Figura 40 - Comunicazione Cloud-Dispositivo

Il Backend, essendo iscritto al topic in questione, riceve una copia del messaggio. L'operazione da esso svolta consiste semplicemente nell'andare a formattare il payload del messaggio ricevuto in formato json ed inoltrarlo all'App mediante il topic *v1/device/CUID/op/statusjson.* Il messaggio appena ricevuto viene elaborato dall'App che va ad aggiornare l'interfaccia grafica sul display, mostrando effettivamente l'icona della "luce cappa" attiva (Figura 41). [11]

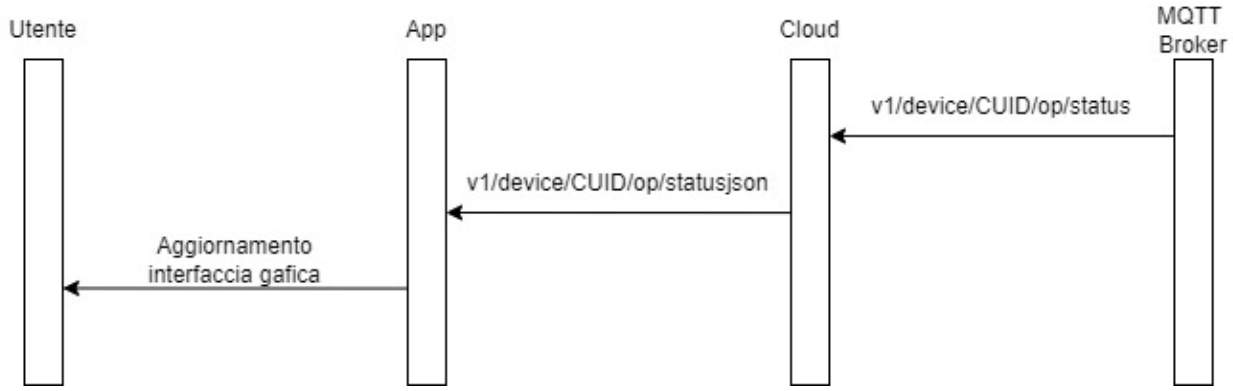


Figura 41 - Comunicazione Utente-App-Cloud

Lo scambio MQTT appena descritto può essere riportato utilizzando ancora una volta il software Wireshark. Per prima cosa, una volta ricevuto il comando dall'applicazione tramite il metodo POST, il Backend va a pubblicare sul broker la richiesta tramite il topic *v1/device/CUID/op/mode,* pubblicazione che viene poi

rigirata a tutti i dispostivi iscritti, tra cui la cappa. L'ack di avvenuta ricezione viene pubblicato dalla cappa sul corrispettivo topic (Figura 42).

```
4719 2022-07-25 09:51:50,767187   3.66.58.207      192.168.137.70   MQTT        107 Publish Message (id=31) [v1/device/OH1KXKYTEOEE/op/mode]
4724 2022-07-25 09:51:51,205029   192.168.137.70   3.66.58.207      MQTT         94 Publish Message (id=54) [v1/device/OH1KXKYTEOEE/ack]
```

Figura 42 - Log Wireshark

A questo punto la cappa ha ricevuto il comando. Questo viene elaborato ed attuato. Una volta che la scheda Main ha eseguito il comando tutte le schede ad essa collegate sono notificate della variazione avvenuta (accensione luce cappa, riprendendo l'esempio presentato nella spiegazione) tramite il protocollo One-Wire bus. Il core Wi-Fi allora, ricevuto il messaggio, pubblica sul broker MQTT la coppia chiave-valore associata alla modifica appena applicata utilizzando il topic *v1/device/CUID/status*. Il messaggio viene letto dal Cloud, iscritto al topic, e rigirato all'App Elica Connect tramite il topic v1/device/CUID/statusjason, topic a cui l'App si iscrive automaticamente ogni volta che viene avviata (Figura 43).

```
4728 2022-07-25 09:51:52,948352   192.168.137.70   3.66.58.207      MQTT        102 Publish Message (id=55) [v1/device/OH1KXKYTEOEE/status]
4729 2022-07-25 09:51:53,056381   3.66.58.207      192.168.137.70   MQTT         58 Publish Ack (id=55)
4730 2022-07-25 09:51:53,088875   3.66.58.207      192.168.137.73   MQTT        131 Publish Message (id=674) [v1/device/OH1KXKYTEOEE/statusjson]
```

Figura 43 - Log Wireshark

Durante il normale funzionamento del prodotto ci sono altri scambi di messaggi tra dispositivo e Backend, come ad esempio la pubblicazione sui topic *v1/device/CUID/ping* e *v1/device/CUID/time*, che rispettivamente forniscono da keepalive nei confronti del Cloud e la sincronizzazione con il server (Figura 44).

```
1668 2022-07-25 09:40:48,094755   192.168.137.70   3.66.58.207      MQTT         87 Publish Message (id=16) [v1/device/OH1KXKYTEOEE/ping]
1669 2022-07-25 09:40:48,228080   3.66.58.207      192.168.137.70   MQTT         58 Publish Ack (id=16)
1670 2022-07-25 09:40:48,251409   3.66.58.207      192.168.137.70   MQTT         92 Publish Message (id=7) [v1/device/OH1KXKYTEOEE/time]
1672 2022-07-25 09:40:48,401174   192.168.137.70   3.66.58.207      MQTT         58 Publish Ack (id=7)
```

Figura 44 - Log Wireshark

4. Mappatura tecnologie: studio e confronto dei protocolli di comunicazione per IoT

Nel capitolo precedente è stata descritta l'architettura di rete, quindi tutto il Backend dietro l'elettrodomestico connesso. L'utilizzo dei controlli remoti è possibile solo tramite App o l'ecosistema di Amazon Alexa, che grazie alla Skill di Elica permette di controllare i dispositivi connessi attraverso la voce. Questa interazione è possibile perché la Skill permette ad Alexa di collegarsi al Cloud e quindi sostituisce in maniera totale l'App. Si evidenzia quindi l'assenza di una integrazione con altri ecosistemi come ad esempio Google Home, assenza che mette in evidenza un proposito molto importante per Elica ma per il mondo Smart Home in generale: la necessità di avere i vari ecosistemi interoperabili tra loro, così da poter utilizzare un unico cloud in grado di interagire con tutti (Figura 45).

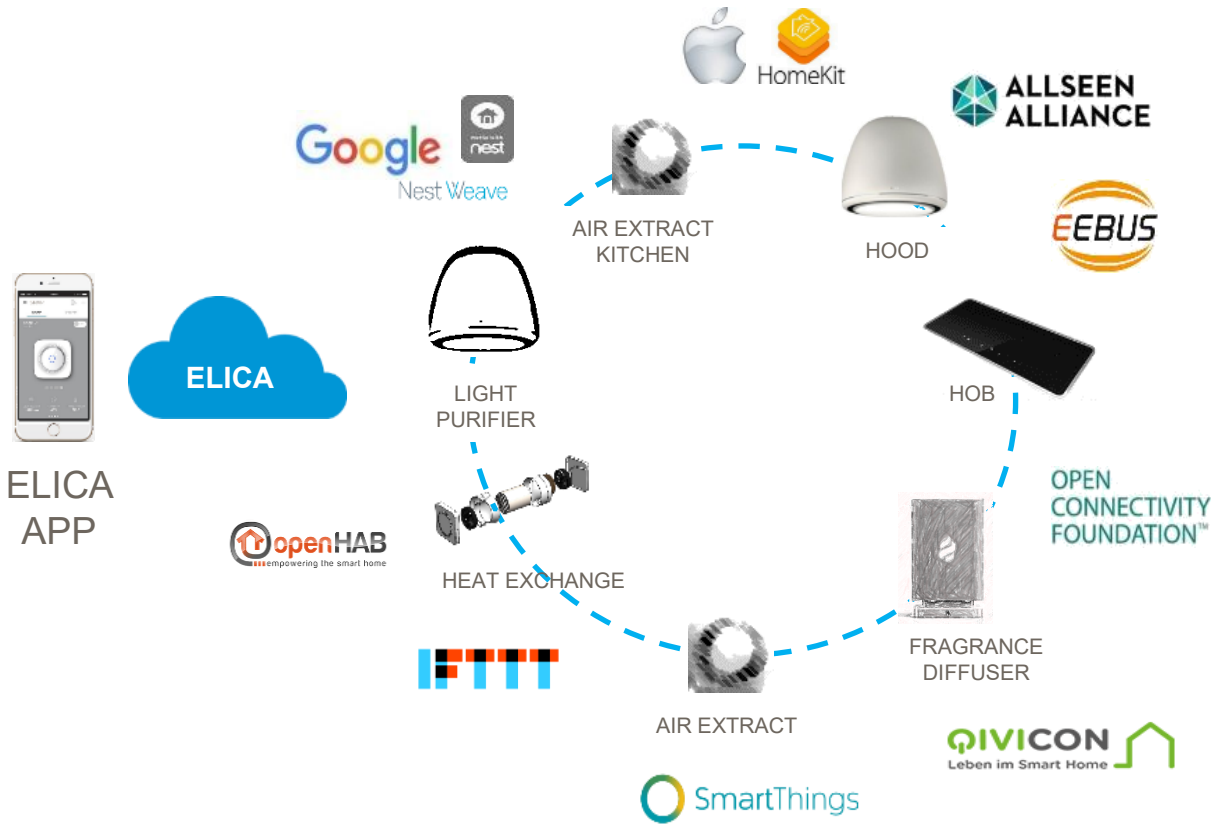


Figura 45 - Proposito Smart Home

L'architettura alla base dell'App Elica Connect risulta essere estremamente funzionale, e può essere vista come una soluzione consolidata nel caso di interazione con un elettrodomestico da remoto. L'applicazione ha quindi un ruolo fondamentale ed è di vitale importanza per quello che è l'obiettivo aziendale per i prossimi anni: creare una piattaforma hardware dotata di modulo Wi-Fi dal basso costo e general purpose così che possa essere poi implementata su tutti i prodotti, permettendo di passare da soli pochi modelli connessi a pochi modelli non connessi.

Questo obiettivo, oltre al nuovo hardware, richiede anche di andare a gestire nuove modalità di interazione con la cappa, sia dal punto di vista della comunicazione per trasmettere i comandi (si ipotizza infatti una comunicazione punto-punto cappa – telefono basata su HTTPS) ma anche per registrare la cappa nell'App.

Al momento, come descritto nel capitolo 3, il processo di On-Boarding viene realizzata utilizzando un'apposita procedura all'interno dell'App Elica Connect che permette, seguendo i passaggi a schermo, di attivare la modalità softAP della cappa, di connettersi a questa rete, di trasmette i parametri per far collegare

la cappa al Wi-Fi di casa ed infine di completare la procedura di registrazione. I vari passaggi, seppur relativamente semplici, richiedono comunque un certo numero di interazioni sia con l'App che con l'elettrodomestico in questione. Può essere utile cercare di definire una nuova procedura basata su una nuova tecnologia, più semplice ed automatica possibile, che permetta di effettuare la registrazione del prodotto sull'App senza l'intervento costante dell'utente.

La comunicazione tra due dispositivi vicini può avvenire utilizzando diversi protocolli, tra questi quelli che possono essere effettivamente presi in considerazioni sono: Wi-Fi/802.11, NFC, Bluetooth, Bluetooth Low Energy, Z-wave, Thread, LoRa e Zigbee. Tutti questi protocolli, ottimi per comunicazioni su brevi distanze e che si adattano perfettamente allo scenario domestico di riferimento, presentano però delle caratteristiche uniche e differenze che possono portare alla scelta di uno piuttosto che di un altro. L'obiettivo di questo capitolo è appunto effettuare una comparazione tra i vari protocolli, trovando i vantaggi e svantaggi delle varie soluzioni con il fine di stabilire la migliore e quindi la tecnologia che sarà poi implementata sulle cappe. È importante evidenziare che il giudizio finale terrà conto non solo delle specifiche tecnologiche e prestazioni che i protocolli sono in grado di offrire, ma un parametro molto importante sarà il costo, seguito poi dall'effettiva complessità di implementazione e di utilizzo.

4.1. Wi-Fi/802.11

Figura 46 - Logo Wi-Fi Alliance

Wi-Fi è un insieme di tecnologie per reti locali senza fili (WLAN) basato sugli standard IEEE 802.11, il quale consente a più dispositivi (per esempio personal computer, smartphone, smart TV, ecc.) di essere connessi tra loro tramite onde radio e scambiare dati. Wi-Fi è anche un marchio di Wi-Fi Alliance (Figura 46), la quale consente l'uso del termine Wi-Fi Certified ai soli prodotti che completano con successo i test di certificazione di interoperabilità.
Il segnale prodotto da un Access Point risulta essere rilevabile ad una distanza che va dai 15 ai 41 metri, in base alla potenza di trasmissione del router stesso. La differenza del Wi-Fi con le altre reti a copertura cellulare risiede nei protocolli di comunicazione, ovvero nello stack protocollare che ridefinisce i primi due livelli (fisico e di collegamento), ovvero i protocolli di strato fisico e i protocolli di accesso multiplo o condiviso al mezzo radio, cioè nella comunicazione "access point-terminali" e i protocolli di trasporto per quanto riguarda la parte cablata. In particolare, dato che la trasmissione di ciascuna stazione avviene alla stessa frequenza operativa (2,4 o 5 GHz), per evitare collisioni in ricezione si utilizza il protocollo di accesso multiplo CSMA/CA. [12]

Carrier Sense Multiple Access with Collision Avoidance (Figura 47), ovvero Accesso Multiplo tramite Rilevamento della Portante con Evitamento delle Collisioni, è un protocollo di accesso multiplo che utilizza il rilevamento della portante ma in cui i nodi tentano di evitare a priori il verificarsi di collisioni. Una volta iniziata, la trasmissione prosegue fino al termine del pacchetto. Nel momento in cui una stazione vorrebbe tentare una trasmissione, essa ascolta il canale. Se il canale risulta libero la stazione attende per un certo lasso di tempo identificato come DIFS (Distributed Inter Frame Space) trascorso il quale, se il canale continua ad essere libero, la stazione inizia la trasmissione del pacchetto. A trasmissione completata il nodo di trasmissione attende per un tempo detto SIFS (Short Inter Frame Space, di durata inferiore al DIFS) la ricezione di un ACK che conferma dell'avvenuta ricezione da parte della stazione ricevente.

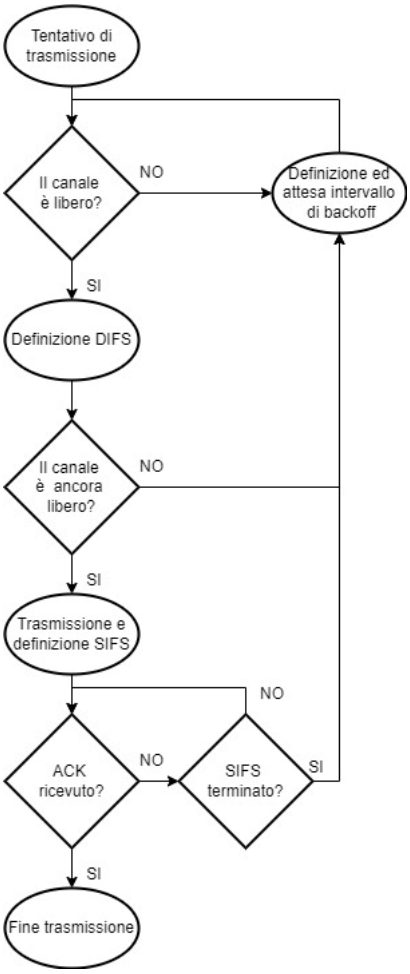


Figura 47 – Diagramma CSMA CA

Durante l'attesa dello SIFS le altre stazioni, sentendo il canale libero, definiranno il proprio DIFS e quindi non invieranno trasmissioni, evitando in tal modo collisioni (la durata del SIFS inferiore a quella del DIFS assicura che nessuna stazione inizi a trasmettere prima della ricezione dell'eventuale ACK).

Qualora, invece, la stazione trasmittente rilevi il canale occupato oppure si siano verificate delle prenotazioni da parte di altre stazioni, la stazione attende per una durata casuale (detto tempo di backoff) che il canale si liberi. Questa attesa è implementata per mezzo di un timer che viene decrementato solo durante i periodi di inattività del canale, mentre viene invece congelato (frozen backoff) durante i restanti periodi di trasmissione sul canale da parte di altre stazioni. Quando il timer raggiunge lo zero la stazione effettua un nuovo tentativo di trasmissione, ricominciando da capo. L'intervallo di tempo casuale CW di back-off estratto è limitato dalla seguente disuguaglianza:

$$0 < CW < 2^N (CW_m + 1) - 1$$

con CW (*Collision Window*) compresa tra un valore minimo ed un valore massimo ed N numero progressivo di tentativo di trasmissione. L'obiettivo di Collision Avoidance si ottiene dunque per via statistica (e non deterministica) proprio grazie all'estrazione del numero casuale compreso in questo intervallo di tempo, data la scarsa probabilità che due o più stazioni estraggano lo stesso numero di back-off, che è tanto minore quanto maggiore è l'intervallo possibile di estrazione, il quale aumenta a sua volta all'aumentare del numero N di tentativi di ritrasmissione.

In base alla potenza di trasmissione dell'Access Point questa tecnologia all'interno di un edificio può avere una portata anche fino a 20metri. I protocolli Wi-Fi consentono anche di adattare la velocità di trasmissione nella tratta wireless di accesso in funzione della distanza della stazione mobile ricetrasmittente dall'access point, minimizzando così le perdite di trasmissione.

I dispositivi wireless spesso supportano più versioni di Wi-Fi, ma per poter comunicare devono utilizzare la stessa versione. Le varie versioni differiscono tra loro per la banda radio su cui operano, la larghezza di banda radio che occupano, la velocità massima nella trasmissione dei dati che possono supportare e altri dettagli. Alcune versioni consentono l'uso di più antenne, questo permette loro di raggiungere velocità maggiori e ridurre le interferenze.

Storicamente i dispositivi differenziavano le varie versioni di Wi-Fi usando il nome dello standard IEEE supportato. Nel 2019 l'organizzazione Wi-Fi Alliance ha introdotto in via informale nuovi nomi per l'identificazione dei dispositivi certificati Wi-Fi. I dispositivi basati sullo standard 802.11ax prendono il nome di Wi-Fi 6, mentre la maggior parte dei dispositivi in vendita (al 2019) che si basano sui precedenti standard 802.11n e 802.11ac sono identificati rispettivamente come Wi-Fi 4 e Wi-Fi 5.

- Wi-Fi b, a, g;
    - b – 11 Mbit/s (2,4 GHz, IEEE 802.11b), anno 1999;
    - a – 54 Mbit/s (5 GHz,IEEE 802.11a), anno 1999;
    - g – 54 Mbit/s (2,4 GHz, IEEE 802.11g), anno 2003.
- Wi-Fi 4 o n;
    - 450 Mbit/s (2,4 GHz e 5 GHz), standard IEEE 802.11n, anno 2009.

- Wi-Fi 5 o ac;
    - 3 Gbit/s (5 GHz), standard IEEE 802.11ac, anno 2014.
- Wi-Fi 6 e 6E
    - Si basa sullo standard IEEE 802.11ax, disponibile a partire dal 2019 a cui corrisponde una banda da 2,4 GHz se certificato "Wi-Fi 6 CERTIFIED", oppure 6 GHz se con la dicitura "Wi-Fi 6E CERTIFIED". Tra le caratteristiche di questa tecnologia c'è: OFDMA (Orthogonal frequency division multiple access), la tecnologia MIMO (multiple input, multiple output) multi utente, il TWT (Target Wake Time) per il risparmio di energia delle batterie, la 1024-QAM (Modulazione di ampiezza quadratica, un canale con una capacità di 160 MHz. L'estensione 6E andrebbe a coprire lo spettro di frequenze dei 6 GHz, permettendo in teoria di gestire meglio i servizi di streaming video ad alta definizione e realtà virtuale in aree congestionate.
- Wi-Fi 7
    - Per il 2024 dovrebbe uscire la nuova tecnologia Wi-Fi 7, corrispondente allo standard IEEE 802.11be e con 30 Gbit/s di velocità. Sarà in grado di inviare dati su più frequenze contemporaneamente e avrà una tecnologia MIMO multiutente coordinata o CMU-MIMO e la 4096-QAM. [12]

Le principali caratteristiche delle varie versioni Wi-Fi sono riportate in tabella (Tabella 11).

Standard IEEE	**Velocità min - MAX**	**Frequenza**	**Anno standardizzazione**
Wi-Fi 1 (IEEE 802.11ax)	1 – 11 Mbit/s	2.4 GHZ	1999
Wi-Fi 2 (IEEE 802.11ac)	1.5 – 54 Mb/s	5 GHZ	1999
Wi-Fi 3 (IEEE 802.11n)	3 – 54 Mbit/s	2.4 GHZ	2003
Wi-Fi 4 (IEEE 802.11ag)	72 – 600 Mbit/s	2.4 / 5 GHZ	2009
Wi-Fi 5 (IEEE 802.11a)	433 – 6933 Mbit/s	5 GHZ	2014
Wi-Fi 6 (IEEE 802.11b)	600 – 9608 Mbit/s	2.4 / 5 GHZ	2019

Tabella 11 - Principali caratteristiche tecnologia Wi-Fi

Per quanto riguarda la sicurezza dello standard IEEE 802.11 nel corso degli anni è stato sviluppato e implementato un nuovo standard di sicurezza, IEEE 802.11i noto come WPA2 (Wi-Fi Protected Access 2), disponibile dal 2004 ed aggiornamento della prima versione di WPA. La transizione dai primi standard di sicurezza (WEP) al WPA2 ha portato all'introduzione di nuove tecniche di cifratura e controllo di integrità, con la conseguente necessità di richiedere hardware più performante, con una capacità di calcolo medio-alta. Sia il controllo di integrità che la cifratura vera e propria vengono realizzati utilizzando AES (Advanced Encryption Standard) rispettivamente in modalità CTR (Counter mode) e CBC (Cypher Block Chaining mode). AES è un algoritmo di cifratura simmetrica, questo significa che per cifrare e decifrare è richiesta la conoscenza di una chiave segreta che può essere scambiata in fase di autenticazione, attraverso un handshake, oppure può avvenire mediante la dimostrazione della conoscenza di un segreto precondiviso (Pre Shared Key), cosa che avviene con la connessione al router di casa: si dimostra di essere un membro affidabile tramite la conoscenza della chiave del modem. La chiave (precondivisa) sarà la base iniziale della cifratura AES con un protocollo di rinegoziazione della chiave quando la comunicazione tra i due terminale è prolungata.

4.2. NFC

Figura 48 - Logo NFC

NFC (Near Field Communication) è un insieme di tecnologie wireless a corto raggio, che in genere richiedono una separazione di 10 cm o meno (Figura 48). NFC opera a 13,56 MHz su interfaccia aerea ISO/IEC 18000-3 e a velocità comprese tra 106 kbit/s e 424 kbit/s. Esso coinvolge sempre un iniziatore e un target; l'iniziatore genera attivamente un campo RF in grado di alimentare un bersaglio passivo. Ciò consente ai target NFC di assumere forme molto semplici come tag non alimentati, adesivi, portachiavi o carte. I tag NFC contengono dati e sono in genere di sola lettura, ma possono essere scrivibili. Possono essere codificati su misura dai loro produttori o utilizzare le specifiche del forum NFC. I tag possono memorizzare in modo sicuro dati personali come informazioni sulla carta di debito e di credito, dati del programma fedeltà, PIN e contatti di rete.

Come con la tecnologia delle schede di prossimità, NFC utilizza l'accoppiamento induttivo tra due antenne ad anello vicine formando efficacemente un trasformatore a nucleo d'aria. Poiché le distanze coinvolte sono minuscole rispetto alla lunghezza d'onda della radiazione elettromagnetica di quella frequenza (circa 22 metri), l'interazione è descritta come campo vicino. Solo un campo magnetico alternato è coinvolto in modo che quasi nessuna potenza sia effettivamente irradiata sotto forma di onde radio e questo permette di evitare interferenze tra questi dispositivi e qualsiasi comunicazione radio alla stessa frequenza o con altri device NFC molto al di là della portata prevista.

Operano all'interno della banda ISM a radiofrequenza disponibile a livello globale e senza licenza di 13,56 MHz. La maggior parte dell'energia RF è concentrata nella larghezza di banda ±7 kHz allocata alla frequenza centrale, ma la larghezza spettrale dell'emissione può essere larga fino a 1,8 MHz al fine di supportare elevate velocità di trasmissione dati. [13]

La distanza di lavoro con antenne standard compatte e livelli di potenza realistici potrebbe arrivare fino a circa 20 cm (ma in pratica, le distanze di lavoro non superano mai i 10 cm).

La comunicazione avviene tra un dispositivo "iniziatore" attivo e un dispositivo di destinazione che può essere:

- Passivo. Il dispositivo iniziatore fornisce un campo portante e il dispositivo di destinazione, che funge da transponder, comunica modulando il campo incidente. In questa modalità, il dispositivo di destinazione può trarre la sua potenza operativa dal campo magnetico fornito dall'iniziatore;
- Attivo. Sia l'iniziatore che il dispositivo di destinazione comunicano generando alternativamente i propri campi. Un dispositivo smette di trasmettere per ricevere dati dall'altro. Questa modalità richiede che entrambi i dispositivi includano alimentatori.

Ogni dispositivo NFC attivo può funzionare in una o più delle tre modalità:

- Emulazione della scheda NFC. Consente ai dispositivi abilitati NFC come gli smartphone di agire come smart card, consentendo agli utenti di eseguire transazioni come il pagamento o la biglietteria;
- Lettore/scrittore NFC. Consente ai dispositivi abilitati NFC di leggere le informazioni memorizzate su tag NFC economici incorporati in etichette;
- NFC peer-to-peer. Consente a due dispositivi abilitati NFC di comunicare tra loro per scambiare informazioni in modo ad hoc. [13]

La comunicazione peer-to-peer NFC è quindi possibile, a condizione però che entrambi i dispositivi siano alimentati.

Sebbene la gamma di NFC sia limitata a pochi centimetri, l'NFC semplice standard non è protetto da eavesdropping e può essere vulnerabile alle modifiche dei dati. Le applicazioni possono utilizzare protocolli crittografici di livello superiore per stabilire un canale sicuro. Senza l'applicazione di protocolli superiori il segnale RF per il trasferimento dati wireless può essere raccolto con antenne da una distanza che dipende da più parametri, ma in genere è inferiore a 10 metri. Inoltre, le intercettazioni sono fortemente influenzate dalla modalità di comunicazione. In generale un dispositivo passivo che non genera il proprio campo RF è molto più difficile da intercettare rispetto a un dispositivo attivo; un utente malintenzionato, infatti, può in genere intercettare entro 10 m da un dispositivo attivo e 1 m da dispositivi passivi.

4.3. Z-wave

Figura 49 - Logo Z-Wave

Z-Wave (Figura 49) è un protocollo di comunicazione wireless utilizzato principalmente per l'automazione di edifici residenziali e commerciali. Si tratta di una rete mesh che utilizza onde radio a bassa energia per comunicare da un dispositivo all'altro consentendo il controllo wireless di device domestici intelligenti, come luci smart, sistemi di sicurezza, termostati, sensori e serrature. Come altri protocolli e sistemi rivolti ai mercati residenziale un sistema Z-Wave può essere controllato da uno smartphone, tablet o computer.

Z-Wave è progettato per fornire una trasmissione affidabile e a bassa latenza di piccoli pacchetti di dati a velocità di trasmissione dati fino a 100 kbit/s, ed è adatto per applicazioni di controllo e sensori, a differenza del Wi-Fi e di altri sistemi LAN wireless basati su IEEE 802.11 progettati principalmente per velocità di dati elevate. La distanza di comunicazione tra due nodi è di 200 metri all'aperto e 50 metri all'interno (entrambe le misure si riferiscono ad un percorso rettilineo, line of sight), e con la capacità di messaggio di saltare fino a quattro volte tra i nodi, offre una copertura sufficiente per la maggior parte delle case residenziali. La modulazione è la chiave di spostamento di frequenza (FSK) con codifica Manchester, e altri schemi di modulazione supportati includono GFSK e DSSS-OQPSK. [14]

Z-Wave utilizza la banda industriale, scientifica e medica (ISM) senza licenza Part 15, che opera su frequenze variabili a livello globale. Ad esempio, in Europa opera nella banda 868-869 MHz mentre in Nord America la banda varia da 908-916 MHz o 912-920 MHz, in base all'applicazione. La banda di rete mesh di Z-Wave compete con alcuni telefoni cordless e altri dispositivi elettronici di consumo, ma evita interferenze con Wi-Fi, Bluetooth e altri sistemi che operano sulla banda affollata a 2,4 GHz. Nel 2012, l'International Telecommunication Union (ITU) ha incluso i livelli Z-Wave PHY e MAC come opzione nel suo standard G.9959 per dispositivi wireless inferiori a 1 GHz. Le velocità di trasmissione dati includono 9600 bit/s e 40 kbit/s, con potenza di uscita a 1 mW o 0 dBm.

Z-Wave è stato rilasciato per essere utilizzato frequenze con le seguenti bande di frequenza in varie parti del mondo. Di seguito sono riportate le principali nazioni (Tabella 12).

Frequenza [MHz]	Paesi
865.2	India
868.4	Cina, Sud Africa
868.4, 869.85	Europa, Nord Africa
869	Russia
908.4, 916	USA
919.8, 921.4	Australia
922.5, 923.9, 926.3	Giappone

Tabella 12 - Frequenze utilizzate dallo Z-Wave nei vari paesi

La rete più semplice è un singolo dispositivo controllabile e un controller primario. I dispositivi possono comunicare tra loro utilizzando nodi intermedi per aggirare gli ostacoli domestici o i punti morti radio che potrebbero verificarsi nell'ambiente a causa del multipath.

Ulteriori dispositivi possono essere aggiunti in qualsiasi momento, così come i controller secondari, tra cui controller portatili tradizionali, controller portachiavi, controller a parete e applicazioni PC progettate per la gestione e il controllo di una rete Z-Wave. Quest'ultima può essere composta da un massimo di 232 dispositivi o fino a 4.000 nodi su una singola rete smart-home con Z-Wave LR. Entrambi consentono la possibilità di collegare le reti se sono necessari più dispositivi. [14]

Ogni rete Z-Wave è identificata da un ID di rete e ogni dispositivo è ulteriormente identificato da un ID nodo. L'ID di rete (chiamato anche Home ID) è l'identificazione comune di tutti i nodi appartenenti a una rete logica Z-Wave. L'ID di rete ha una lunghezza di 4 byte (32 bit) e viene assegnato a ciascun dispositivo, dal controller primario, quando il dispositivo è "incluso" nella rete. I nodi con ID di rete diversi non possono comunicare tra loro. L'ID nodo è l'indirizzo di un singolo nodo nella rete. L'ID nodo ha una lunghezza di 1 byte (8 bit) e deve essere univoco nella sua rete.

Z-Wave si basa su un design proprietario, supportato da Sigma Designs come principale fornitore di chip, ma la business unit Z-Wave è stata acquisita da Silicon Labs nel 2018. Nel dicembre 2019, Silicon Labs ha annunciato che avrebbe rilasciato la specifica Z-Wave come standard wireless aperto per lo sviluppo da certificare dalla Z-Wave Alliance. Il 17 novembre 2016, la Z-Wave Alliance ha annunciato standard di sicurezza più rigorosi per i dispositivi che ricevono la certificazione Z-Wave. Conosciuto come Security 2 (o S2), fornisce sicurezza avanzata per dispositivi domestici intelligenti, gateway e hub. Rafforza gli standard di crittografia per le trasmissioni tra nodi e impone nuove procedure di accoppiamento per ciascun dispositivo, con codici PIN o QR univoci su ciascun device. Il nuovo livello di autenticazione ha lo scopo di impedire agli hacker di assumere il controllo di dispositivi non protetti o scarsamente protetti.

Secondo la Z-Wave Alliance, il nuovo standard è la sicurezza più avanzata disponibile sul mercato per dispositivi domestici intelligenti e controller, gateway e hub. Il chip della serie 800, rilasciato alla fine del 2021, continua a supportare le funzionalità di sicurezza S2 standard, nonché la tecnologia Silicon Labs Secure Vault, abilitando i dispositivi wireless con sicurezza di livello 3 della certificazione PSA.

4.4. Zigbee

Figura 50 - Logo Zigbee

Zigbee (Figura 50) è una specifica basata su IEEE 802.15.4 ed è una suite di protocolli di comunicazione di alto livello utilizzati per creare reti senza fili locali (WLAN) con esigenze di bassa potenza e larghezza di banda ridotta. La tecnologia definita dalla specifica Zigbee è destinata ad essere più semplice e meno costosa rispetto ad altre reti wireless come bluetooth o più generali come il Wi-Fi.

Il suo basso consumo energetico limita le distanze di trasmissione a 10-100 metri (line of sight), a seconda della potenza erogata e delle caratteristiche ambientali. I dispositivi Zigbee possono trasmettere dati su lunghe distanze passando i dati attraverso una rete mesh di dispositivi intermedi per raggiungere quelli più distanti. Zigbee ha una velocità definita di 250 kbit/s, più adatta per trasmissioni di dati intermittenti da un sensore o dispositivo di input.

Le aree di applicazione tipiche includono:

- Domotica;
- Reti di sensori wireless;
- Sistemi di controllo industriale;
- Raccolta di dati medici;
- Avviso di fumo e intrusione;
- Automazione degli edifici.

Il design radio utilizzato da Zigbee ha pochi stadi analogici e utilizza circuiti digitali ove possibile. Il processo di qualificazione Zigbee prevede una convalida completa dei requisiti dello strato fisico. Le radio Zigbee hanno vincoli molto stretti su potenza e larghezza di banda. Un livello fisico non certificato che non funziona correttamente può aumentare il consumo energetico di altri dispositivi, pertanto, le radio sono testate con la guida fornita dalla clausola 6 dello standard 802.15.4-2006. [15]

Questo standard specifica il funzionamento nelle bande ISM da 2,4 a 2,4835 GHz in tutto il mondo, da 902 a 928 MHz per Americhe e Australia e da 868 a 868,6 MHz per l'Europa. Sedici canali sono allocati nella banda a 2,4 GHz, distanziati di 5 MHz, sebbene utilizzino solo 2 MHz di larghezza di banda ciascuno. Le radio utilizzano la codifica a spread spectrum a sequenza diretta, che è gestita dal flusso digitale nel modulatore. La chiave a sfasamento binario (BPSK) viene utilizzata nelle bande 868 e 915 MHz e la codifica a sfasamento in quadratura con offset (OQPSK) che trasmette due bit per simbolo viene utilizzata nella banda a 2,4 GHz.

La velocità dati raw over-the-air è di 250 kbit/s per canale nella banda a 2,4 GHz, 40 kbit/s per canale nella banda a 915 MHz e 20 kbit/s nella banda a 868 MHz. La velocità effettiva dei dati sarà inferiore alla velocità in bit massima specificata a causa del sovraccarico del pacchetto e dei ritardi di elaborazione. Per applicazioni indoor a 2,4 GHz la distanza di trasmissione è di 10-20 m, a seconda dei materiali di costruzione, del numero di pareti da penetrare e della potenza di uscita consentita in quella posizione geografica ma generalmente è 0-20 dBm (1-100 mW).

Esistono tre classi di dispositivi Zigbee:

- Coordinatore Zigbee (ZC): il dispositivo più capace, il coordinatore costituisce la radice della rete e può collegarsi ad altre reti. C'è esattamente un coordinatore Zigbee in ogni rete poiché è il dispositivo che l'ha avviata in origine.
- Router Zigbee (ZR): oltre a eseguire una funzione applicativa, un router può fungere da router intermedio, trasmettendo dati da altri dispositivi.

- Dispositivo finale Zigbee (ZED): contiene funzionalità sufficienti per comunicare con il nodo padre (il coordinatore o un router); non può inoltrare dati da altri dispositivi. Uno ZED richiede la minima quantità di memoria e quindi può essere meno costoso da produrre rispetto a uno ZR o ZC.

I dispositivi Zigbee devono essere conformi allo standard IEEE 802.15.4-2003 Low-rate Wireless Personal Area Network (LR-WPAN). Lo standard specifica i livelli di protocollo inferiori, ovvero il livello fisico (PHY) e la parte di controllo dell'accesso multimediale del livello di collegamento dati. La modalità di accesso al canale di base è l'accesso multiplo con rilevamento del vettore con prevenzione delle collisioni (CSMA/CA).

Come una delle sue caratteristiche distintive, Zigbee fornisce strutture per l'esecuzione di comunicazioni sicure, proteggendo l'istituzione e il trasporto di chiavi crittografiche e crittografando i dati. Si basa sul framework di sicurezza di base definito in IEEE 802.15.4. [15]

Il meccanismo di base per garantire la riservatezza è l'adeguata protezione di tutto il materiale consiste in un sistema di chiavi. Le chiavi sono la base dell'architettura di sicurezza; in quanto tale, la loro protezione è di fondamentale importanza e le chiavi non dovrebbero mai essere trasportate attraverso un canale insicuro. All'interno dello stack di protocollo, i diversi livelli di rete non sono separati crittograficamente, quindi sono necessari criteri di accesso. Il modello di trust aperto all'interno di un dispositivo consente la condivisione delle chiavi, che riduce notevolmente i costi potenziali. Poiché possono esistere dispositivi dannosi, ogni payload a livello di rete deve essere cifrato, in modo che il traffico non autorizzato possa essere immediatamente interrotto.

4.5. Thread

Figura 51 - Logo Thread

Thread (Figura 51) è una tecnologia di rete mesh a basso consumo basata su IPv6 per prodotti Internet of Things (IoT). La specifica del protocollo Thread è disponibile gratuitamente; tuttavia, ciò richiede l'accordo e la continua adesione a un Contratto di licenza con l'utente finale (EULA), che afferma che "L'appartenenza a Thread Group è necessaria per implementare, esercitare e distribuire la tecnologia Thread e le specifiche thread Group".

Thread utilizza 6LoWPAN, che, a sua volta, utilizza il protocollo wireless IEEE 802.15.4 con comunicazione mesh, così come Zigbee e altri sistemi. Tuttavia, Thread è indirizzabile IP, con accesso al cloud e crittografia AES. Lo standard viene utilizzato perché è in grado di fornire una trasmissione affidabile dei messaggi tra i singoli dispositivi del collegamento Thread. IEEE 802.15.4 fornisce un meccanismo CSMA-CA (descritto in precedenza) per consentire a più dispositivi di utilizzare la larghezza di banda condivisa a 2.4 GHz e permette una data rate massima di 250 Kbps, evitando la sovrapposizione di trasmissioni. Vengono inoltre fornite crittografia AES, autenticazione e protezione della riproduzione per garantire una comunicazione sicura.

Ci sono diversi tipi di dispositivi e ruoli all'interno di una rete thread:

- Routing full Thread Devices:
    - Router. Un Thread Router fornisce servizi di routing ai Thread Device nella rete. Esso fornisce anche servizi di connessione e sicurezza per i dispositivi che tentano di connettersi alla rete. I router possono eseguire il downgrade delle loro funzionalità e diventare REED;
    - Leader. È un ruolo aggiuntivo di un Router in una rete Thread. Il Leader prende determinate decisioni nella rete Thread come, ad esempio, consente ai REED di passare a Router.

- Non-Routing Full Thread Devices:

- Router-Eligible End Device (REED). I REED hanno la capacità di diventare router ma a causa della topologia o delle condizioni della rete non agiscono come router. La Thread Network gestisce i REED facendoli diventare Router attraverso il Leader, senza l'interazione dell'utente;
- Full End Device (FED). I FED sono dispositivi finali simili ai REED, tuttavia non hanno la capacità di essere Router; quindi, non diventerà mai un Routing Thread Device o Leader.

- Non-Routing Minimal Thread Devices:

  - Minimal End Device (MED). I dispositivi MED comunicano solo con il loro router genitore e non possono inoltrare messaggi per altri dispositivi. Ha la radio sempre attiva, pronto a comunicare;
  - Sleepy End Device (SED). I dispositivi SED comunicano solo con il loro router genitore e non possono inoltrare messaggi per altri dispositivi. Durante i periodi di inattività la radio viene spenta e poi periodicamente accesa per comunicare con il router di riferimento;
  - Synchronized Sleepy End Device (SSED). I dispositivi SSED comunicano solo con il loro router genitore e non possono inoltrare messaggi per altri dispositivi. Durante i periodi di inattività la radio viene spenta e poi periodicamente accesa per ascoltare i messaggi trasmessi dal router;
  - Bluetooth End Device (BED). I dispositivi BED comunicano solo con il loro router principale, che è un Bluetooth LE Bridge Router e non possono inoltrare messaggi per altri dispositivi. A differenza degli altri dispositivi essi comunicano con u Bluetooth Low Energy Link e non rispettano quindi lo standard IEEE 802.15.4;
  - Border Router. Un Border Router è un Thread Device che fornisce connettività alla rete Thread collegandola a reti adiacenti come ad esempio Wi-Fi o Ethernet. I Border Router forniscono servizi per i dispositivi all'interno della Thread Network, incluso appunto il routing, necessario per eseguire operazioni fuori dalla rete. [16]

Le reti di thread non hanno un singolo punto di errore e includono la capacità di auto-guarigione. Ad esempio, sebbene nel sistema siano presenti dispositivi che svolgono funzioni speciali, la Thread Network funziona in modo tale da poterli sostituire automaticamente senza influire sulla comunicazione in corso all'interno della rete. Ad esempio, uno Sleepy End Device (SED) richiede un router genitore per la comunicazione, quindi questo genitore rappresenta un singolo punto di errore. Tuttavia, il SED può e selezionerà un altro genitore se il suo attuale genitore non è disponibile, quindi questo errore dovrebbe essere invisibile all'utente. Volendo fare un altro esempio possiamo riferirci al ruolo di Leader. Questo Router è necessario per prendere decisioni all'interno della rete stessa. Il ruolo di Leader viene eletto dinamicamente e se il Leader fallisce un altro Router assume il ruolo. È questa operazione autonoma che garantisce che non ci sia un singolo punto di errore. Nonostante il sistema sia progettato per avere nessun singolo punto di errore, in determinate topologie ci saranno dispositivi che non dispongono di funzionalità di backup. Ad esempio, in un sistema con un solo Border Router, se il Border Router perde alimentazione, non è possibile passare a un'alternativa. L'affidabilità della rete, quindi, non dipende solo dal protocollo utilizzato ma anche dall'implementazione fisica vera e propria.

4.6. LoRa

Figura 52 - Logo LoRa

LoRa (Long Range, lungo raggio, Figura 52) è una tecnica di comunicazione radio a livello fisico proprietaria. Si basa su tecniche di modulazione dello spettro diffuso derivate dalla tecnologia Chirp Spread Spectrum (CSS).
LoRa utilizza la banda 2.4 GHz in tutto il mondo e bande di frequenza radio sub-gigahertz differenziate per i vari paesi, come riportato in tabella (Tabella 13).

Paese	**Banda**
Europa	eu868 (863-870/873 MHz)
Sud America	AU915/AS923-1 (915–928 MHz)
Nord America	US915 (902-928 MHz)
India	IN865 (865-867 MHz)
Asia	AS923 (915-928 MHz)

Tabella 13 - Banda utilizzata dal protocollo LoRa nei vari paesi

La tecnologia LoRa consente trasmissioni a lungo raggio con un basso consumo energetico. Questa soluzione copre il livello fisico, mentre altre tecnologie e protocolli come LoRaWAN (Long Range Wide Area Network) coprono gli strati superiori. Può raggiungere velocità di trasmissione dati comprese tra 0,3 kbit/s e 27 kbit/s, a seconda del fattore di diffusione (SF). [17]

Come anticipato, LoRa utilizza una modulazione proprietaria dello spettro diffuso che è simile e un derivato della modulazione dello spettro diffuso del chirp (CSS). Ogni simbolo è rappresentato da un chirp spostato sull'intervallo di frequenza $[fo - \frac{B}{2}, fo + \frac{B}{2}]$ dove f_0 è la frequenza centrale e B la larghezza di banda del segnale (in Hz). Il fattore di diffusione è un parametro radio selezionabile da 5 a 12 e rappresenta il numero di bit inviati per simbolo e inoltre determina quanto l'informazione è distribuita nel tempo. Ci sono $M = 2^{SF}$ diverse frequenze di Chirp e varia tra il valore minimo e massimo (raggiunta la frequenza massima $fo + \frac{B}{2}$ la frequenza istantanea viene riavvolta dal valore $fo - \frac{B}{2}$.

La tecnologia può scambiare la velocità dei dati trasmessi selezionando il SF, ossia la quantità di spread utilizzato. Un SF più basso corrisponde a una velocità di trasmissione dati più elevata ma una sensibilità peggiore, una SF più alta implica una sensibilità migliore ma una velocità di dati inferiore. Rispetto alla SF inferiore, l'invio della stessa quantità di dati con SF più elevato richiede più tempo di trasmissione, noto come time-on-air. Più time-on-air significa che il modem trasmette per un tempo più lungo e consuma più energia. I tipici modem LoRa supportano potenze di trasmissione fino a +22 dBm; tuttavia, le normative del rispettivo paese possono limitare ulteriormente la potenza di trasmissione consentita. Una maggiore potenza di trasmissione si traduce in una maggiore potenza del segnale al ricevitore e quindi in una qualità del collegamento più elevata, ma al costo di consumare più energia.

LoRaWAN definisce il protocollo di comunicazione software e l'architettura del sistema. Il continuo sviluppo del protocollo LoRaWAN è gestito dalla LoRa Alliance. È un protocollo MAC (Medium Access Control) basato su cloud, ma funge principalmente da protocollo a livello di rete per la gestione della comunicazione tra gateway LPWAN e dispositivi end-node come protocollo di routing.

LoRaWAN definisce il protocollo di comunicazione e l'architettura di sistema per la rete, mentre il livello fisico LoRa consente il collegamento di comunicazione a lungo raggio. LoRaWAN è anche responsabile della gestione delle frequenze di comunicazione, della velocità dati e dell'alimentazione per tutti i dispositivi. I dispositivi della rete sono asincroni e trasmettono quando sono disponibili dati da inviare. I dati trasmessi da un dispositivo end-node vengono ricevuti da più gateway, che inoltrano i pacchetti di dati a un server di rete centralizzato. La tecnologia mostra un'elevata affidabilità per il carico moderato, tuttavia, presenta alcuni problemi di prestazioni relativi all'invio di riconoscimenti.

Insieme, LoRa e LoRaWAN definiscono un protocollo di rete LPWA (Low Power, Wide Area) progettato per connettere in modalità wireless i dispositivi a batteria a Internet in reti regionali, nazionali o globali e si rivolge ai requisiti chiave dell'Internet of Things (IoT) come la comunicazione bidirezionale, la sicurezza end-to-end, la mobilità e i servizi di localizzazione. La bassa potenza, la bassa velocità in bit e l'utilizzo dell'IoT distinguono

questo tipo di rete da una WAN wireless progettata per connettere utenti o aziende e trasportare più dati, utilizzando più energia. [17]

4.7. Bluetooth

Figura 53 - Logo Bluetooth

Bluetooth (Figura 53) è uno standard tecnico-industriale di trasmissione dati per reti personali senza fili e viene generalmente utilizzato per realizzare WPAN (Wireless Personal Area Network) cioè piccole reti dall'estensione tipica di qualche metro. Fornisce un metodo standard, economico e sicuro per scambiare informazioni tra dispositivi diversi attraverso una frequenza radio sicura a corto raggio in grado di ricercare i dispositivi coperti dal segnale radio entro un raggio di qualche decina di metri mettendoli in comunicazione tra loro. Questi dispositivi possono essere ad esempio palmari, telefoni cellulari o personal computer purché provvisti delle specifiche hardware e software richieste dallo standard stesso.

Bluetooth funziona in banda ISM 2.45 GHz (2400-2483.5 MHz), con una modulazione frequency hopping – spread spectrum (FHSS) per ridurre l'effetto di interferenze e fading (cammini multipli). Sono disponibili 79 canali FHSS. In ogni canale, per minimizzare la complessità del radiotrasmettitore si usa una modulazione binaria FM a 1Mbit/s (lordo). Da standard, la distanza massima di comunicazione è 10 m (100 m con un trasmettitore potenziato). Tipicamente, un canale radio fisico è occupato da più dispositivi sincronizzati su una stessa sequenza di frequency hopping. Tale insieme di dispositivi si chiama "piconet". Un dispositivo, detto "master", è responsabile della sincronizzazione. Gli altri sono "slave".

Una rete di Bluetooth è organizzata in strati (livelli). Sopra al canale radio fisico abbiamo una serie di canali e collegamenti (link), e i relativi protocolli. Partendo dal canale radio fisico, abbiamo il livello fisico, composto dal canale fisico (physical channel) e dal collegamento fisico (physical link), il livello logico, composto dal trasporto logico (logical transport) e da collegamento logico (logical link), poi il livello "L2CAP" (Figura 54).

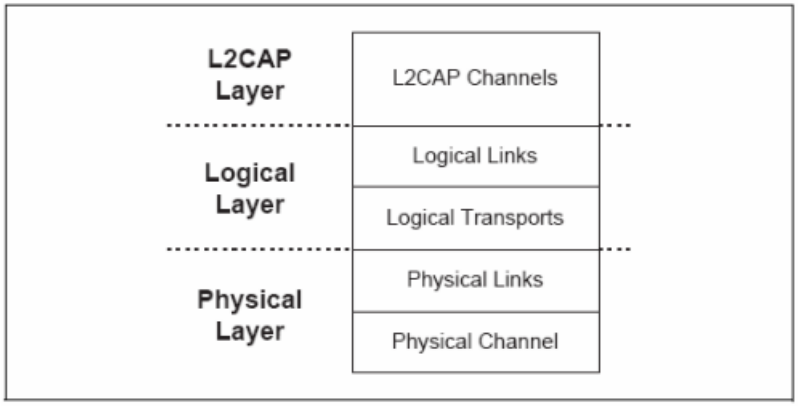


Figura 54 - Layer comunicazione Bluetooth

Bluetooth opera in una banda affollata da altri sistemi di comunicazione (la banda ISM è non regolata). Per ridurre gli effetti delle interferenze, si deve mettere in atto una tecnica di spread spectrum, che consenta di utilizzare al meglio tutta la banda disponibile (83.5 MHz). In particolare, si implementa una tecnica di "frequency hopping", cioè di variazione della frequenza di trasmissione secondo una particolare sequenza di salto (hopping) pseudocasuale specifica per ciascuna piconet. Il frequency hopping è una tecnica di cosiddetta "collision avoidance". Variando la frequenza di trasmissione su tutta la banda ISM si può evitare con alta probabilità l'interferenza di altri sistemi di comunicazione a banda stretta fissa o in frequency

hopping. In altre parole, si ha collisione solo quando la frequenza di trasmissione si sovrappone alla banda utilizzata dal sistema "interferente", cioè per un intervallo di tempo breve e per una frazione molto piccola del tempo di trasmissione. [19]

Le frequenze di trasmissione possibili sono 79, f = 2402 + k MHz (k=0 ÷ 78). C'è quindi una banda di sicurezza inferiore di 2 MHz, e una banda di sicurezza superiore di 3.5 MHz. Il tempo è suddiviso in intervalli ("slot") di 625 µs. Durante uno slot viene trasmesso un "pacchetto". In alcuni casi (vedremo più avanti), è possibile trasmettere pacchetti della durata multipla di uno slot. La frequenza di trasmissione viene cambiata, secondo una sequenza pseudocasuale, ogni volta che viene trasmesso un pacchetto. Nel caso tipico, in cui un pacchetto ha la durata di uno slot, la frequenza di trasmissione viene quindi cambiata ogni 625 µs ("hopping rate" = 1600 hop/s). Altri casi sono possibili. La sequenza pseudocasuale di hopping viene determinata dal numero seriale del master.

Il trasmettitore può appartenere a una di quattro classi di potenza di trasmissione (Tabella 14):

- Potenza ERP: massima potenza trasmissiva in radiofrequenza, comprendente l'incremento dovuto al guadagno in trasmissione dell'antenna del dispositivo;
- Distanza: è il raggio massimo di copertura a portata ottica, cioè senza ostacoli, entro cui può avvenire il collegamento fra dispositivi BT.

Classe	**Potenza ERP**		**Distanza [m]**
	[mW]	**[dBm]**	
1	100	20	~100
2	2.5	4	~10
3	1	0	~1
4	0.5	-3	~0.5

Tabella 14 - Descrizione classi trasmettitori bluetooth

Lo standard prevede una sensibilità del ricevitore di -70 dBm, per una BER (bit error rate) grezza (cioè escludendo meccanismi di correzione dell'errore) dello 0.1%. Confrontata con altre reti radio la sensibilità non è particolarmente spinta (ad esempio per il Wi-Fi la sensibilità è –90 dBm) e la cosa si paga in termini di minore portata. Tipicamente si riesce a realizzare un ricetrasmettitore bluetooth in un unico chip in tecnologia CMOS, e quindi in modo economico.

La rete elementare bluetooth si chiama "piconet". È costituita da 2 a 8 radiotrasmettitori (a e b della figura in basso). Un dispositivo ha il ruolo di "master", gli altri sono "slave". Il collegamento fisico può essere realizzato solo tra il master e uno slave. Non è possibile avere un collegamento fisico tra due slave. Da notare che l'architettura della rete è simmetrica, nel senso che ciascun radiotrasmettitore può fare sia da master, sia da slave. Nel momento in cui una rete si forma, il primo dispositivo che partecipa alla rete prende il ruolo di master, gli altri quello di slave (Figura 57a,57b). Un dispositivo può inoltre appartenere a più di una piconet (come slave o come master), ma può essere master solo di una, e in tal caso si chiama "bridge" (Figura 55), e permette di unire più piconet in una "scatternet" (in c della figura in basso tre piconet sono unite in una scatternet).

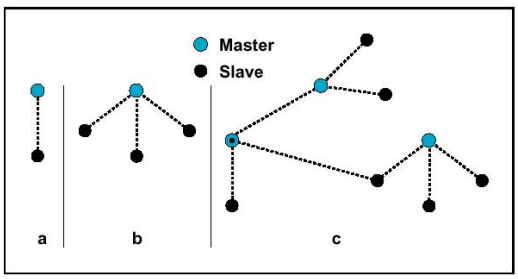


Figura 55 - Esempio piconet

Per quanto riguarda il Bluetooth la cifratura è implementata mediante una somma modulo 2 bit a bit tra il pacchetto da spedire in uno slot temporale e una chiave altrettanto lunga. La particolarità di questo algoritmo è che l'operazione di cifratura e di decifratura sono identiche: si somma modulo due una chiave di lunghezza pari al messaggio da trasmettere sia per cifrare che per decifrare. La chiave viene generata da entrambi i dispostivi sulla base di una serie di parametri scambiati e precondivisi poi elaborati da un algoritmo.

4.8. Bluetooth Low Energy

Figura 56 - Logo BLE

Il Bluetooth Low Energy (BLE, Figura 56), in passato conosciuto come Bluetooth Smart, è una tecnologia che il gruppo Bluetooth SIG ha prodotto appositamente per applicazioni che necessitano di trasmissione wireless con un consumo di energia ancora minore rispetto al Bluetooth classico ma con un bitrate maggiore. Il progetto è stato ideato nel 2001 e commercializzato nel 2006 da Nokia con il nome di Wibree. Nel 2007 il marchio è stato poi incluso all'interno delle specifiche Bluetooth. L'integrazione con la versione 4.0 è avvenuta all'inizio del 2010 mentre i primi dispositivi che implementavano tale caratteristica sono usciti nel 2011. Oggi il Bluetooth Low Energy si basa sulle specifiche del Bluetooth 4.1, rilasciate nel dicembre 2013.

Il primo componente fondamentale del BLE è il GAP (Generic Access Profile). Esso si occupa della gestione della connessione e della fase di advertising, rendendo il dispositivo visibile al mondo esterno e determinando quali dispositivi possono o non possono interagire con gli altri. Il GAP definisce diversi ruoli che possono essere ricoperti dai due dispositivi connessi:

- Peripheral: il device è visibile agli altri dispositivi (fa advertising) e può accettare connessioni in ingresso (slave). Non è, però, in grado di iniziare una connessione. Questo ruolo è utilizzato, generalmente, per dispositivi di sensoristica;
- Central: il device è in grado di ricercare dispositivi visibili e di iniziare la connessione (master). Non è, però, in grado di accettare connessioni in ingresso. Questo ruolo è generalmente ricoperto dagli smartphone, dai tablet o dagli altri dispositivi che si connettono ai sensori. [19]

Due dispositivi che ricoprono lo stesso ruolo non sono in grado di connettersi l'un l'altro. Inoltre, un dispositivo peripheral è in grado di connettersi solamente ad un dispositivo Central alla volta (Figura 57).

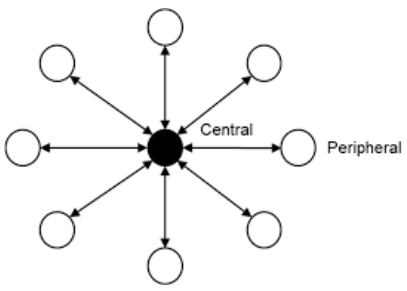


Figura 57 - esempi dispostivi BLE

Tutti i servizi che utilizzano la tecnologia BLE si basano sul GATT (Generic Attribute Profile). Esso non è altro che un'interfaccia software che definisce come i dispositivi possano inviare e ricevere dati, descrivendo i concetti di Servizio e Caratteristica. Il GATT sfrutta a sua volta l'ATT (Attribute Protocol), che viene utilizzato per contenere i dati dei Servizi e delle Caratteristiche che il GATT mette a disposizione all'esterno. I dati relativi a Servizi e Caratteristiche sono memorizzati in un'apposita lookup-table usando un identificatore lungo 16 byte chiamato UUID. Di questi 16 byte i primi 4 vengono scelti dal programmatore mentre gli altri sono stabiliti dal dispositivo stesso. Poiché nel BLE è importante limitare al massimo la quantità di dati trasmessi, il SIG ha stabilito uno UUID base formato dai primi 12 byte dell'UUID completo. In questo modo non è necessario trasmettere ogni volta l'intero UUID, ma è sufficiente comunicare solamente gli ultimi 4 byte.

Lo scambio di dati tra dispositivi BLE è basato su oggetti di alto livello che prendono il nome di Profili, Servizi e Caratteristiche (Figura 58). Si può accedere ad ogni oggetto solo nelle modalità previste dal progettista (sola lettura, sola scrittura, entrambe o nessuna) e, se necessario, solo dopo aver ottenuto un'autorizzazione.

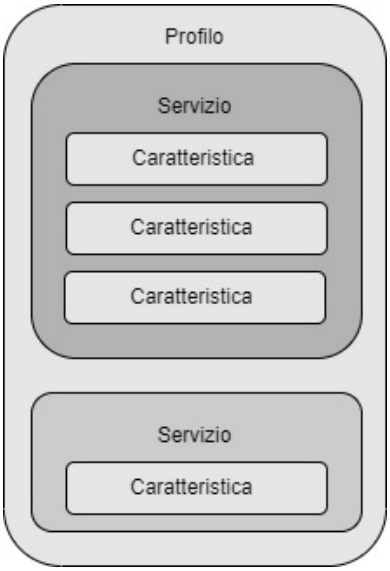


Figura 58 - GATT

- Profilo: collezione di Servizi definita dal BSIG (Bluetooth Special Interest Group) o dal progettista della periferica. Essi combinano Servizi che mettono a disposizione informazioni di vario tipo;
- Servizio: identificato da uno UUID, funge da contenitore per una serie di caratteristiche.
- Caratteristiche: sono gli oggetti di livello più basso. Ognuna di esse incapsula un puntatore ai dati (dati singoli di varia lunghezza, come numeri interi o decimali, oppure array di valori). Esse sono identificate da uno UUID. Oltre ai permessi di lettura e/o scrittura esistono altre proprietà memorizzate nel descrittore della caratteristica che permettono, per esempio, di definire se il valore può essere inviato broadcast oppure di notificare automaticamente il dispositivo connesso della disponibilità di un nuovo dato. [19]

Il Bluetooth Special Interest Group sopra indicato è un'organizzazione che sovrintende lo sviluppo degli standard Bluetooth e che possiede il marchio denominativo, il segno di figura e il segno di combinazione Bluetooth. Questi marchi sono concessi in licenza per l'uso a società che incorporano la tecnologia wireless Bluetooth nei loro prodotti. Per diventare un licenziatario, un'azienda deve diventare un membro del Bluetooth SIG pagando una quota associativa da rinnovare ogni anno e il suo valore dipende dalle entrate della singola società:

- $ 35.000 per aziende con un fatturato annuo superiore a $ 100 milioni negli Stati Uniti d'America (considerate Large Associates);

- $ 7.500 per quelle organizzazioni con entrate inferiori a $ 100 milioni negli Stati Uniti d'America (considerate Small Associates).

Riprendendo lo scambio di dati invece, ogni servizio, caratteristica e descrittore ha un proprio UUID (Universally Unique IDentifier), un numero unico a 128 bit, come il seguente:

55072829-bc9e-4c53-938a-74a6d4c78776

Questo codice viene utilizzato per identificare univocamente una informazione, ad esempio una particolare caratteristica può essere identificata tramite il suo codice.
Bluetooth standard e Bluetooth Low Energy possono essere tra loro comparati utilizzando la seguente tabella (Tabella 15)

	Bluetooth Low Energy	**Bluetooth**
Ottimizzato per	Trasmissioni brevi	Trasmissioni continue
Banda	2.4 GHz ISM Band (2.402 – 2.480 GHz)	2.4 GHz ISM Band (2.402 – 2.480 GHz)
Canali	40 canali con ampiezza 2 MHz	79 canali con ampiezza 1 MHz
Utilizzo del canale	FHSS	FHSS
Modulazione	GFSK	GFSK, DQPSK, 8DPSK
Consumi	0.01 – 0.5 rispetto al riferimento	riferimento
Data rate	LE 2M PHY: 2 Mb/s LE 1M PHY: 1 Mb/s LE Coded PHY (S=2): 500 Kb/s LE Coded PHY (S=8): 125 Kb/s	EDR PHY (8DPSK): 3 Mb/s EDR PHY (DQPSK): 2 Mb/s BR PHY (GFSK): 1 Mb/s
Massima potenza consumata in Tx	Classe 1: 100 mW (+20 dBm) Classe 1.5: 10 mW (+10 dBm) Classe 2: 2.5 mW (+4 dBm) Classe 3: 1 mW (0 dBm)	Classe 1: 100 mW (+20 dBm) Classe 2: 2.5 mW (+4 dBm) Classe 3: 1 mW (0 dBm)
Topologia di rete	Point-to-Point (Piconet inclusa) Broadcast Mesh	Point-to-Point (Piconet inclusa)

Tabella 15 - Confronto Bluetooth standard e Bluetooth Low Energy

Da questo confronto è possibile evidenziare come il BLE si adatti meglio a brevi ed istantanee comunicazioni e sia in grado di garantire consumi molto più bassi, almeno la metà della potenza consumata rispetto al Bluetooth standard.

La connessione tra due dispositivi, un Master e uno Slave per la precisione, avviene nel seguente modo: si inizia con una prima fase chiamata "Advertising" in cui il dispositivo BLE con ruolo Peripheral (ESP32) invia, ad intervalli regolari, un pacchetto di advertise. Essi hanno dimensioni comprese tra 6 e 37 byte e contengono informazioni relative al dispositivo che li ha inviati (Figura 59). Tali pacchetti sono inviati su 3 dei 40 canali dedicati alla funzione (canali 37, 38 e 39). Se un altro dispositivo è interessato a stabilire una connessione si mette in ascolto su uno di questi canali in attesa di intercettare un pacchetto di advertising; quando questo accade il dispositivo può effettuare una richiesta di connessione per richiedere dati aggiuntivi e diventa il Master della comunicazione. L'intervallo di advertising è impostato dal programmatore e può variare tra 20 ms e 10,24 s in intervalli di 0,625 ms. Viene inoltre aggiunto un intervallo pseudo-random compreso tra 0 e 10 ms per ridurre la possibilità di collisioni tra advertisement di differenti dispositivi. È importante selezionare

con cura la durata dell'intervallo per bilanciare ragionevolmente il consumo di energia e la velocità nel farsi riconoscere da un eventuale altro dispositivo.

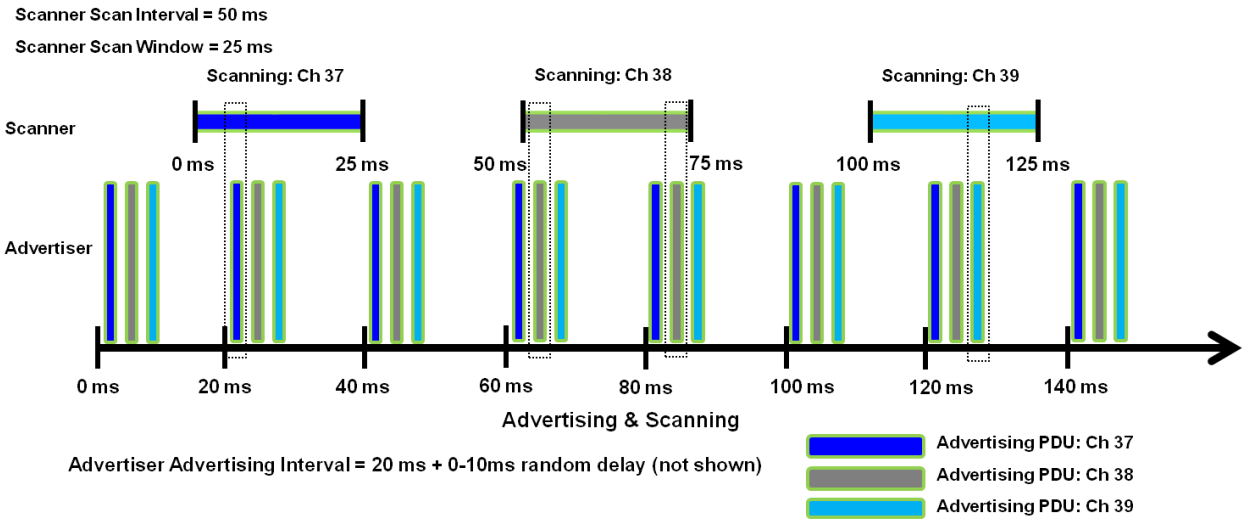


Figura 59 - BLE Scanning

Una volta che il device Central ha richiesto informazioni aggiuntive al device Peripheral si può stabilire una connessione. Devono essere a questo punto definiti alcuni parametri: l'intervallo di connessione e la Slave Latency. I dispositivi mantengono in piedi la connessione scambiando periodicamente dati anche se non c'è nulla da trasmettere: questa operazione è detta Connection event. Il periodo di tempo che intercorre tra uno scambio e l'altro è dettato dall'intervallo di connessione, valore che può variare tra 7,5 ms e 4 s. Per risparmiare ulteriormente energia il dispositivo peripheral, qualora non abbia informazioni da scambiare, può decidere di non rispondere all'evento di connessione. Il numero di eventi di connessione che il device peripheral può ignorare senza far cadere la connessione viene definito dal parametro detto Slave Latency. In questo modo i dispositivi si troveranno a comunicare più frequentemente quando è necessario inviare dati, mentre più raramente quando ciò non è necessario. [19]

4.9. Confronto delle tecnologie e scelta della soluzione più adatta

Una prima comparazione molto utile può essere realizzata andando ad analizzare i campi di applicazione di tutte le tecnologie appena descritte. La tabella seguente (Tabella 16) mette in evidenza se il particolare protocollo può essere utilizzato nei seguenti ambiti:

- Outdoor Mobile-Dispositivo. Comunicazione in ambiente esterno tra smartphone con installata l'App Elica Connect ed il dispositivo Cappa connessa alla rete Wi-Fi domestica;
- Indoor Mobile-Dispositivo. Comunicazione all'interno dell'abitazione tra smartphone con installata l'App Elica Connect ed il dispositivo Cappa connessa alla rete Wi-Fi domestica;
- Indoor Dispositivo-Dispositivo. Comunicazione tra i vari elettrodomestici connessi all'interno della stessa abitazione.

Tecnologia	Outdoor Mobile-Dispositivo	Indoor Mobile-Dispositivo	Indoor Dispositivo-Dispositivo
Wi-Fi	✓	✓	✓
NFC		✓	
Z-Wave	✓	✓	✓
Zigbee	✓	✓	✓
Thread	✓	✓	✓
LoRa	✓	✓	✓
Bluetooth		✓	✓
Bluetooth Mesh		✓	✓

Tabella 16 - Confronto tecnologie in tre scenari applicativi

Nella tabella seguente (Tabella 17) verranno invece confrontate le varie tecnologie con il fine di evidenziale i loro punti di forza. L'analisi verrà fatta sulla base dei seguenti parametri:

- Distanza. La tecnologia deve garantire il funzionamento ad una distanza di almeno 10 metri;
- Consumi. I consumi, sia durante il funzionamento che durante lo stand-by, devono essere sottosoglia;
- Dimensione antenna. La tecnologia per comunicare richiede l'utilizzo di antenne specifiche, queste devono avere dimensioni tali da poter essere stampate agevolmente sul PCB senza aumentarne le dimensioni in maniera eccessiva;
- Sicurezza. Se le tecnologie garantiscono cifratura delle informazioni trasmesse utilizzando soluzioni direttamente integrate o tramite l'azione su protocolli di livello superiore;
- Mesh. La tecnologia può dover permettere la connessione tra i vari nodi della rete (prodotti Elica) con fine di creare una rete mesh. Questo, tuttavia, non è al momento un requisito fondamentale;
- ISM. È importante che le frequenze utilizzate dalle varie tecnologie rientrino nella banda ISM, ovvero utilizzino frequenze destinate a scopi Industriali, Scientifici e Medici, cioè di libero impiego;
- Costi. L'analisi tiene conto dei costi di introduzione e gestione della tecnologia;
- Velocità. Data rate a disposizione;

- Comunicazione diretta smartphone-cappa. Vista la natura dell'analisi, definita con l'obiettivo di trovare una nuova tecnologia in grado di permettere la registrazione dell'App sulla cappa, è necessaria la possibilità di comunicare direttamente tra lo smartphone e la cappa.

Tecnologia	Distanza	Consumi	Dimensione Antenna	Sicurezza	Mesh	ISM	Costi	Velocità	Comunicazione diretta smartphone-cappa
Wi Fi ALLIANCE	✓	✓	✓	✓		✓	5,150$	1-9608 Mbit/s	✓
		✓	✓	✓		✓	5,000$	106-424 Kbit/s	✓
Z-WAVE	✓	✓	✓	✓	✓	✓	10,000$	100 Kbit/s	
zigbee	✓	✓	✓	✓	✓	✓	10,000$	250 Kbit/s	
THREAD	✓	✓	✓	✓	✓	✓	7,500$	250 Kbit/s	
LoRa®	✓	✓	✓	✓	✓	✓	6,000$	0.3-27 Kbit/s	
Bluetooth®	✓	✓	✓	✓	✓	✓	9,600$	1-3 Mbit/s	✓
	✓	✓	✓	✓	✓	✓	9,600$	1-2 Mbit/s	✓

Tabella 17 - Confronto principali caratteristiche delle tecnologie proposte

Nel confronto, ad eccezione della data rate e dei costi, non sono riportati i valori ma semplicemente un simbolo che permette di indicare se le specifiche della tecnologia soddisfano i requisiti richiesti. Ad esempio, per la distanza, il valore cambia in base alla potenza irradiata. La spunta significa che è possibile raggiungere il valore di distanza minimo richiesto per il corretto utilizzo. ISM significa invece che le frequenze utilizzate nella comunicazione sono appunto le bande libere. Questa logica è applicabile a tutti gli altri campi

della tabella. Unica eccezione sono i campi “Velocità” e “Costi”: nel primo caso sono riportate le velocità raggiungibili dal particolare protocollo mentre nel secondo vengono riportati i soli costi di gestione, quindi tasse da pagare alle “alliance” e costi legati alla certificazione dei vari prodotti. Per la maggior parte delle tecnologie, infatti, per avere accesso a tool di certificazione è necessario fare parte della rispettiva alleanza mentre per poter esibire il logo del protocollo utilizzato è necessario superiore una fase di test in centri appositi con il fine di garantire poi al prodotto finiti i requisiti minimi di funzionamento. È importante evidenziare come gli abbonamenti e costi per i singoli prodotti vadano rinnovati ogni anno, si tratta quindi di una spesa fissa da sostenere ma che permette di avere accesso a materiale, tools, librerie, convegni ed altri tipi di informazioni utili allo sviluppo di un nuovo prodotto.

Dalla tabella (Tabella 17) è possibile estrarre alcune conclusioni. L’NFC, seppur soddisfi la maggior parte dei requisiti, mostra un vincolo estremamente importante in termini di distanza di utilizzo; l’obbligo di non potersi trovare ad una distanza superiore a 20 cm rende questa tecnologia inutilizzabile su alcuni tipi di cappe (basti pensare alle Ceiling che sono cappe a soffitto, quindi a 2.5 m di altezza circa). Alcune delle altre soluzioni invece, nonostante garantiscano distanze maggiori, trovano invece un blocco per quanto riguarda l’utilizzo dello smartphone per effettuare una comunicazione diretta con la cappa senza passare attraverso il cloud. Più precisamente, infatti, tutte le reti descritte sopra fanno riferimento ad un router; quindi, la comunicazione attraverso un cloud e quindi uno smartphone è sempre possibile. Tuttavia, la cappa è già dotata di un sistema di comunicazione basato su rete Wi-Fi e la nuova tecnologia dovrebbe essere in grado di garantire una comunicazione alternativa, appunto diretta, tra lo smartphone e la cappa. Di conseguenza ai fini dell’On-boarding sull’App Elica Connect tecnologie come Z-wave, Zigbee, Thread e LoRa devono essere scartate.
La scelta ricade quindi tra due tecnologie, anche se rientrano nelle stesse specifiche e sono tra loro integrati: Bluetooth e Bluetooth Low Energy. Ai fini dell’applicazione in questione, in cui non è richiesta eccessiva capacità di trasmissione o elevate prestazioni, le due tecnologie garantiscono il corretto funzionamento ad una distanza non inferiore a 10 metri e di conseguenza il parametro di scelta diventa il consumo: caratteristica che porta a prediligere il BLE rispetto alla versione standard. Ultima considerazione che è possibile fare riguarda il costo: in generale si va da un valore minimo di 5,000$ ad un massimo di 10,000$, valori indicativi sulla base della realizzazione di un singolo prodotto che implementa quella particolare tecnologia (ad esempio per il Bluetooth si può pagare una quota associativa al SIG e poter poi risparmiare sulla tassa del prodotto, in questo caso si ha un risparmio quando si devono certificare più prodotti tra loro diversi). La differenza di costo è quindi relativa e non vincolante ai fine della scelta finale. Per quanto riguarda invece eventuali costi legati allo sviluppo di un nuovo hardware la soluzione più facilmente implementabile è anche in questo caso il Bluetooth, dato che la tecnologia può già essere utilizzata con i moduli ESP32 che implementano congiuntamente Wi-Fi e Bluetooth. Esistono moduli ESP32 contenenti librerie per utilizzare protocolli come Zigbee o Thread, ad esempio l’ESP32-H2, ma questo modulo è disegnato per comunicazioni a bassa potenza IoT e non supporta quindi il Wi-Fi.

5. Sviluppo della nuova User Interface

Dopo aver descritto l'attuale stato dell'arte e svolto un'analisi comparativa delle principali tecnologie al momento disponibili si è deciso di implementare il Bluetooth Low Energy come soluzione al problema del dover semplificare il processo di registrazione della cappa sull'App Elica Connect.
In questo capitolo verrà descritto tutto il processo che ha portato alla realizzazione della nuova User Interface, quindi dalla definizione delle specifiche, passando per il dialogo con le possibili aziende per la produzione della nuova board fino alla sua realizzazione, trattando poi l'implementazione vera e propria della comunicazione smartphone-cappa. Infine, verrà descritto più nel dettaglio il processo di certificazione di un prodotto, riportando tutte le prove che sono generalmente eseguite e le corrispondenti normative di riferimento.

5.1. La nuova UI

Nel capitolo uno, durante la descrizione della cappa è stata approfondita la User Interface della Superplat. Questa interfaccia utente e relativo hardware poi descritto, quindi board della UI e core Wi-Fi separato, rappresentano il vecchio modo di intendere l'implementazione della connettività sulle cappe.
In questo momento l'Azienda si pone come obiettivo non solo semplificare il processo di registrazione del prodotto sull'App Elica Connect ma anche abbattere i costi di produzione. L'intento è infatti valutare la fattibilità realizzativa di un unico hardware UI + Connectivity; quindi, una unica board con i pulsanti capacitivi ed il core Wi-Fi, insieme naturalmente a tutta l'elettronica necessaria per il corretto funzionamento. Questa necessità nasce da un intento di estrema importanza in ambito industriale: risparmiare. La presenza di due componenti distinti infatti porta un costo superiore rispetto ad un unico hardware. Inizialmente si è inserito il core Wi-Fi come terzo elemento sul One Wire Bus per due ragioni: economiche e di implementazione. Nel primo caso non sapendo quale sarebbe stata la risposta del mercato ad una cappa connessa e la necessità di dover coprire tutti i costi associati all'infrastruttura di rete, server, sviluppo di codici ed applicazioni per smartphone non permettevano anche di caricarsi dei costi di sviluppo della nuova scheda; nel secondo caso invece la soluzione è general purpose, ovvero applicabile a qualunque cappa si voglia rende Smart, dato che si tratta appunto di un componente aggiuntivo totalmente indipendente dagli altri da collegare al bus dati. Ora, passati alcuni anni dal lancio del primo prodotto connesso e guidati da una politica aziendale che ha deciso di implementare la connettività su più prodotti, si è presentata la necessità di investire nuove risorse con la possibilità di poter contare su una domanda tale da permettere di recuperare i costi sostenuti nel breve termine.

Durante la mia esperienza in Azienda ho seguito il processo che porta all'implementazione sul prodotto finito di una nuova scheda hardware. Sostituire un componente comporta la definizione delle specifiche desiderate e la ricerca di un nuovo fornitore che sia in grado di progettare il componente e soddisfare le richieste aziendali. Per completare questo primo step Elica si affida, appunto, a ditte esterne; infatti all'interno dell'Azienda non vengono eseguite le realizzazioni hardware e software vere e proprie, bensì essa mette a disposizione le proprie competenze interne e know-how per la definizione delle specifiche tecniche e funzionali che l'hardware deve possedere, come ad esempio i componenti necessari, le dimensioni, il numero di pulsanti capacitivi, quando accendere led o emettere suoni e così via; tutte queste informazioni sono poi riportate in dei documenti interni chiamati STF (Specifiche Tecniche Funzionali) ed inviati alle aziende produttrici di schede elettroniche per valutare la fattibilità e ricevere le loro offerte. Queste ultime si occupano solamente della fase di esecuzione e produzione, lasciando il controllo sul progetto e sul testing ad Elica. Seguono poi una serie di processi interni per la sostituzione del componente, che va dalle modifiche delle distinte all'esecuzione di test nel laboratorio.

Il completamento del processo appena descritto naturalmente richiede del tempo, può occupare due mesi per lo sviluppo di un semplice hardware fino a cinque o sei mesi nel caso di schede molto più complesse come quella in esame. Proprio per questo non è stato possibile seguire tutto il processo nel tempo a disposizione ma le fasi a cui ho partecipato attivamente nel periodo di tirocinio curriculare sono state due: la definizione delle specifiche e la valutazione delle offerte.

5.1.1. Definizione delle specifiche tecniche e funzionali

Le specifiche tecniche funzionali sono dei documenti ufficiali e confidenziali che contengono tutte informazioni e requisiti di una scheda o di un qualsiasi altro protocollo, applicazione o datamodel utilizzato dall'azienda. La loro stesura è di fondamentale importanza perché rappresenta un riferimento univoco per Elica e produttori, se il prodotto finale non è conforme alla specifica sarà infatti obbligo del fornitore risolvere il problema, ma allo stesso modo se il prodotto finale non funziona a causa di un errore della specifica sarà invece obbligo di Elica farsi carico dei costi di correzione. Il documento può essere macroscopicamente diviso in due parti: requisiti generali dell'ingegnerizzazione dell'hardware e requisiti di funzionamento. Durante il tirocinio ho partecipato ad una serie di riunione volte a definire questi punti.

Per quanto riguarda le specifiche hardware il punto di partenza sono gli standard normativi legati alla sicurezza ed alla compatibilità elettromagnetica: la scheda deve essere costruita con criteri e caratteristiche comprovate da normative internazionali con il fine di soddisfare i criteri minimi imposti. Inoltre, tutti i componenti richiesti da inserire nella scheda devono infatti rispettare standard normativi oltre a particolari richieste di Elica stessa. L'elenco dei componenti che la nuova board deve contenere sono i seguenti:

- 1 microcontrollore;
- 1 sezione controllata dal microcontrollore per comandare I relè sulla scheda Main e per implementare la comunicazione seriale;
- 7 pulsanti capacitivi;
- 11 LEDs (8 bianchi, 3 gialli)
- 1 o più regolatori di tensione per garantire un'alimentazione di 5 V e 3.3 V;
- 1 NTC, sensore di temperatura;
- 1 buzzer;
- 1 modulo Wi-Fi + Bluetooth ESP32-WROOM-32D o equivalente (in ogni caso il produttore deve essere EspressIf);
- 1 voltage level shifter 3.3V/5V;
- 1 connettore su PCB Lumberg MICS, 8 pin, pitch 1.27 mm;
- 1 connettore su PCB Micro-MaTch femmina Top-Entry 6 pos. SMD (188275-6, TE Connectivity o equivalente), sarà usato per collegare il sensore per la qualità dell'aria;
- Altri componenti discreti (come transistori, diodi, resistenze e capacità). [6]

È inoltre richiesto che la capacità di elaborazione del microcontrollore installato sulla scheda sia in grado di gestire correttamente il protocollo One-Wire bus, la connettività, gli aggiornamenti OTA ed una adeguata dimensione della memoria.
La componentistica che viene inserita, oltre a quella base per garantire il corretto funzionamento della scheda (cioè che la pressione del pulsante effettivamente accenda la luce, per questo sono sufficienti il pulsante ed il micro con un'uscita sulla seriale), presenta molte scelte personalizzate legate all'utilizzo vero e proprio, ovvero alla UX (User Experience), necessarie al soddisfacimento della seconda parte dell'STF (i led servono per dare una risposta all'utente, così come il suono emesso dal buzzer).

Oltre al semplice elenco di componenti sono poi indicate linee guida da seguire in fase di design. Innanzitutto, se non specificato diversamente si suppone un "Pollution Degree" = 3, ovvero un grado di inquinamento di livello tre, ovvero in cui si può verificare inquinamento conduttivo o inquinamento non conduttivo o secco

ma che a causa di condensa diventa comunque conduttivo. Viene poi riportata la distanza di dispersione tra le piste che è necessario rispettare sulla base di un insieme di parametri:

- CTI (Comparative Tracking Index) usato per misurare la capacità di tenuta di un materiale isolante alle scariche superficiali, maggiore è il suo valore e migliori sono le sue capacità di resistere a scariche superficiali;
- PD (Pollution Degree);
- Tensione di funzionamento.

La tabella di seguito (Tabella 18) riportata descrive i valori di distanza minimi nelle varie situazioni.

Gruppo I: CTI>600 **Gruppo II**: 400 < CTI ≤ 600 **GRUPPO IIIa**: 175 < CTI ≤ 400	**Distanza di dispersione [mm]**			
	Isolamento base		**Isolamento funzionale**	
	PD3		**PD3**	
Tensione di lavoro [V]	**Gruppo II**	**Gruppo IIIa/IIIb**	**Gruppo II**	**Gruppo IIIa/IIIb**
≤ 50	1.7	1.9	1.6	1.8
> 50 e ≤ 125	2.1	2.4	2	2.2
> 125 e ≤ 250	3.6	4.0	2.8	3.2
> 250 e ≤ 400	5.6	6.3	4.5	5

Tabella 18 - Distanza di dispersione

Nella definizione della distanza sono riportati due tipi di isolamento: base e funzionale. Nel primo caso rappresenta l'isolamento realizzato tra due parti attive per provvedere ad una protezione base contro l'elettro shock, il secondo invece rappresenta l'isolamento tra due parti conduttive poste ad una certa differenza di potenziale e che è necessario solo al semplice funzionamento del dispositivo stesso.
Vengono poi inserite nel documento quelle che sono le condizioni ambientali in cui si potrà trovare l'apparato durante l'immagazzinamento, trasporto e utilizzo vero e proprio. Il prodotto e quindi la scheda si troveranno nelle seguenti condizioni (Tabella 19):

	Lavoro	**Trasporto/Immagazzinamento**
Umidità	0% ÷ 95%	0% ÷ 95%
Temperatura	0°C ÷ 70°C	-40°C ÷ 85°C

Tabella 19 - Livelli di temperatura ed umidità

Sono poi riportati due valori di consumo in stand-by da soddisfare, che fanno riferimento a due possibili situazioni differenti:

1. Stand-by con il Wi-Fi ON: il consumo totale del sistema deve essere < 2 W;
2. Stand-by con il Wi-Fi OFF: il consumo totale del sensore deve essere < 0,5 W.

Questi due valori rappresentano la condizione in cui l'utente spegne l'apparato (ventola a velocità zero e luci spente) distinguendo i due casi con il Wi-Fi attivo o disattivo. In entrambe le condizioni il limite è normativo ed il non soddisfacimento di questo requisiti causa l'impossibilità di vendere il prodotto sul mercato. È importante evidenziare che il caso di stand-by con il livello inferiore non deve essere rappresentato in alcuno modo; infatti, normativamente il limite è molto basso ed il consumo può essere ritenuto trascurabile. Nel caso con il Wi-Fi attivo, il limite accettato è maggiore ma questa condizione deve essere in qualche modo segnalata all'utente; proprio per questo quando il Wi-Fi è attivo un led bianco fisso è sempre presente sulla User Interface, in questo modo l'utente può riconoscere la situazione ed il consumo così da decidere se spegnere anche il Wi-Fi e rientrare nel caso di assorbimento più basso. Fornire questi valori è molto importante affinché la scheda implementi sia dal punto hardware che software soluzioni atte alla minimizzazione dei consumi in caso di stand-by.

Definite tutte le specifiche legate alla realizzazione dell'hardware il documento descrive poi nel dettaglio il funzionamento della cappa. Sono riportate tutte le operazioni che la User Interface deve permettere e come

questa deve rispondere ad ogni possibile comando, sia dal punto di vista visivo per l'utente che di funzionamento vero e proprio. Questa parte della specifica è di fondamentale importanza affinché il fornitore sia in grado di capire come sviluppare il firmware della board, dato che il suo compito è restituire un prodotto perfettamente in linea con la specifica sia dal punto di vista hardware che software. Per quanto riguarda questa sezione è possibile riportarne un estratto legato al lampeggio dei led posti al di sotto della UI: la specifica descrive tre diversi tipi di pulsazioni del led, riportate di seguito attraverso il corrispondente segnale di alimentazione (Tabella 20).

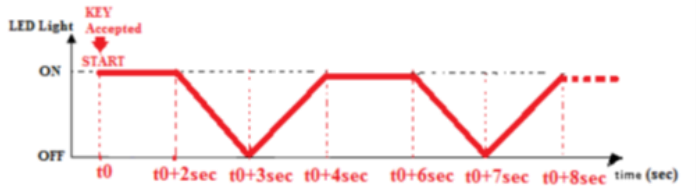
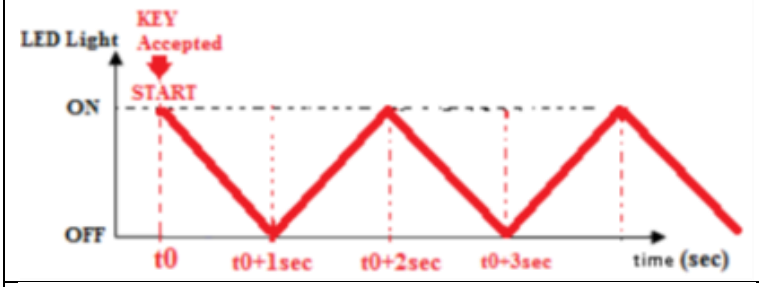
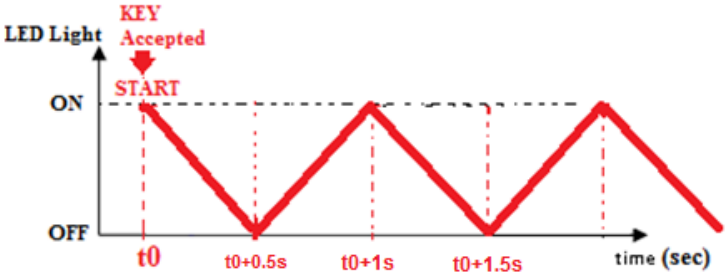
	**SLOW** Pulsazione lenta
	**FAST** Pulsazione veloce
	**VERY FAST** Pulsazione molto veloce

Tabella 20 – Segnale elettrico per i vari tipi di pulsazioni

Queste informazioni possono poi essere utilizzate come segue: nella specifica viene ad esempio di come la User Interface deve comportarsi per quanto riguarda la gestione delle luci della cappa, viene quindi fornita una tabella (Tabella 21) di tutte le funzioni che questa deve essere in grado di garantire e come deve comportarsi durante l'esecuzione di ognuna di queste. Per semplicità di comprensione è riportata anche la rappresentazione stilizzata della UI (Figura 60).

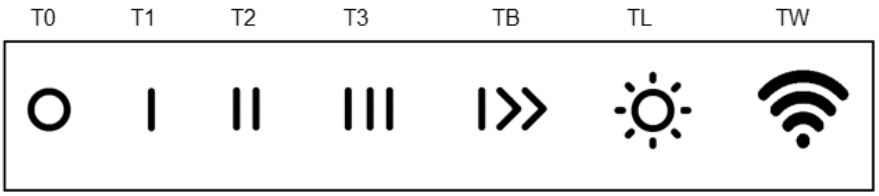


Figura 60 - User Interface

Funzione	Stato	Azione	Nuovo stato	Info UI
1	Luce principale OFF	Pressione corta TL	Luce principale ON	Bip buzzer corto TL ON
2	Luce principale ON	Pressione corta TL	Luce principale OFF	Bip buzzer corto TL OFF
3	Luce principale ON	Pressione lunga TL	Dimmer intensità luce principale	TL FAST PULSE
4	Luce principale OFF	Pressione lunga TL	/	/

Tabella 21 - Comando luci attraverso UI

La tabella sopra riportata (Tabella 11) mostra quindi come ogni comando rivolto alle luci eseguibile sulla User Interface debba essere interpretato. Per fornire maggiore chiarezza è possibile esaminare la "Funzione 1": si parte da uno stato iniziale in cui la luce della cappa è spenta; l'azione è l'operazione che l'utente esegue sulla UI (in questo caso premere con una pressione corta il pulsante TL) mentre il nuovo stato è la conseguenza dell'azione eseguita (ovvero si accende la luce); la UI segnala il cambiamento di stato quindi emette un bip breve dal buzzer ed accende il led al di sotto del pulsante TL a segnalare appunto sulla User Interface l'effettiva accensione della luce. [6]

La specifica tecnica deve fornire tutte le informazioni necessarie affinché il produttore possa rilasciare un hardware perfettamente integrabile nella piattaforma in questione, di conseguenza oltre a descrivere le funzioni legate alle luci deve anche contenere una descrizione dettagliata di come tutte queste operazioni si vadano a riflettere sulla comunicazione con le altre schede, ovvero 1-Wire bus. Ogni paragrafo contiene anche le variabili del protocollo interessate e i valori assumibili nelle varie situazioni e nel caso delle luci le grandezze sono due:

1. 0x60 Cooktop light intensity (Intensità della luce cappa sopra al piano);
2. 0x63 Cooktop light Command (Comandi ricolti alla luce cappa sopra al piano).

Nel momento in cui il comando è la semplice pressione del pulsante TL, ovvero accensione e spegnimento luce, le variabili assumono i seguenti valori (Tabella 22).

Messaggio inviato alla Main board	0x60	0x63
Accensione luce	0x64 (valore max)	(non trasmesso)
Spegnimento luce	0x00 (valore min)	(non trasmesso)

Tabella 22 - Comportamento variabili 0x60/0x63 caso accensione e spegnimento luci

Nel caso di semplice comando accensione/spegnimento l'unica variabile utilizzata è la 0x60, ovvero si va a settare l'intensità al valore massimo o al valore minimo. Operazioni più complesse come il dimmer (pressione prolungata di TL) vanno ad agire su entrambe le variabili, come riportato in tabella (Tabella 23).

Messaggio inviato alla Main board	0x60	0x63
Aumentare intensità	Aumenta	0x01
Ridurre intensità	Decresce	0x02

Tabella 23 - Comportamento variabili 0x60/0x63 caso dimmerazione luci

Il comando di dimmer va ad interagire direttamente sulle variabili 0x60 e 0x63: se l'intensità deve aumentare, quindi 0x63 = 0x01, il valore della 0x60 aumenta fino a raggiungere 0x64; se l'intensità deve diminuire, 0x63 = 0x02, il valore della 0x60 diminuisce fino ad azzerarsi. La ricezione corretta delle due variabili permette alla Main di andare a comandare i dimmer luci ed eseguire le operazioni richieste. [6]

5.1.2. Valutazione delle offerte

Per quanto riguarda la fase di valutazione delle offerte inizialmente le varie aziende hanno formulato proposte più o meno dettagliate e sulla base di queste si è deciso di contattare ed incontrare singolarmente ognuna di esse per definire gli eventuali dettagli. Ho avuto la possibilità di partecipare ad incontri con i rappresentanti e tecnici sia delle aziende interessate ma anche con i responsabili marketing di Elica. Da queste riunioni si è cercato di ottenere una quantità di informazioni tale da poter confrontare correttamente le varie offerte ricevute. Principalmente le specifiche richieste sono state le seguenti:

- Codice esatto core Wi-Fi. Nelle specifiche STF è infatti richiesto di utilizzare un modello prodotto da Espressif, la scelta finale è lasciata libera al produttore (scelta che naturalmente deve poi essere approvata da Elica);
- Codice esatto microprocessore. In questo caso non sono date specifiche particolari, ma si cerca di capire se il produttore ha già lavorato con quel particolare micro e che quindi sia in grado di garantire le funzionalità richieste;
- Dimensione finale PCB ed eventuali schemi o progetti 3D per permettere una valutazione del lavoro;
- Numero di release del PCB, ovvero quanti giri di layout sono previsti;
- Numero di campioni prodotti durante lo sviluppo e messi a disposizione ad Elica per eseguire test;
- Collaudo. Si è cercato di capire se i prodotti, prima di essere venduti, subiscano un processo di collaudo e che tipo di operazioni verranno eseguite.

Queste informazioni permettono di comprendere il livello di competenza del produttore per quanto riguarda prodotti di questo tipo. È molto importante valutare questo aspetto del fornitore, altrimenti si possono poi incontrare problemi e ritardi durante la produzione vera e propria. Oltre all'aspetto tecnico ci si è naturalmente concentrati sull'aspetto economico e logistico. È importante evidenziare come il costo del singolo pezzo non debba obbligatoriamente essere preso come riferimento discriminante per la scelta dato che ci sono tutta una serie di costi da valutare nel complesso prima di giungere alla soluzione. Più nel dettaglio, le informazioni richieste sono state:

- Valuta dei prezzi. È fondamentale allinearsi sulla valuta indicata, con il fine di evitare incomprensioni e disguidi finali;
- Prezzo. Ci si riferisce al costo del singolo pezzo (singola UI);
- Costi di sviluppo. Questa sezione dei costi generalmente comprende il costo umano (ore di lavoro), costi di analisi, progettazione, sviluppo firmware e costi di redazione della documentazione finale;
- Investimenti per gli stampi. Indicare se è richiesto l'utilizzo di stampi ed il loro costo;
- Costi per le attrezzature di produzione;
- Costi per le attrezzature di collaudo;
- MOQ: Minimum Order Quantity. Sta dunque ad indicare la quantità d'ordine minima che è necessario raggiungere per poter inoltrare la richiesta d'acquisto al fornitore. In parole povere, è la soglia sotto cui non è possibile scendere: solo raggiungendo e superando quella quantità il produttore riesce a coprire i costi legati a quel dato prodotto, e ad avere un guadagno;
- Termini di pagamento. Descrizione su come deve avvenire il pagamento, ad esempio una certa percentuale al momento dell'ordine ed il restante al termine della progettazione;
- Tempi di sviluppo. Per quanto riguarda l'aspetto dei tempi di sviluppo e di consegna sono emersi gli innumerevoli problemi associati alla crisi di componenti e di materiale che attualmente sta colpendo l'economia globale, si parla infatti di ritardi e tempi di consegna per i componenti attivi che raggiungono anche le 60 settimane, di conseguenza se un progetto deve partire il prossimo anno è necessario individuare i materiali necessari già da ora;
- Termini di consegna. Generalmente sono due: DAP ed EXW. DAP (Delivered At Place) è il gruppo delle massime obbligazioni per il venditore, il quale assume su di sé oneri e rischi di consegna fino a destinazione. EXW (EX Works) in cui le maggiori obbligazioni sono a carico del compratore.

Tutti questi parametri sono fondamentali per la scelta del fornitore, dato che ora tutte le offerte sono oggettivamente confrontabili. A questo punto è necessario valutare le informazioni ricevute, analizzandole nel complesso, ad esempio: se un fornitore propone un prezzo finale del singolo componente 1€ più basso di un altro, questo può sembrare un enorme risparmio su grandi numeri di acquisiti, ma si devono considerare eventuali costi di sviluppo: il fornitore meno caro potrebbe richiedere decine di migliaia di euro di sviluppo, il più caro invece può aver diviso costi sul pezzo senza richiedere nulla per lo sviluppo, di conseguenza le due offerte inizialmente diverse diventano molto simili e la scelta di uno dell'altro può dipendere dai volumi considerati, se molto alti può convenire pagare lo sviluppo a parte mentre se relativamente bassi il singolo euro in più su ogni scheda può risultare più conveniente. È molto importante anche non sovraccaricare un fornitore, con il fine di evitare ritardi di consegna legati alle troppe richieste, oltre naturalmente a cercare di diversificare i fornitori così da evitare il crearsi di dipendenze con un particolare produttore.

A valle di questi incontri si è definito il nuovo hardware che andrà a sostituire la soluzione attualmente in uso. La nuova board User Interface + Connectivity verrà infatti standardizzata ed utilizzata su una serie di prodotti che saranno lanciati nei prossimi anni. Questi elettrodomestici, dunque, condivideranno la scheda UI ma si differenzieranno per i codici firmware su di essi implementati, garantendo così differenti funzionalità.

5.2. Confronto tra la vecchia e la nuova UI

Dal punto di vista hardware la vecchia e la nuova board si differenziano nel fatto che tutti i componenti sono in una unica scheda invece che due, di conseguenza vengono meno alcuni connettori e cablature fino ad ora presenti. Interessante è invece confrontare il vecchio e nuovo hardware dal punto di vista economico. Uno dei punti principali è proprio il fattore costo, con l'intento dell'Azienda di muoversi sempre verso soluzioni che permettano di ridurre le spese di produzione. La combinazione di due schede infatti porta con sé i seguenti importi:

- 8.48 € Scheda User Interface;
- 12.00 € Assieme connettività: si tratta di un contenitore plastico con all'interno il modulo Wi-Fi ESP32. È compreso anche il connettore per il cablaggio sul bus di comunicazione.

Il tutto porta ad un costo di 20.48 €. I due componenti sono riportati di seguito (Figura 61).

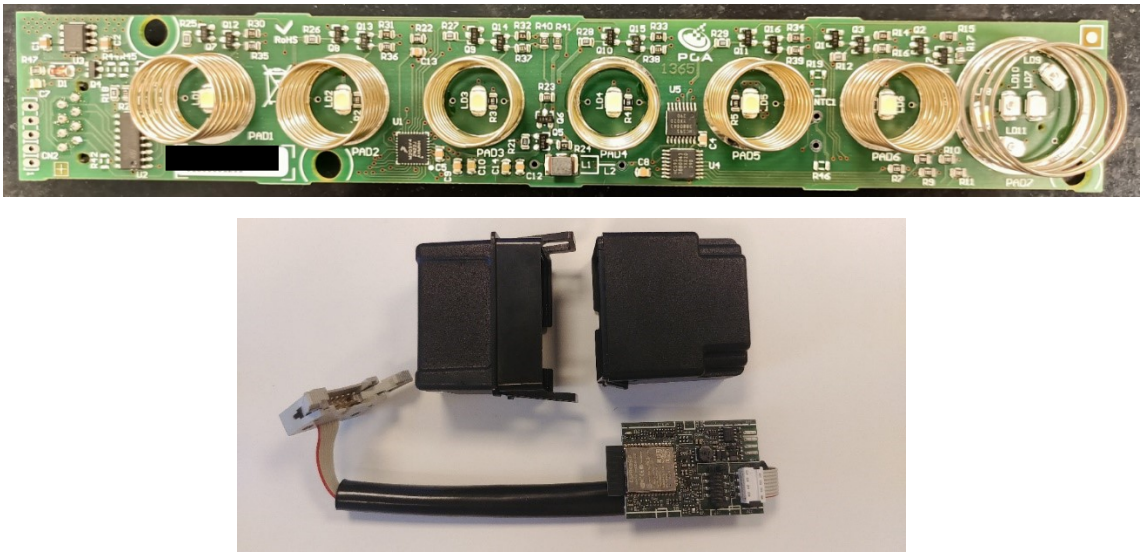


Figura 61 - User Interface e modulo Wi-Fi

Il nuovo prodotto invece ha un costo attualmente stimato di circa 9.85 €. Questa soluzione garantirebbe quindi un risparmio di 10.63 € e considerando la standardizzazione di questa board su una serie di modelli per un totale di 50 mila pezzi l'anno il risparmio può essere considerato notevole. Uno schematico 3D del nuovo hardware è qui riportato (Figura 62).

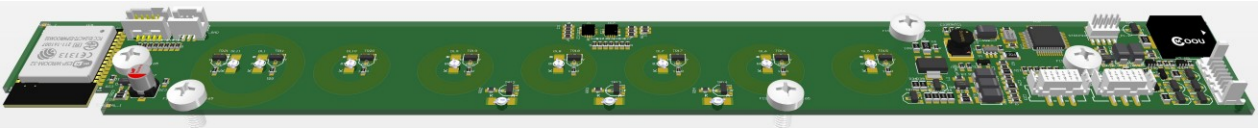


Figura 62 - CAD nuova User Interface con modulo Wi-Fi integrato

Questa soluzione, oltre a garantire un risparmio economico rilevante, viene accompagnata da una semplificazione nel processo di registrazione della cappa sull'App Elica Connect. Al momento uno schematico dei passaggi principali (si rimanda al capitolo 3 per una descrizione più dettagliata) è il seguente (Figura 63):

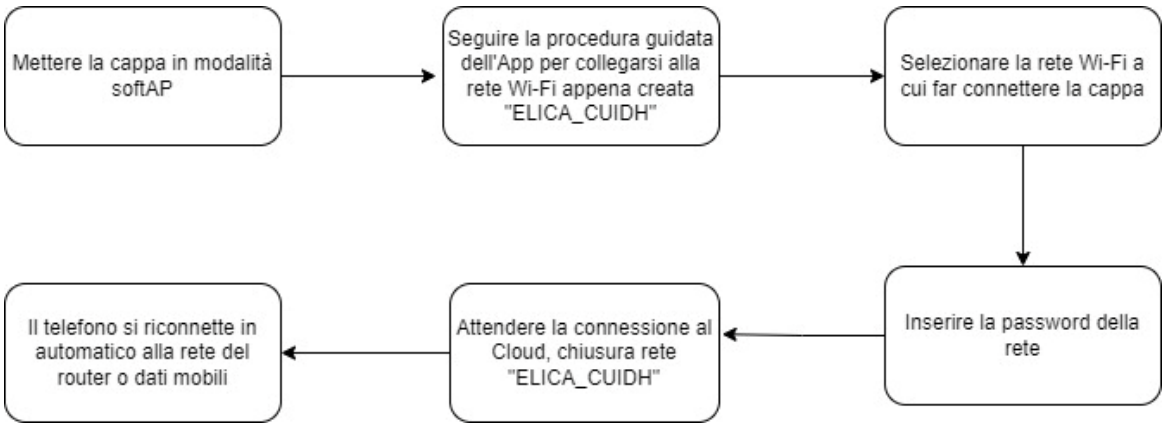


Figura 63 - Diagramma procedura di On-boarding dispositivo su App

Dallo schema appena riportato è possibile evidenziare alcuni aspetti che l'utilizzo della tecnologia Bluetooth potrebbe migliorare ed ottimizzare. In ordine di esecuzione la prima operazione da compiere è mettere la cappa in modalità SoftAP andando ad interagire con il prodotto stesso (User Interface) o utilizzando il telecomando. Questa modalità deve essere attivata manualmente perché di base il modulo Wi-Fi è spento dato che il prodotto, se non connesso al router di casa (quindi non sta garantendo particolari funzionalità di controllo remoto), deve rispettare dei vincoli normativi che fissano il consumo energetico dell'elettrodomestico in stand-by a 0.5W. Senza il rispetto di questa condizione il prodotto non può essere venduto. Tuttavia, un core Wi-Fi sempre attivo comporterebbe il superamento di questo limite e proprio per questo la sua accensione avviene manualmente e solo in caso di effettivo utilizzo.

Il secondo passaggio invece richiede di disconnettersi dalla rete Wi-Fi a cui si è connessi (o dati mobili) per collegarsi alla rete aperta dal modulo. Nonostante alla fine della procedura i dispositivi mobili siano in grado di ricollegarsi autonomamente alla rete Wi-Fi a cui erano inizialmente connessi (o dati mobili), per tutta il processo di On-Boarding il telefono è scollegato da internet. Come anticipato il Bluetooth può andare ad ottimizzare queste due operazioni: nel primo caso si potrebbe pensare di lasciare il BLE sempre attivo ed il Wi-Fi spento, poi nel momento in cui un dispositivo si collega tramite Bluetooth alla cappa si accende anche l'access point del modulo. Questa soluzione, tuttavia, per essere implementata richiede test sul consumo in stand-by; come riportato in precedenza infatti si ha un limite da rispettare ed è necessario testare se i consumi di un dispositivo Bluetooth Low Energy siano tali da rimanere sottosoglia. Per quanto riguarda l'ESP32 è possibile prendere come riferimento i seguenti valori (Tabella 24):

Modalità	Consumi
Wi-Fi in Tx, potenza trasmessa: 13-24 dBm	160 ÷ 260 mA
Wi-Fi/BT in Tx, potenza trasmessa: 0 dBm	120 mA
Wi-Fi/BT in Rx	80 ÷ 90 mA

Tabella 24 - Consumi ESP32

Di base Wi-Fi e Bluetooth comportano quindi consumi molto simili e che portano il totale oltre la soglia, ma per quanto riguarda il Bluetooth Low Energy i consumi sono invece circa la metà di quelli del Bluetooth standard, quindi 40 ÷ 45 mA. Test futuri in laboratorio forniranno una risposta sulla effettiva implementazione della soluzione. Se non risulterà implementabile sarà necessario mantenere l'interazione fisica con la cappa per avviare il processo di on-boarding.

Per quanto riguarda il secondo passaggio il BLE permetterebbe di comunicare con la cappa senza dover scollegare il proprio smartphone dalla rete internet. Nonostante BLE e Wi-Fi utilizzino la stessa banda ISM tra loro non c'è interferenza. Questo è possibile perché durante una comunicazione BLE si cambia in continuazione il canale occupato: la banda a 2.4 GHz è infatti divisa in 36 canali e questi vengono periodicamente controllati, in questo modo da creare una mappatura dei canali in cui è indicata la qualità del canale stesso (1 canale utilizzabile, 0 canale bloccato) e sulla base di questa si sceglie il successivo intervallo di frequenze su cui comunicare. La mappatura viene fatta dal Master della comunicazione ed è poi aggiornata con il dispositivo slave. La mappatura disponibile viene utilizzata nel seguente modo: i due terminali della comunicazione condividono un algoritmo, il CSA (Channel Selection Algorithm, Figura 64), utilizzato per definire di volta in volta il successivo canale di comunicazione. Dato che i parametri dell'algoritmo sono gli stessi i dispositivi troveranno sempre lo stesso canale al termine di ogni calcolo. Trovato un nuovo indice lo si va a valutare sulla mappatura condivisa per poter capire se il canale ha una buona qualità o meno: in caso positivo si avvia la comunicazione, altrimenti se ne calcola un altro e si ripete la procedura.

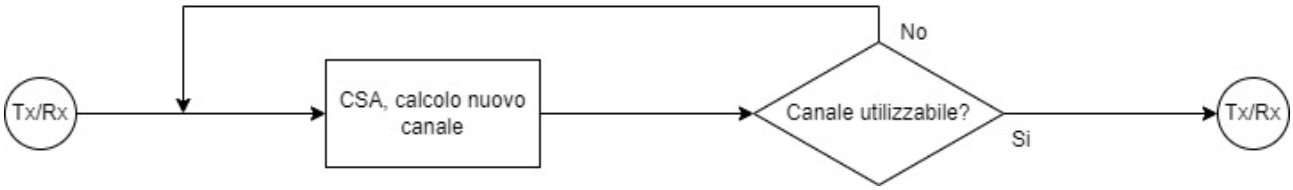


Figura 64 - Diagramma CSA

Il BLE permette quindi di comunicare con la cappa senza doversi scollegare da internet, rendendo quindi la procedura molto più semplice per l'utente. Il diagramma a blocchi finale, con riferimento ad entrambe le modifiche appena descritte, è il seguente (Figura 65).

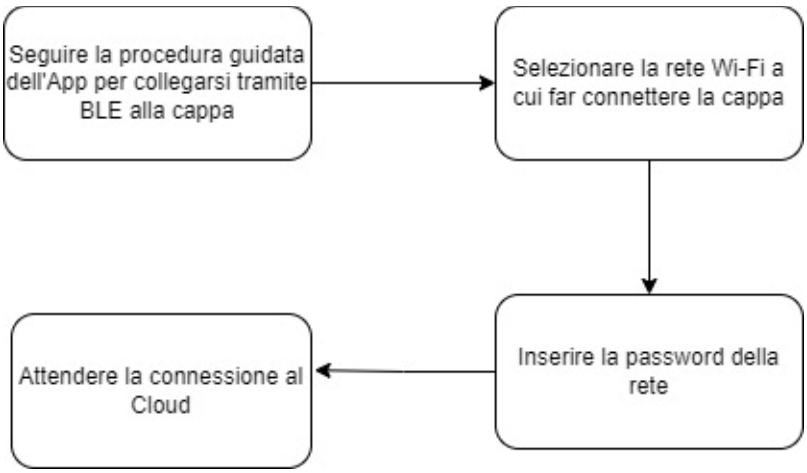


Figura 65 - Nuovo diagramma procedura di On-boarding dispositivo su App

Il risultato è una procedura molto più semplice ed immediata, con un numero di interazioni richieste all'utente molto inferiore.

Al momento è in valutazione la possibilità di trasferire in automatico anche la password Wi-Fi della rete selezionata, quindi saltare la fase di inserimento della chiave della rete, se questa memorizzata nel dispositivo. Questa operazione semplificherebbe ancora di più la procedura di registrazione dato che richiederebbe all'utente una singola interazione durante tutto il processo (basterebbe solo selezionare la rete a cui far collegare il dispositivo) ma è necessario valutare la realizzabilità di questa soluzione, soprattutto dal punto di vista della sicurezza perché l'applicazione Elica Connect dovrebbe essere in grado di accedere alle password salvate nello smartphone, dato ritenuto sensibile.

Viene data molta importanza a processo di registrazione di un nuovo prodotto nell'App Elica Connect perché questo passaggio rappresenta la prima vera interazione con un prodotto connesso e con l'App stessa, il primo "scoglio" da superare. Da come questa procedura è implementata derivano tutti i feedback e le recensioni sullo store dell'App ma più in generale influenza l'idea che il consumatore si fa del prodotto: una serie di step confusionari o complicati può mettere in difficoltà la persona meno esperta e renderebbe l'utilizzo smart vincolato a pochi. L'user experience è uno dei punti cardini di Elica, adattare design ed usabilità è alla base di ogni progetto e qualunque evoluzione tecnologica deve andare a migliorare ed ottimizzare questi aspetti.

5.3. Implementazione della tecnologia scelta

All'interno di questo paragrafo viene descritta una possibile implementazione Bluetooth Low Energy all'interno dei prodotti connessi Elica.

Smartphone e cappa ricoprono rispettivamente il ruolo di Master e Slave (è l'App che stabilisce la connessione) ma nello scambio di informazioni è la cappa a ricoprire il ruolo di Server; quindi, è necessario programmare il modulo Wi-Fi ESP32 affinché contenga al suo interno le caratteristiche da poter modificare durante la comunicazione. Si costruisce la GATT (Generic ATTribute, Figura 66) ovvero la struttura gerarchica che verrà esposta al dispositivo slave connesso. Si definiscono il profilo, il servizio e quattro caratteristiche: l'SSID rete, la password rete (entrambe in modalità solo scrittura), la lista delle reti Wi-Fi che l'ESP32 rileva ed a cui può connettersi ed infine una variabile "Stato" che sarà utilizzata per monitorare lo stato di avanzamento della connessione al Cloud del prodotto. Le ultime due caratteristiche sono in modalità sola lettura.

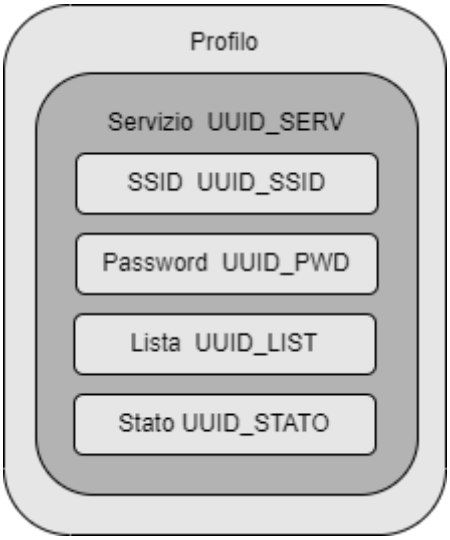


Figura 66 - GATT utilizzato

Lo smartphone, utilizzando l'App Elica Connect, si comporta da Master: inizia la fase di discovery, rileva lo Slave e si instaura la connessione; a questo punto comunicando con la cappa legge il valore della terza caratteristica (lista SSID a cui l'ESP può connettersi) e con una serie di passaggi invia SSID e password della rete Wi-Fi alla cappa affinché quest'ultima possa connettersi al router di casa. A queste tre caratteristiche se ne aggiunge una quarta che permette all'App di monitorare lo stato del modulo Wi-Fi, in modo tale da aggiornare l'applicazione per segnalare lo stato in cui l'elettrodomestico si trova (l'utilizzo di questa variabile sarà più chiaro nelle righe successive). Le quattro caratteristiche ed il servizio che le contiene sono identificati da un codice UUID univoco (Tabella 25), e sono questi codici che vengono utilizzati per eseguire le operazioni di lettura e scrittura.

	Codice UUID
Servizio	UUID_SERV
SSID	UUID_SSID
Password	UUID_PWD
Lista	UUID_LIST
Stato	UUID_STATO

Tabella 25 - UUID utilizzati

L'applicazione Elica Connect una volta stabilita la connessione BLE con la cappa presenterà una procedura guidata per trasmettere le credenziali richieste: la prima schermata riporta una lista delle reti rilevate dal modulo Wi-Fi (la lista è ottenuta andando a leggere la terza caratteristica nel GATT, ovvero la caratteristica con UUID = UUID_LIST contenuta nel service con UUID = UUID_SERV) e l'utente seleziona la "SSID" a cui far connettere la cappa; segue poi una seconda schermata in cui viene richiesto di inserire la "Password" della rete appena selezionata all'interno di una casella testuale. La pressione del bottone "Next" avvia la trasmissione tra smartphone e cappa ed i dati inseriti vengono scritti all'interno della corrispondete caratteristica grazie ai codici UUID. Per esempio:

- "SSID" selezionato viene scritto come valore della caratteristica con UUID = UUID_SSID contenuta nel servizio con UUID = UUID_SERV;
- "Password" viene scritta come valore della caratteristica con UUID = UUID_PWD contenuta nel servizio con UUID = UUID_SERV.

Il firmware all'interno del core Wi-Fi è in grado di rilevare la scrittura delle caratteristiche ed utilizza i parametri inseriti per collegarsi ad internet e successivamente al broker MQTT. Se questa operazione avviene con successo il core sarà in grado di iscriversi ai topic del broker.

Nell'intervallo temporale richiesto dal modulo per collegarsi ad internet e poi accedere al Cloud l'utente deve aver modo di poter monitorare l'avanzamento delle operazioni, proprio per questo è stata implementata una quarta caratteristica che viene aggiornata dal firmware contenuto nel modulo in base allo stato in cui quest'ultimo si trova: lo stato di partenza è "Disconnesso", quindi non collegato ad una rete Wi-Fi; una volta trasferite la credenziali di accesso la caratteristica contiene il valore "Connessione al router" e mantiene tale valore fino allo stato "Connesso al router", i passi successivi saranno "Connessione al Cloud" e "Connesso al Cloud". La possibilità di avere queste informazioni permette all'App di andare a mostrare all'utente una diversa grafica in base allo stato, cosicché la procedura guidata possa essere resa il più dinamica possibile, evitando lunghe attese senza feedback.

La lettura del valore "Connesso al Cloud" permette all'App di andare ad interagire con il Cloud stesso per completare l'operazione di on-boarding: inserimento nome del prodotto, filtri e tipo di installazione. Il funzionamento successivo dell'applicazione segue poi quanto attualmente implementato.

5.4. Test e simulazione

Il test non può essere provato direttamente con i prodotti finiti dato che l'applicazione viene sviluppata esternamente ed i tempi di rilascio sono al momento fissati per Gennaio 2023 mentre la nuova board User Interface + Wi-Fi non è ancora in produzione; tuttavia, è possibile effettuare delle simulazioni in grado di controllare il corretto funzionamento e l'effettiva fattibilità di questa soluzione.

5.4.1. Sviluppo del codice per l'ESP32

L'obiettivo della simulazione è andare a replicare il processo di on-boarding dell'elettrodomestico sull'App, quindi, si devono andare a trasmettere alla cappa il nome della rete Wi-Fi a cui connettersi e relativa password tramite BLE ed utilizzare queste credenziali per connettersi ad internet; da questo punto il processo che segue è lo stesso identico già implementato nei prodotti attualmente in commercio. Per effettuare questa simulazione è necessario programmare un modulo ESP32 e sviluppare un'App per smartphone in grado di rilevare i dispositivi BLE nelle vicinanze, connettersi e trasmettere le credenziali, praticamente il processo di registrazione nell'App Elica Connect vero e proprio. Come slave della comunicazione BLE si utilizza una scheda di sviluppo D1 R32 ESP32 CH340G (Figura 67) compatibile con Arduino IDE. La board della Az-Delivery monta un ESP32-WROOM-32 con Wi-Fi e Bluetooth e può essere programmato utilizzando il linguaggio C++.

Figura 67 - D1 R32 ESP32 CH240G

Il codice da caricare sulla scheda si basa sulle seguenti librerie del Wi-Fi e del Bluetooth:

1. WiFi.h, abilita la connessione di rete (locale o ethernet) tramite una scheda compatibile Arduino. Con questa libreria si possono istanziare Server o Client e ricevere/trasmettere pacchetti UDP. È possibile connettersi sia a reti aperte che reti crittografate tramite WPA2. Una volta connesso il modulo può ricevere un indirizzo IP assegnato in modo statico o tramite DHCP. Contiene anche una libreria interna per gestire i DNS;
2. BLEDevice.h, permette di definire alcuni parametri funzionali al BLE come, ad esempio, il nome del device così da renderlo riconoscibile ad un utente che sta effettuando una ricerca dei dispositivi Bluetooth vicini;
3. BLEUtils.h, permette di andare a costruire e definire il GATT, ovvero definizione del Servizio e delle Caratteristiche;
4. BLEServer.h, permette di gestire e caratterizzare il modulo come un server BLE.

Ognuna di queste mette a disposizione dei metodi che saranno poi utilizzati nelle successive righe di codice.

La prima operazione consiste nella configurazione del GATT che sarà esposto ai dispostivi connessi: si definisce l'UUID dell'unico servizio abilitato e gli UUID delle quattro caratteristiche necessarie: SSID,

password, lista reti Wi-Fi rilevate dall'ESP32 e stato (Figura 68). Le caratteristiche vengono poi settate in modalità scrittura o lettura (in base al loro utilizzo, in accordo con i paragrafi precedenti).

```
BLECharacteristic pCharacteristic1(CHARACTERISTIC_UUID1,BLECharacteristic::PROPERTY_WRITE);
BLECharacteristic pCharacteristic2(CHARACTERISTIC_UUID2,BLECharacteristic::PROPERTY_WRITE);
BLECharacteristic pCharacteristic3(CHARACTERISTIC_UUID3,BLECharacteristic::PROPERTY_READ);
BLECharacteristic pCharacteristic4(CHARACTERISTIC_UUID1,BLECharacteristic::PROPERTY_READ);
```

Figura 68 - Assegnazione UUID e proprietà alle caratteristiche

Il successivo passaggio contiene il settaggio di un valore iniziale alle varie caratteristiche, "SSID" e "Password" sono settate come variabili vuote, senza valore, la caratteristica Lista assume il valore del vettore descritto in precedenza mentre la caratteristica "Stato" parte dal valore "Disconnesso" (Figura 69).

```
BLEDevice::init("Elica_XXXX"); //Device name

BLEServer *pServer = BLEDevice::createServer();
BLEService *pService = pServer->createService(SERVICE_UUID);

pService->addCharacteristic(&pCharacteristic1);
pCharacteristic1.setValue("");

pService->addCharacteristic(&pCharacteristic2);
pCharacteristic2.setValue("");

pService->addCharacteristic(&pCharacteristic3);
pCharacteristic3.setValue("Lista");

pService->addCharacteristic(&pCharacteristic4);
pCharacteristic4.setValue("Disconnesso");
```

Figura 69 - Assegnazione valori iniziali alle caratteristiche

A questo punto viene inizializzata la fase di advertising ed il dispositivo slave resta in attesa della connessione con un device master. Nel momento in cui uno smartphone si connette la prima operazione che viene eseguita è una scansione delle reti Wi-Fi presenti nell'ambiente circostante. Questa operazione, come riportato nell'immagine (Figura 70) può essere eseguita utilizzando un semplice metodo WiFi.scanNetworks(), funzione che restituisce il numero delle reti trovate e memorizza le seguenti informazioni: SSID rilevate, l'elenco di tutti i valori di RSSI ed infine il tipo di protocollo di sicurezza utilizzato. In figura sono presenti anche tutti i comandi e metodi utilizzati per leggere e stampare a schermo la seriale della board, inseriti per fare debug.

```
  int n = WiFi.scanNetworks();
Serial.println(F("Scansione WiFi eseguita"));
if (n == 0) {
    Serial.println(F("no networks"));
} else {
  Serial.print(n);
  Serial.println(F(" networks found"));
  for (int i = 0; i < n; ++i) {
    // Print SSID e RSSI
    Serial.print(i + 1);
    Serial.print(": ");
    Serial.print(WiFi.SSID(i));
    Serial.print(" (");
    Serial.print(WiFi.RSSI(i));
    Serial.print(")");
    Serial.println((WiFi.encryptionType(i) == WIFI_AUTH_OPEN)?" ":"*");
    delay(10);
  }
}
```

Figura 70 - Codice scansione Wi-Fi

Metodi come WiFi.SSID(), Wi-Fi.RSSI(), WiFi.encryptionType() sono funzioni che permettono di ottenere una particolare informazione dell'i-esima rete rilevata in precedenza così da poter stampare su seriale tutte le informazioni necessarie. Le informazioni ottenute da questi metodi sono poi utilizzate per andare a creare una stringa da inserire nella caratteristica "Lista" (Figura 68), stringa costruita con la seguente logica:

Lista = [SSID_1, RSSI_1, ENCR_1, SSID_2, RSSI_2, ENCR_2, SSID_3, RSSI_3, ENCR_3, …]

In cui RSSI_i è l'SSID dell'i-esima rete, RSSI_i è il valore di RSSI ed infine ENCR_i è tipo di sicurezza implementato (se rete aperta o protetta con WPA2 ad esempio). L'applicazione, leggendo la caratteristica e conoscendo la logica con il quale la stringa è composta, sarà in grado di ricostruire correttamente un'interfaccia grafica in grado di mostrare tutte le informazioni necessarie all'utente: SSID, qualità del segnale ed eventuale lucchetto per segnalare la sicurezza della rete.

Il funzionamento del codice durante il normale utilizzo può essere rappresentato dal diagramma a blocchi riportato in figura(Figura 72). Dopo una prima preparazione ed avvio del BLE il codice attende la connessione di un device esterno. Appena connesso il codice esegue una scansione delle reti Wi-Fi vicine, compila la stringa e la rende disponibile al master tramite la caratteristica "Lista"; poi opera un continuo controllo della caratteristica SSID in attesa che il valore nullo inizialmente settato venga modificato da una scrittura esterna. Una volta ricevuto una grandezza dall'esterno viene effettuata una verifica sulla sicurezza della rete, ovvero se questa è una rete aperta o privata: nel primo caso si procede subito alla connessione, altrimenti si attende la ricezione della password ed una volta ottenuti tutti i parametri necessari si procede alla connessione al router. Nelle righe di codice che seguono (Figura 71) è riportato il caso della connessione ad una rete privata: alla funzione WiFi.begin sono passati l'SSID (NTWK) e la password (PWD) della rete a cui il modulo deve connettersi (se la rete fosse stata aperta sarebbe stato necessario un solo parametro: NTWK). Le credenziali sono a loro volta ottenute dalla lettura delle caratteristiche SSID e Password.

```
WiFi.begin(NTWK, PWD);
pCharacteristic4.setValue("Connessione al Router");
```

Figura 71 - Codice per la connessione al router

È durante questa fase che la caratteristica "Stato" viene aggiornata: inizialmente, appena passati i parametri, il valore è fissato a "Connessione al router" e se questa avviene con successo si passa allo stato "Connesso al router" ed il codice termina, altrimenti rimuove i valori delle caratteristiche SSID e Password, imposta lo stato come "Connessione fallita" e resetta il modulo, facendo ripartire il codice da capo.

È importare evidenziare che, a causa di alcuni vincoli di risorse e di autorizzazioni, la prova non è in grado di emulare perfettamente tutto il processo di registrazione del prodotto in App: nel caso in questione, infatti, il firmware installato nell'ESP32 arriva allo stato "Connesso al router", vista l'impossibilità di gestire un codice in grado di emulare correttamente quello installato in una cappa. In generale è possibile affermare che il processo più complesso e che doveva essere rivisto è il passaggio delle credenziali per la connessione al router di casa, tutto il resto dell'architettura è da considerarsi stabile e va mantenuto.

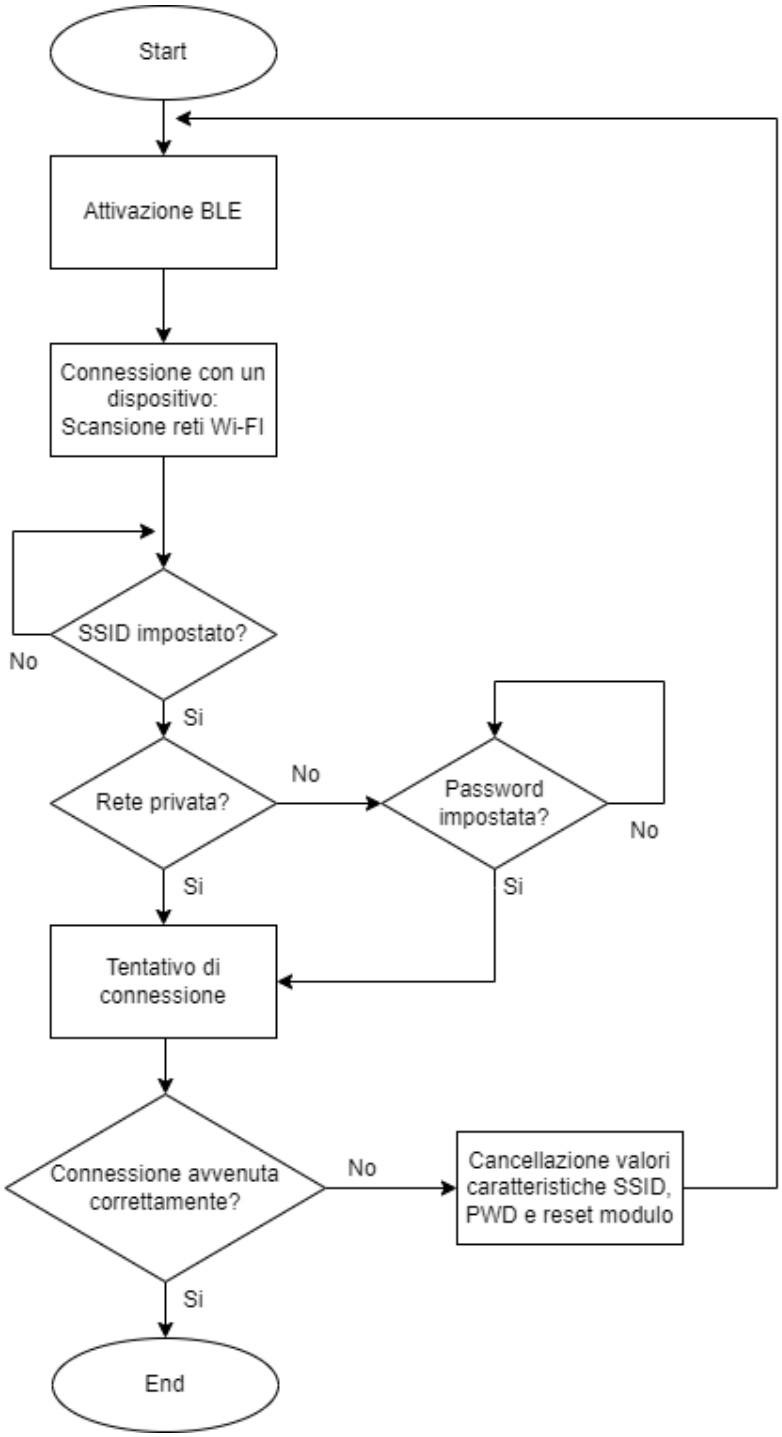


Figura 72 - Diagramma codice modulo ESP32

5.4.2. Sviluppo app Android

L'App per smartphone è stata scritta utilizzando il software messo a disposizione da Android stesso, Android Studio, con il quale si può costruire il file apk da installare nel device mobile. Il linguaggio utilizzato è il Java e l'applicazione sviluppata permette di simulare i vari passaggi del processo di on-boarding.

Per prima cosa l'applicazione permette di connettersi ad un altro dispositivo BLE nelle vicinanze, per questo la prima schermata (Figura 73) presenta a schermo il tasto "Inizia scansione" che permette di identificare e

riportare su schermo i vari device rilevati (Figura 74) ed ai quali è poi possibile connettersi utilizzando il tasto “Con” (diminutivo di “Connetti”).

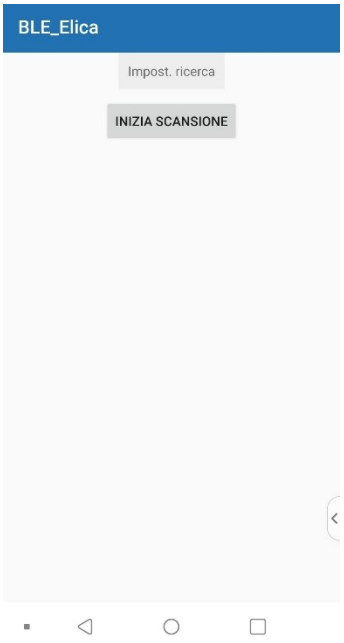


Figura 73 - Prima schermata

Figura 74 - Lista BLE rilevati

Una volta connesso ad un dispositivo slave l’app è in grado di elencare i servizi disponibili e le relative caratteristiche, indicando per ognuno i rispettivi codici UUID e se la caratteristica è in modalità lettura o scrittura. Di seguito (Figura 75) sono riportate le quattro caratteristiche contenute nel GATT con i relativi UUID. Cliccando su una delle caratteristiche, in base alla modalità impostata, sarà possibile leggere o scrivere il valore.

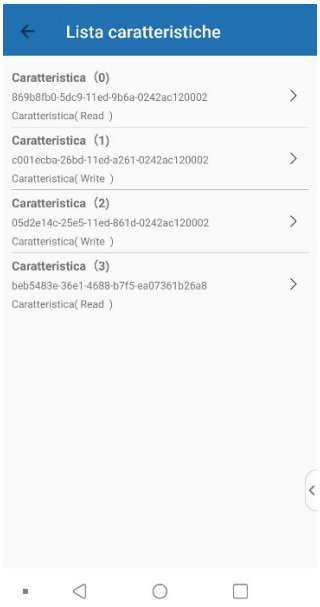


Figura 75 - Lista caratteristiche

La schermata appena riportata (Figura 75) è costruita su una base di informazioni ottenute dalla lettura del GATT costruito nel BLE Service. Tali dati sono ottenuti tramite una serie di metodi get(), come riportato di seguito (Figura 76). Per prima cosa si va a rilevare l’indice della caratteristica, ovvero la sua posizione nel GATT, e si ottiene un valore incrementale che in questo caso va da 0 a 3 (4 caratteristiche); poi si ricava il

codice UUID identificativo della caratteristica attraverso il metodo getUuid() e le due informazioni appena ottenute sono organizzate per andare a formare l'interfaccia. Il passaggio successivo è formulare l'elenco delle proprietà associate alla caratteristica e per fare ciò si costruisce una stringa che conterrà il testo "Read", "Write" o "Read, Write" a seconda della modalità di lettura/scrittura. Queste informazioni appena ottenute vengono riportate a schermo (prestando attenzione a rimuovere eventuali virgole in eccesso) e se la lunghezza di questa stringa appena formata è maggiore di zero significa che si può interagire con tale caratteristica (scrivendo o leggendo un valore) quindi l'immagine della freccia posizionata sulla destra della schermata viene resa visibile a segnalare appunto la possibile interazione, altrimenti è invisibile. La presenza di una modalità di interazione permette inoltre di passare ad un'altra schermata in corrisponde della pressione su una caratteristica dell'elenco, schermate descritte nelle righe successive.

```
BluetoothGattCharacteristic characteristic = characteristicList.get(position);
String uuid = characteristic.getUuid().toString();

holder.txt_title.setText(String.valueOf("Caratteristica" + " (" + position + ")"));
holder.txt_uuid.setText(uuid);

StringBuilder property = new StringBuilder();
int charaProp = characteristic.getProperties();
if ((charaProp & BluetoothGattCharacteristic.PROPERTY_READ) > 0) {
    property.append("Read");
    property.append(" , ");
}
if ((charaProp & BluetoothGattCharacteristic.PROPERTY_WRITE) > 0) {
    property.append("Write");
    property.append(" , ");
}
if (property.length() > 1) {
    property.delete(property.length() - 2, property.length() - 1);
}
if (property.length() > 0) {
    holder.txt_type.setText(String.valueOf("Caratteristica" + "( " + property.toString() + ")"));
    holder.img_next.setVisibility(View.VISIBLE);
} else {
    holder.img_next.setVisibility(View.INVISIBLE);
}
```

Figura 76 - Organizzazione informazioni schermata 75

Cliccando su una delle caratteristiche quindi, se in modalità lettura, la pressione su di essa porta ad una schermata in cui è presente il bottone "Leggi". La pressione del pulsante fa apparire a schermo l'attuale valore della caratteristica selezionata. La lettura (o la scrittura) avviene grazie alla conoscenza degli UUID della caratteristica in questione e del relativo servizio che la contiene. Il codice di seguito riportato (Figura 77) mostra come il codice dell'applicazione, per poter leggere il valore, debba ottenere le seguenti informazioni: il dispositivo BLE su cui leggere le informazioni, la stringa dell'UUID del servizio che le contiene e la stringa dell'UUID della caratteristica stessa. Gli oggetti "bleDevice" e "characteristic" rappresentano rispettivamente il dispositivo a cui si è connessi e la caratteristica selezionata dalla lista della schermata precedente mentre i metodi utilizzati permettono di ottenere gli UUID interessati sotto forma di stringa. Seguono poi una serie di istruzioni per tradurre il binario letto in una stringa e poterla mostrare a schermo.

Per semplificare l'implementazione dell'App di simulazione l'SSID non è scelta da una lista, ma come per la password va inserita in un campo di testo ed inviata.

```java
@Override
public void onClick(View view) {
    BleManager.getInstance().read(
            bleDevice,
            characteristic.getService().getUuid().toString(),
            characteristic.getUuid().toString(),
            new BleReadCallback() {

                @Override
                public void onReadSuccess(final byte[] data) {
                    final String str1 = new String(data);
                    runOnUiThread(new Runnable() {
                        @Override
                        public void run() {
                            addText(txt, str1);

                        }
                    });
                }
```

Figura 77 - Codice lettura caratteristica

Nella figura che segue (Figura 78) è riportato un esempio di lettura della caratteristica “Stato” ed è visibile come il suo valore cambi durante la connessione del modulo al Wi-Fi. La lettura viene fatta manualmente, cliccando ogni volta il tasto “Leggi”, ma nella versione finale questa lettura avverrà attraverso una fase di polling ed il valore letto permetterà di cambiare la schermata con il fine di dare un feedback all’utente.

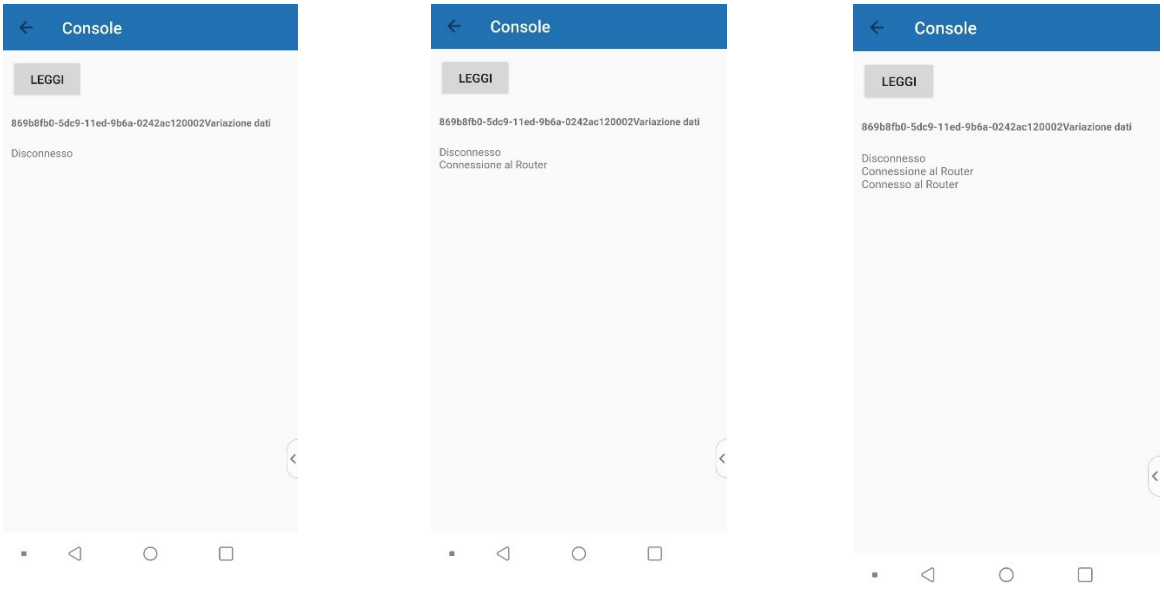


Figura 78 - Lettura caratteristica "Stato"

Se in modalità scrittura, la schermata (Figura 80) presenta una casella di testo in cui inserire l’informazione da trasmettere ed il bottone “Invia” avvia la comunicazione così da modificare il valore della caratteristica sul GATT dello slave. La figura sotto riportata (Figura 79) mostra il codice eseguito in seguito alla pressione del tasto “Invia” presente sulla schermata (Figura 80). Si ha una prima fase in cui si legge il contenuto della casella di testo presente a schermo e la si traduce in una stringa binaria, poi come nel caso della lettura si ottengono tutti gli UUID necessari alla trasmissione e si scrive il nuovo valore della caratteristica. A schermo dell’applicazione, a conferma della corretta scrittura, viene riportato il valore appena scritto.

```java
@Override
public void onClick(View view) {
    String data = et.getText().toString();
    byte[] dataByte = data.getBytes();
    if (TextUtils.isEmpty(data)) {
        return;
    }
    BleManager.getInstance().write(
            bleDevice,
            characteristic.getService().getUuid().toString(),
            characteristic.getUuid().toString(),
            dataByte,
            new BleWriteCallback() {

                @Override
                public void onWriteSuccess(final int current, final int total, final byte[] justWrite) {
                    runOnUiThread(new Runnable() {
                        @Override
                        public void run() {
                            addText(txt,  content: " justWrite: " + justWrite);
                        }
                    });
                }
```

Figura 79 - Codice scrittura variabile

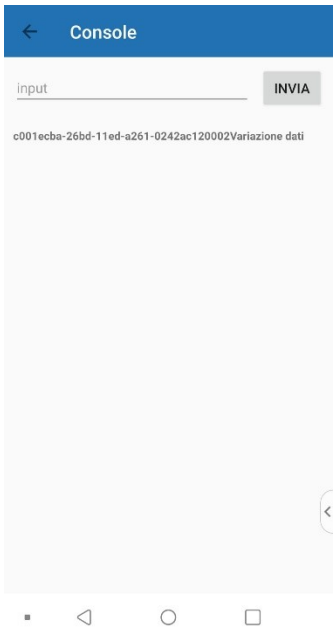


Figura 80 - Schermata scrittura variabile

Naturalmente questa implementazione è solo per il test e non rappresenta in maniera fedele quella in sviluppo dall'azienda esterna che sarà poi pubblicata sullo store; le principali differenze saranno dal punto da vista grafico, con schermate appositamente progettate da risultare semplici ed intuitive.

5.4.2.1. Versione ufficiale dell'App Android

Nella versione ufficiale, infatti, l'App sarà in grado di collegarsi in maniera autonoma al corretto device Bluetooth grazie alla scansione del codice QR presente nell'etichetta caratteristica del prodotto. Tramite questa scansione, infatti, l'App riesce ad entrare in possesso del codice CUID e MAC (in realtà si ottiene anche un ulteriore campo, REV, che permette di distinguere i vari prodotti ed avviare la procedura di connessine alla cappa effettivamente implementata: BLE o SoftAP, necessario per garantire retrocompatibilità dell'applicazione). Con queste informazioni sarà poi possibile collegarsi al device corretto, riconoscibile dal nome ELICA_CUIDH (CUIDH sono le prime quattro cifre del CUID, codice che l'App conosce attraverso la scansione del QR caratteristico. Figura 81), ma sarà poi anche in grado di interagire con il prodotto corretto passando attraverso il Cloud. Il processo appena descritto coincide con quanto attualmente implementato, a meno dello standard di comunicazione utilizzato per collegarsi alla cappa e passare i parametri della rete di casa. L'App, una volta collegata, è in grado di leggere le caratteristiche e fornire all'utente una interfaccia grafica tale da semplificare al massimo l'interazione con la cappa. Nel dettaglio, una volta connessa all'elettrodomestico, leggendo la caratteristica "Lista" l'App sarà in grado di generare una schermata (Figura 82) in cui saranno riportate tutte le reti con la relativa qualità del segnale; selezionandone una e cliccando su "Next" se aperta si passa subito alla trasmissione del valore altrimenti alla schermata per la richiesta della password (Figura 83). La pressione del tasto "Next" trasmette i parametri al modulo BLE installato nella cappa, scrivendoli rispettivamente nelle caratteristiche "SSID" e "Password".

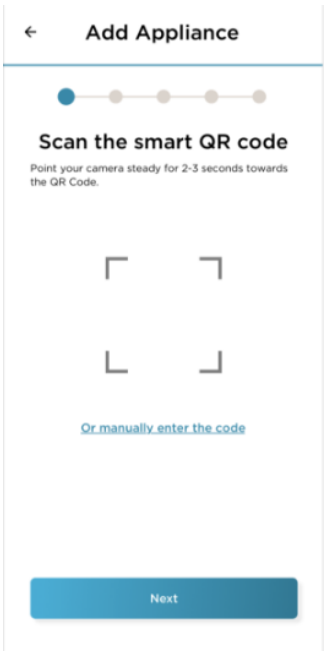


Figura 81 - Scan QR code

Figura 82 - Lista reti Wi-Fi

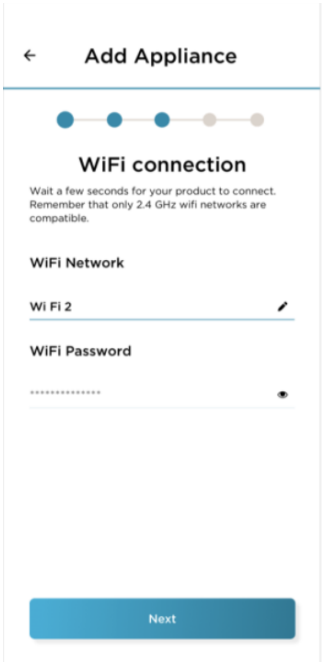


Figura 83 - Inserimento password

A questo punto l'App inizia a controllare il valore della caratteristica "Stato", mostrando le seguenti schermate (Figura 84) per rappresentare l'avanzare della connessione: "Connessione al router", "Connesso al router" e "Connessione al Cloud". "Connesso al Cloud" non viene visualizzato, ma l'App fornirà le schermate per inserire altri parametri funzionali all'installazione (es. modalità di installazione, filtri, nickname), proseguendo la procedura di registrazione del prodotto. Questi ultimi parametri vengono forniti al Cloud e non alla cappa; quindi, in questa fase finale, la connessione con l'elettrodomestico si interrompe perché non più necessaria.

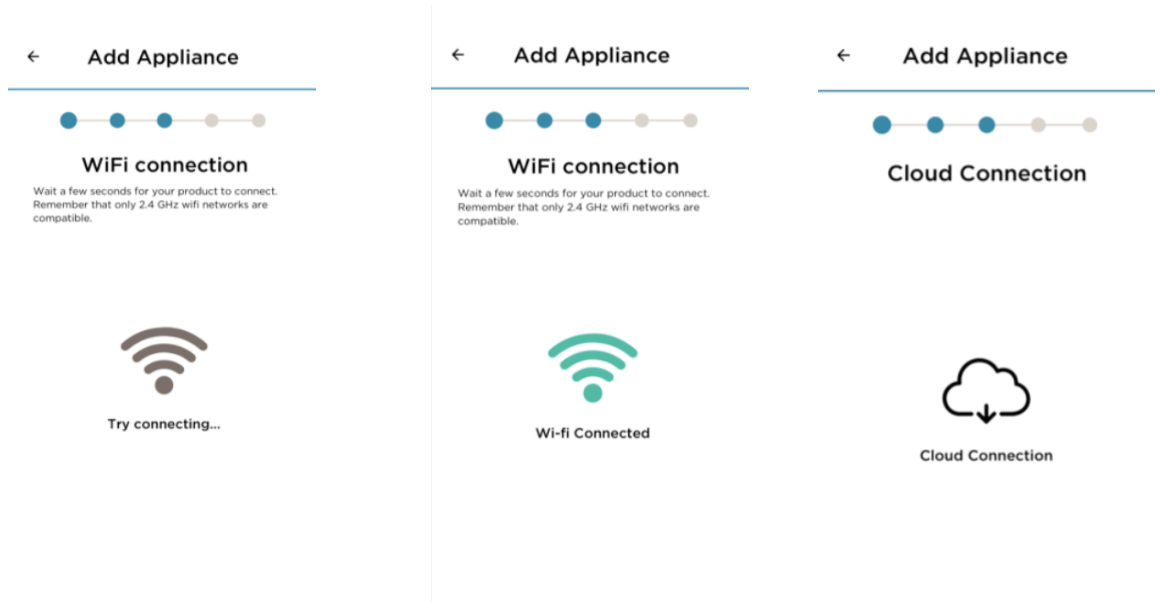


Figura 84 - Grafiche connessione

Il restante funzionamento dell'App coincide con quanto attualmente implementato, con la comunicazione verso la cappa che passa attraverso il Cloud. Eventuali fail durante il processo appena descritto, come ad esempio un errore durante la scrittura della password della rete o lo spegnimento del router, portano ad un fallimento della connessione al Cloud. Questa condizione comporta un reset del modulo. Questo reset non è tuttavia improvviso, ma prima che avvenga il codice setta la caratteristica "Stato" con il valore "Connessione

fallita", in questo modo l'applicazione è anch'essa in grado di dare un feedback all'utente e riavviare da capo la procedura di on-boarding, riportando quindi la procedura guidata alla schermata di scansione del QR code caratteristico.

Il codice nel caso BLE emula in maniera quanto più fedele possibile l'attuale processo di registrazione del prodotto. Questa scelta è legata alla possibilità di poter riutilizzare tutte le schermate attualmente in uso dall'App Elica Connect, a meno di qualche variazione di label. Naturalmente anche questa scelta è dettata dalla necessità di ridurre al minimo eventuali investimenti e cercare di riutilizzare quanto possibile dell'attuale soluzione.

5.5. Studio del processo di certificazione

Nel capitolo uno è stata riportata una breve descrizione del processo di certificazione, descrivendo il processo di analisi che porta alla definizione dei test e prove da effettuare. Le linee guida e gli standard armonizzati permettono di identificare il particolare prodotto e di conseguenza le norme a dover applicare e rispettare.

In questo paragrafo verrà descritto più nel dettaglio il processo di certifica vero e proprio, ovvero la lista delle prove tecniche da eseguire con il fine di poter rilasciare il prodotto sul mercato.

Il laboratorio EPL sulla base della linea guida ETSI EG 203 367 e dello standard Europeo ETSI EN 303 446-1 identifica le norme e prove da eseguire relative al particolare prodotto. Per rendere più chiaro questo passaggio viene ora riportato un esempio: all'interno dello standard ETSI EN 303 446-1 sono riportate le varie normative di riferimento che devono essere rispettate; naturalmente non tutte devono essere soddisfatte; queste si differenziano infatti in base alle caratteristiche del prodotto. Di conseguenza vanno individuate le norme da rispettare e svolti tutti i relativi test. Ad esempio, tra le normative generiche legate all'EMC, troviamo:

CENELEC EN 61000-3-3 (2013): "Electromagnetic compatibility (EMC) - Part 3-3: Limits - Limitation of voltage changes, voltage fluctuations and flicker in public low-voltage supply systems, for equipment with rated current <= 16 A per phase and not subject to conditional connection" [18]

Questa norma fissa i limiti delle fluttuazioni di tensione per sistemi alimentati da bassa tensione con al massimo 16 A per fase. La cappa o il piano aspirante rispettano queste condizioni e di conseguenza devono essere effettuati tutti i test richiesti dalla normativa.

Un'altra norma indicata è la seguente:

CENELEC EN 61000-3-12 (2011): "Electromagnetic compatibility (EMC) - Part 3-12: Limits - Limits for harmonic currents produced by equipment connected to public low-voltage systems with input current > 16 A and <= 75 A per phase" [18]

Questa fissa invece limiti delle correnti armoniche ma il prodotto in questione deve essere alimentato con una corrente compresa tra 16 A e 75 A per fase, di conseguenza non è necessario eseguire i test da essa descritti dato che fa riferimento ad un prodotto diverso dalla cappa in questione.

Seguendo questa logica si vanno a definire tutte le norme e prove da eseguire per rispettare il punto 3.1b della direttiva 2014/53/UE, necessarie per soddisfare tutti i limiti di compatibilità elettromagnetica previsti dalla legge.

Entrando più nel dettaglio delle prove eseguite, la lista completa e i corrispondenti riferimenti normativi è riportata di seguito. La tabella (Tabella 26) contiene al suo interno il tipo di prova, la normativa a cui fa riferimento e una breve descrizione del fenomeno che si va a valutare con la prova. [19]

Tipo di prova	Norma di riferimento	Descrizione
IEC 61000-4-5 Surge	CEI EN 61000-4-5: 201	Immunità ad impulso
IEC 61000-4-5 Surge	ETSI 301 489-1	Immunità ad impulso
IEC 61000-4-11 Voltage Dips and Variation	CEI EN 61000-4-11: 2006	Buchi di tensione ed interruzioni
IEC 61000-4-11 Voltage Dips and Variation	ETSI 301 489-1	Buchi di tensione ed interruzioni
IEC 61000-4-6 Correnti iniettate	CEI EN 61000-4-6: 2014	Correnti Iniettate
IEC 61000-4-6 Correnti iniettate	ETSI 301 489-1	Correnti Iniettate
IEC 61000-4-2 ESD	CEI EN 61000-4-2: 2011	Scariche di elettricità
IEC 61000-4-2 ESD	ETSI 301 489-1	Scariche di elettricità
IEC 61000-4-4 EFT	CEI EN 61000-4-4: 2013	Immunità a transitori
IEC 61000-4-4 EFT	ETSI 301 489-1	Immunità a transitori
CISPR 14-1 Potenza Irradiata (No US)	US EN 55014-1:2017	Potenza Irradiata
EN 61000-3-2 Armoniche	CEI EN 61000-3- 2:2015	Correnti armoniche
EN 61000-3-3 Flikers	IEC 61000-3-3:2013+Am1:2017	Flikers
EN 62233 EMF	CEI EN 62233:2009; EN 62233:2008; IEC 62233 (2005- 10)	Campo magnetico
CISPR 14-1 Emissioni condotte FCC part15	FCC Part 15 EN 55014-1:2017	Emissioni condotte

Tabella 26 - Elenco prove eseguite

Con il fine di garantire la certificazione del prodotto vengono eseguite tutte queste prove e per ognuna di esse viene redatto un “Rapporto di prova”. Questo documento ha una struttura generalmente fissa e viene utilizzato per descrivere la prova eseguita con i relativi risultati; l’insieme di questi documenti forma il “Dossier di prova”.

Un rapporto di prova è di base diviso in vari paragrafi ed organizzato come segue:

- Oggetto: breve descrizione del test da eseguire;
- Piano delle prove: tabella riepilogativa che contiene le prove da eseguire (un test può richiedere più prove per essere superato), normativa di riferimento, codice del DUT (Device Under Test), data di arrivo del campione ed il risultato del test;
- Descrizione del prodotto testato: nome del prodotto ed informazioni generiche come ad esempio tensione di alimentazione, frequenza, potenza nominale e classe di isolamento;
- Configurazione di prova: lista di tutti i componenti (con i relativi codici Elica) che formano il campione, come ad esempio gruppi motore e schede PCB;
- Condizioni ambientali: temperatura ambiente, pressione atmosferica e umidità relativa. Queste informazioni sono necessarie per garantire la ripetibilità delle prove eseguite;
- Tabella riepilogativa sulla compatibilità: vengono indicate le prove da eseguire e la valutazione minima richiesta per definire la prova superata. In genere si hanno più livelli per la valutazione: A, B, C, D che vanno rispettivamente dal miglior risultato ammissibile (A) al peggiore (D). Segue un elenco di tutte le prove eseguite con la rispettiva valutazione e l’esito finale, se positivo o negativo.
- Setup di misura: viene riportato il cablaggio e setup della misurazione. È importante evidenziare che questo passaggio è descritto nei minimi dettagli all’interno della normativa, in cui appunto vengono indicati i cavi da utilizzare, la loro posizione, la loro lunghezza e tutte le informazioni necessarie affinché la prova possa poi essere ripetuta in un altro stabilimento o in un’altra nazione ma nelle stesse identiche condizioni. Come già descritto, l’obiettivo è quello di garantire la ripetibilità della misurazione;
- Note: eventuali commenti o osservazioni sui prodotti o sull’esecuzione ed i risultati del test;

- Immagini: serie di fotografie del setup di misura o del DUT;
- Lista strumenti: lista di tutti gli strumenti utilizzati nel test con la relativa data di scadenza della taratura. Un test eseguito con uno strumento con taratura scaduta è da ritenersi non valido perché non si ha la certezza del corretto funzionamento dello stesso. Quando tarato e certificato da un ente appropriato lo strumento è invece ritenuto affidabile;
- Incertezza estesa della catena di misura: viene riportata l'incertezza estesa di ogni strumento (le incertezze sono determinate in maniera conforme alla guida GUM ed al documento EA-4/02) e questa viene ottenuta moltiplicando l'incertezza tipo per il fattore di copertura "k" pari a 2 corrispondente ad un valore di fiducia pari al 95%.

Il rapporto di prova viene poi firmato dall'operatore che ha eseguito il test e dal Project Manager. Il Dossier finale è invece firmato dal Responsabile del laboratorio EPL.

Per ognuna delle prove indicate nella tabella vengono eseguiti i test indicati nella normativa, sono poi valutati i risultati e confrontati con il criterio di valutazione richiesto. Sulla base di questa analisi i test sono giudicati superati o no. I criteri di valutazione sono quattro e descrivono quello che deve essere il comportamento dell'apparato sia durante l'esecuzione del test che nel normale utilizzo successivo. Le definizioni sono riportate di seguito (Tabella 27). [19]

Criterio di valutazione	Descrizione
A	L'apparecchiatura deve continuare a funzionare come previsto durante e dopo la prova. Non è permessa alcuna degradazione di prestazione o perdita di funzione al di sotto di un certo livello di prestazione (o una perdita di prestazione permessa) specificato dal costruttore, quando l'apparecchiatura viene utilizzata come previsto.
B	L'apparecchiatura deve continuare a funzionare come previsto dopo la prova. Durante la prova è permessa una temporanea degradazione della prestazione con auto ripristino. Non è permessa nessuna modifica dello stato di funzionamento o dei dati memorizzati.
C	È permessa la perdita o la degradazione temporanea della funzione, purché la funzione sia auto recuperabile mediante un reset del sistema o possa essere ristabilita dall'intervento sui dispositivi di controllo o da qualunque soluzione specificata nelle istruzioni per l'uso. Non è permesso il ripristino mediante interruzione dell'alimentazione.
D	È permessa la degradazione o perdita di funzione non recuperabile a causa di danni permanenti di apparecchiature (componenti) o software o perdita di dati. Nessuna condizione non sicura è consentita: l'apparecchio non deve causare un malfunzionamento pericoloso, non vi è alcun guasto nei circuiti di circuiti elettronici di protezione (PEC), ove previsti, se l'apparecchio è ancora operativo. L'isolamento dielettrico deve rimanere integro e perfettamente funzionante. Durante o dopo le prove la macchina non deve emettere fiamme, metallo fuso, gas tossivi o infiammabili in quantità pericolosa.

Tabella 27 - Criteri di valutazione

Generalmente il criterio D non è mai ritenuto livello minimo; infatti, tutte le prove eseguite nel laboratorio richiedono una valutazione minima a partire da C.

5.6. Prove eseguite

Nella tabella precedente è riportata una lista delle prove da eseguire sul prodotto ed all'interno di questo paragrafo verranno ora analizzate più nel dettaglio, fornendo una descrizione generica della prova e dei risultati attesi per essere definita superata. Analizzandole in ordine, i tipi di prova eseguiti sono i seguenti

5.6.1. IEC 61000-4-5

Tesi di immunità ad impulso. La corrispondente norma si riferisce ai requisiti di immunità, ai metodi di prova e alla gamma dei livelli di prova raccomandati per le apparecchiature nei riguardi di impulsi unidirezionali causati da sovratensioni derivanti da transitori di commutazioni oppure da fulmini. Vengono definiti differenti livelli di prova che si riferiscono a diverse condizioni ambientali e di installazione: il livello di test è di 1 kV tra fase-neutro e 2 kV tra fase-conduttore di protezione e neutro-conduttore di protezione. Vengono fornite anche altre informazioni oltre all'ampiezza dell'impulso: il tempo di salita è di 1,2/8 µs ed il tempo necessario per raggiungere la metà del valore finale è 20/50 µs. Per il caso della valutazione fase-neutro è utilizzato il circuito seguente (Figura 85), con il generatore collegato tra i due conduttori indicati.

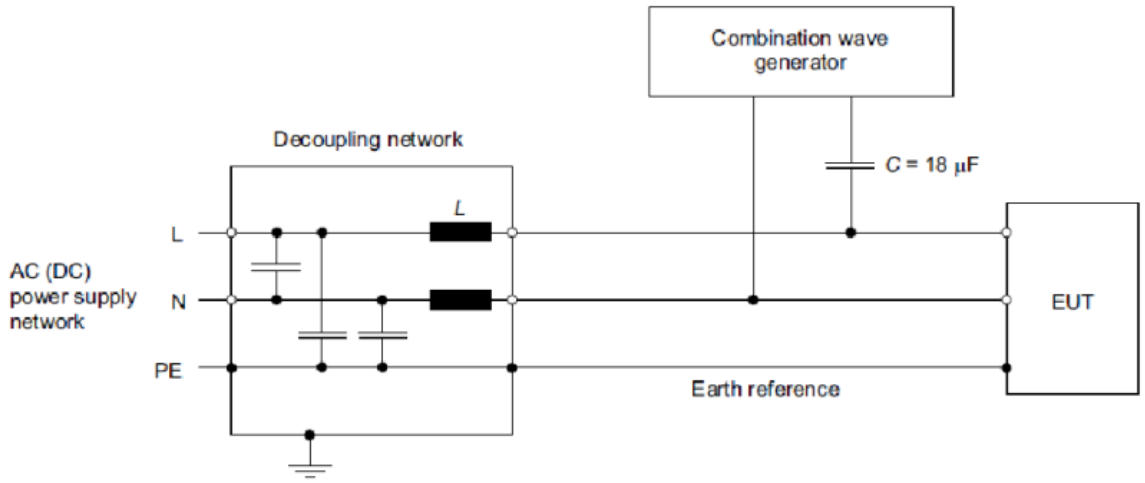


Figura 85 - Setup test di immunità ad impulso

Il criterio richiesto è il B: l'apparecchiatura deve continuare a funzionare come previsto dopo la prova. Durante la prova è permessa una temporanea degradazione della prestazione con auto ripristino. Non è permessa nessuna modifica dello stato di funzionamento o dei dati memorizzati.

5.6.2. IEC 61000-4-11

Test di immunità a buchi di tensione e brevi interruzioni. La presente norma definisce i metodi di prova di immunità ed il campo dei livelli di prova preferiti per apparecchiature elettriche ed elettroniche collegate a reti di alimentazione in bassa tensione per buchi di tensione, brevi interruzioni e variazioni di tensione. Si applica ad apparecchiature elettriche ed elettroniche che hanno un valore di corrente in ingresso che non supera i 16 A per fase. Non si applica ad apparecchiature elettriche ed elettroniche collegate a reti in c.c. o a reti in c.a. a 400 Hz. Lo scopo è di stabilire un riferimento comune per valutare l'immunità delle apparecchiature elettriche ed elettroniche quando vengono sottoposte a buchi di tensione, a brevi interruzioni e variazioni di tensione. La norma indica la durata temporale dell'interruzione ed il valore di tensione (espresso in percentuale rispetto a quello di alimentazione) e la relativa durata per quanto riguarda i buchi di tensione. Sono in totale richieste cinque prove: due per le interruzioni e tre per i buchi di tensione. Sono di seguito riportate due rappresentazioni grafiche (Figure 86 e 87) che rappresentano l'ampiezza dell'alimentazione: una per i buchi di tensione ed una per le interruzioni.

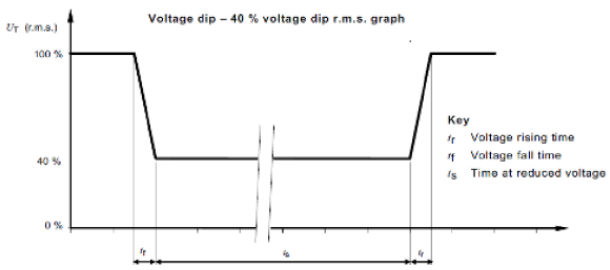


Figura 86 - Setup test di immunità a buchi di tensione e brevi interruzioni

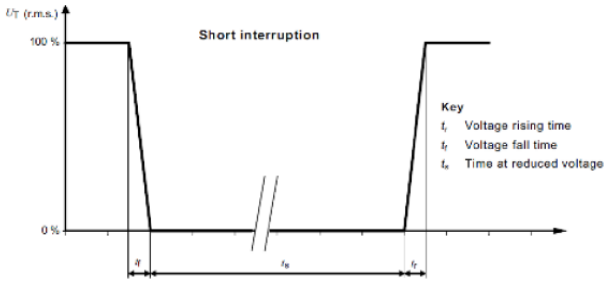


Figura 87 - Setup test di immunità a buchi di tensione e brevi interruzioni

Il criterio richiesto è il B: l'apparecchiatura deve continuare a funzionare come previsto dopo la prova. Durante la prova è permessa una temporanea degradazione della prestazione con auto ripristino. Non è permessa nessuna modifica dello stato di funzionamento o dei dati memorizzati.

5.6.3. IEC 61000-4-6

Test di immunità ai disturbi condotti, indotti da campi a radiofrequenza. La presente Norma di base detta le modalità di esecuzione della prova di immunità di apparecchiature elettriche ed elettroniche ai disturbi elettromagnetici indotti sui cavi da trasmettitori intenzionali di radiofrequenza nell'intervallo di frequenza da 150 kHz a 80 MHz. Obiettivo principale di questa Norma è di dare un riferimento di base oggettivo e coerente per la valutazione dell'immunità funzionale delle apparecchiature elettriche ed elettroniche sottoposte a disturbi indotti sui cavi da campi a radiofrequenza. Questa prova nasce da un fenomeno fisico molto importante: quando fili e cavi sono esposti a questi campi, correnti e tensioni vengono create in questi conduttori. I disturbi vengono iniettati utilizzando un dispositivo di accoppiamento e disaccoppiamento CDN (Couplin Decouplin Network); questi dispositivi accoppiano il segnale al cavo con bassa perdita di inserzione. La gamma di frequenza viene spazzata da 150 kHz a 80 MHz utilizzando livelli di segnale di 3 V e con un segnale di disturbo con ampiezza pari all'80% del livello di segnale modulato con un'onda sinusoidale di frequenza 1 kHz. Il setup di misura è riportato di seguito (Figura 88).

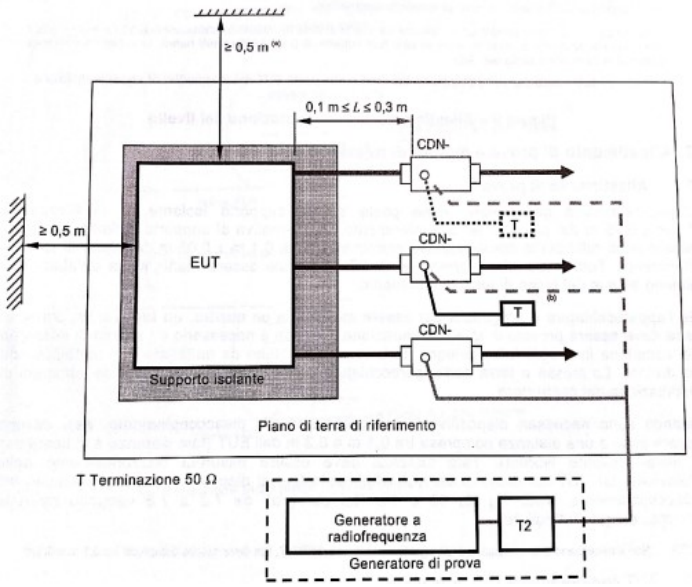


Figura 88 - Setup test di immunità a disturbi condotti

Il criterio richiesto è l'A: l'apparecchiatura deve continuare a funzionare come previsto durante e dopo la prova. Non è permessa alcuna degradazione di prestazione o perdita di funzione al di sotto di un certo livello

di prestazione (o una perdita di prestazione permessa) specificato dal costruttore, quando l'apparecchiatura viene utilizzata come previsto.

5.6.4. IEC 61000-4-2 ESD

Test di immunità a scariche di elettricità statica. La presente Norma riguarda le prescrizioni relative all'immunità ed ai metodi di prova per apparecchiature elettriche ed elettroniche sottoposte a scariche di elettricità statica causate dagli operatori e dagli oggetti adiacenti, in modo diretto e in modo indiretto. Le apparecchiature, i sistemi, i sottosistemi e le periferiche possono essere interessati da scariche di elettricità statica a causa delle condizioni ambientali e di installazione, come bassa umidità relativa, uso di tappeti a bassa conduttività o indumenti in tessuto sintetico. Vengono applicate due tipi di scariche: a contatto diretto (valore di 4 kV) o scarica che avviene utilizzando l'aria (valore di 8 kV, questa soluzione è necessaria per tutti quei punti in cui non è possibile applicare un contatto diretto). Una rappresentazione dei punti di contatto è la seguente (Figura 89).

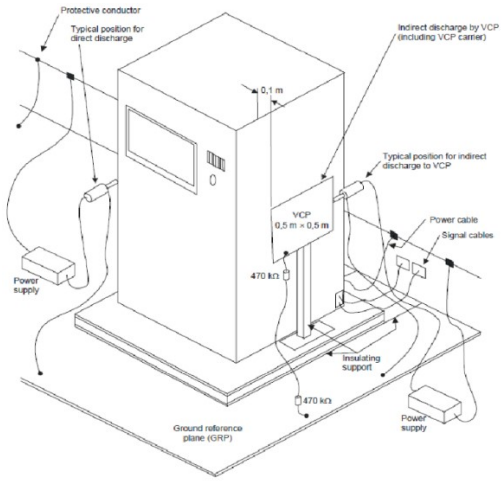


Figura 89 -Setup test di immunità a scariche di elettricità statica

Il criterio richiesto è il B: l'apparecchiatura deve continuare a funzionare come previsto dopo la prova. Durante la prova è permessa una temporanea degradazione della prestazione con auto ripristino. Non è permessa nessuna modifica dello stato di funzionamento o dei dati memorizzati.

5.6.5. IEC 61000-4-4 EFT

Test di immunità a transitori. La presente norma riguarda le prescrizioni relative all'immunità ed ai metodi di prova per apparecchiature elettriche ed elettroniche sottoposte a transitori elettrici veloci ripetitivi. Vengono utilizzati due treni di impulsi con durate differenti: burst a 5 kHz della durata di 15 ms e burst a 100 kHz della durata di 0.75 ms. Per la prova viene utilizzato un EFT/B Generator, ovvero un generatore di burst (Electrical Fast Transient Burst Generator). Il setup di misura è il seguente (Figura 90).

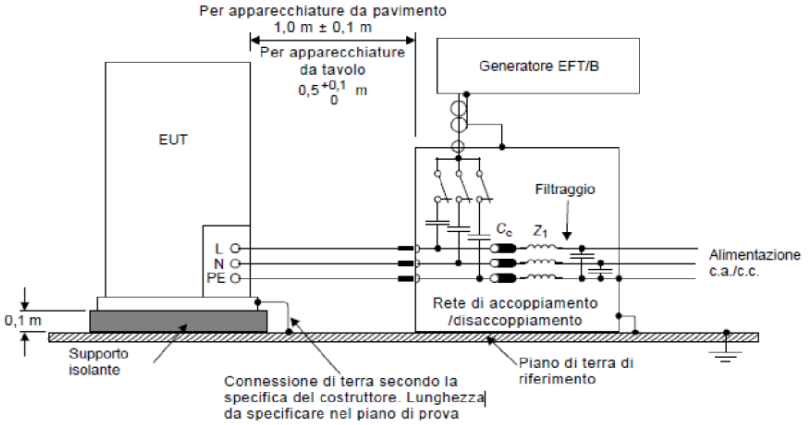


Figura 90 - Setup test di immunità a transitori

Il criterio richiesto è l'A: l'apparecchiatura deve continuare a funzionare come previsto durante e dopo la prova. Non è permessa alcuna degradazione di prestazione o perdita di funzione al di sotto di un certo livello di prestazione (o una perdita di prestazione permessa) specificato dal costruttore, quando l'apparecchiatura viene utilizzata come previsto.

5.6.6. CISPR 14-1

Misura della potenza irradiata. La presente Norma si applica ai radiodisturbi condotti o irradiati provenienti dagli apparecchi le cui principali funzioni sono espletate da motori o da dispositivi di commutazione o di regolazione, a meno che l'energia a radiofrequenza non sia intenzionalmente generata o prevista per l'illuminazione. La norma considera apparecchi come elettrodomestici, utensili elettrici, dispositivi di comando o di regolazione che utilizzano dispositivi a semiconduttore, apparecchi elettromedicali a motore, giocattoli elettrici, distributori automatici e proiettori cinematografici o per diapositive.
A differenza delle altre prove qui non è possibile dare una valutazione, ma si hanno delle soglie e l'emissione deve essere al di sotto di questi valori massimi. La soglia è 30-300 MHz in cui il valore di quasi picco QP deve essere al massimo di 35 dBpW (per 30 MHz) e 45 dBpW (per 300 MHz), da notare che il valore deve crescere linearmente con la frequenza.

5.6.7. EN 61000-3-2

Misura dell'emissione di correnti armoniche. La norma contiene i requisiti per la limitazione delle correnti armoniche causate da apparecchiature elettriche ed elettroniche con una corrente di ingresso < = 16 A per fase, che sono destinate al collegamento a reti pubbliche di distribuzione di energia a bassa tensione.
Per eseguire questa prova i limiti di riferimento sono quelli di un dispositivo classe A, ovvero che rientra in questa categoria: apparecchiatura trifase bilanciata, elettrodomestici esclusi quelli indicati nella classe D (Classe D: computer, monitor e televisori), utensili con esclusione di quelli portatili, dimmer per lampade ad incandescenza e apparecchiature audio. I limiti sono applicati come segue: i valori medi del valore efficace delle correnti armoniche trattate con un filtro passa basso del primo ordine a costante di tempo di 1.5s, calcolati come media aritmetica dei valori misurati dalle finestre di calcolo della DFT e poi mediati sull'intero periodo di osservazione della prova, devono essere inferiori o pari ai limiti applicabili.
I valori limite, divisi in armoniche pari e dispari, sono riportati in tabella (Tabella 28).

Limite armoniche dispari	
Armonica [n]	**CLASSE A**
3	2.30
5	1.14
7	0.77
9	0.40
11	0.33
13	0.21
15 ≤ n ≤ 39	0.15 × 15/n

Limite armoniche pari	
Armonica [n]	**CLASSE A**
2	1.08
4	0.43
6	0.30
8 ≤ n ≤ 40	0.23 × 8/n

Tabella 28 - Limite armoniche pari e dispari

5.6.8. EN 61000-3-3

Misura di variazioni di tensioni e flicker. La norma si occupa della limitazione delle fluttuazioni di tensione e dello sfarfallio impressi sul sistema pubblico a bassa tensione. Per realizzare la misura viene utilizzato un particolare strumento in grado di rilevare e misurare i flicker. I limiti applicati sono i seguenti:

- L'indicatore di flicker di breve durata (PST) non deve essere maggiore di 1.0;
- L'indicatore di flicker di lunga durata (PLT) non deve essere superiore a 0.65;
- La variazione di tensione relativa (DT) non deve superare il 3.3% per più di 500 ms;
- La variazione di tensione relativa allo steady-state (DC) non deve superare il 3.3%;
- La variazione di tensione relativa massima (Dmax) non deve superare:
    - 4% senza ulteriori condizioni;
    - 6% se il DUT è a commutazione manuale o commuta automaticamente più di due volte al giorno o ha un riavvio ritardato;
    - 7% per un'apparecchiatura che deve essere sorvegliata durante l'uso oppure avviata automaticamente;

Per eseguire la misurazione è applicato il seguente metodo statistico. Sono effettuate 24 misurazioni di corrente di spunto nel seguente ordine:

1. Avviare la misura;
2. Accendere il DUT (in modo da creare la massima variazione di tensione)
3. Lasciare che il DUT funzioni normalmente al massimo per un minuto;
4. Spegnere il DUT prima dello scadere del minuto assicurandosi che tutte le parti in movimento al suo interno siano ferme;
5. Attendere il raffreddamento del DUT e ripetere la misura.

Il risultato del test finale è calcolato eliminando i valori minimo e massimo e calcolando la media aritmetica dei rimanenti 22 valori.

5.4.9. EN 62233 EMF

Misura del campo magnetico. La norma si occupa dei campi elettromagnetici per frequenze fino a 300 GHz. In particolare, essa descrive un metodo di valutazione della intensità dei campi elettrici e della densità del flusso magnetico nello spazio circostante agli apparecchi elettrici per uso domestico (elettrodomestici) e similari, compresi gli utensili ed i giocattoli elettrici. Il metodo descritto serve per misurare i campi EM ed i loro effetti potenziali sul corpo umano con riferimento agli standard di esposizione (ICNIRP 98, IEEE C95.1 e IEEE C95.6) definiti come livelli di massima esposizione permissibile. La misura viene effettuata con un B-field Probe, strumento dotato di un'antenna a loop isotropa (quindi realizzata con tre loop perpendicolari) in grado di rilevare e misurare il campo magnetico (Figura 91).

Figura 91 – Loop antenna

CARATTERISTICHE ANTENNA:

- Bassa frequenza: 1 Hz – 400 kHz;
- Misura di campo magnetico
- Produttore NARDA PMM
- Misura sugli assi X,Y,Z.

Questa viene effettuata all'accensione del DUT e dopo un periodo di riscaldamento di 30 minuti, con lo strumento posto ad una distanza di 30 cm in due posizioni: davanti e sopra il DUT, in un intervallo di frequenza 10 Hz – 400 kHz. Il risultato della misura è considerato conforme allo standard se il valore misurato sommato all'incertezza non supera il limite o se nel caso in cui questo venga superato in alcuni punti, detti hot spot, si prende in considerazione il fattore di accoppiamento dell'apparato e lo si moltiplica per il valore misurato, se il risultato è al di sotto del limite il DUT supera la prova.

5.4.10. CISPR 14-1

Misura delle emissioni condotte. La norma si applica ai radiodisturbi condotti o irradiati provenienti dagli apparecchi le cui principali funzioni sono espletate da motori o da dispositivi di commutazione o di regolazione, a meno che l'energia a radiofrequenza non sia intenzionalmente generata o prevista per l'illuminazione. La norma considera apparecchi come elettrodomestici, utensili elettrici, dispositivi di comando o di regolazione che utilizzano dispositivi a semiconduttore, apparecchi elettromedicali a motore, giocattoli elettrici, distributori automatici e proiettori cinematografici o per diapositive.
A differenza delle altre prove qui non è possibile dare una valutazione, ma si hanno delle soglie e l'emissione deve essere al di sotto di questi valori massimi. Le soglie sono:

- 0.009-0.050 MHz in cui il valore di quasi picco QP deve essere al massimo 110 dB µV;
- 0.050-0.150 MHz in cui il valore di quasi picco QP deve essere al massimo di 90 dB µV (per 0.050 MHz) e 80 dB µV (per 0.150 MHz), da notare che il valore deve decrescere linearmente con il logaritmo della frequenza;
- 0.150-0.5 MHz in cui il valore di quasi picco QP deve essere al massimo di 66 dB µV (per 0.150 MHz) e 56 dB µV (per 0.5 MHz), da notare che il valore deve decrescere linearmente con il logaritmo della frequenza;
- 0.05-5 MHz in cui il valore di quasi picco QP deve essere al massimo 56 dB µV;
- 5-30 MHz in cui il valore di quasi picco QP deve essere al massimo 60 dB µV.

Per eseguire la prova viene utilizzata una LISN (Line Impedance Stabilization Network). Una rete LISN è anche necessaria per disaccoppiare il dispositivo in prova dall'alimentazione esterna e avere un'impedenza definita per l'ingresso del DUT.

5.4.11. Certificazione parte radio

Terminata la parte di test legata alla compatibilità elettromagnetica si deve passare ad analizzare la parte radio. Certificare ed effettuare test di questo tipo richiedono strumentazione ed infrastrutture molto complesse, non a disposizione del laboratorio EPL Elica. Tuttavia, per rispettare il punto 3.2 della normativa 2014/53/EU RED, la linea guida ETSI EG 203 367 riporta che se il modulo radio utilizzato è installato rispettando una serie di requisiti (distanza da piani metallici ad esempio) allora per esso è valida la certificazione fatta dal costruttore; quindi, non è necessario ripetere prove legate alle sue emissioni.

Il modulo Wi-Fi ESP32 viene fornito con una serie di certificazioni legate all'EMC: CE (quindi RED 2014/53) per il mercato Europeo, FCC (Federal Communications Commission) per il mercato statunitense, KC (Korea Certification) per la Korea, CCC (China Compulsory Certificate) per la Cina, ISED (Innovation, Science and Economic Development) per il Canada e JRL (Japan Radio Law) per il Giappone. A queste si sommano poi la certificazione Wi-Fi Alliance e Bluetooth SIG, che rispettivamente garantiscono l'interoperabilità con altri dispositivi certificati Wi-Fi ed il rispetto degli standard e vincoli normativi della tecnologia Bluetooth.

L'installazione permette ad Elica di prendere ed utilizzare la certificazione di base fornita dal core Wi-Fi ESP32 senza dover ripetere ulteriori prove. Elica ed EPL si riservano comunque la possibilità di effettuare un test legato alle emissioni del modulo ma per effettuare ciò è necessaria una camera semi anecoica, non presente nel laboratorio. Per questo motivo questo test viene eseguito all'interno dei laboratori UL (Underwriters Laboratories Inc è un'organizzazione indipendente di certificazioni di sicurezza) che mettono a disposizione la loro strumentazione per eseguire le prove, test che poi hanno validità riconosciuta da Accredia. Il test viene eseguito quindi in camera semi anecoica UL sulla base dello standard Europeo armonizzato ETSI EN 300 328, standard che regola l'accesso allo spettro radio per tutti i dispositivi che operano nella banda 2.4 GHz. Qui vengono forniti i limiti per l'occupazione di banda e per le emissioni fuori banda, mediante la maschera riportata di seguito (Figura 92).

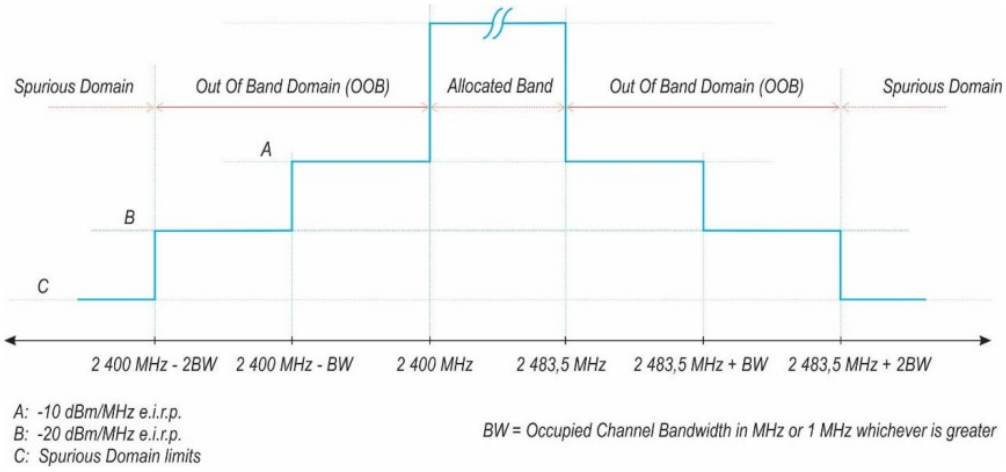


Figura 92 - Maschera occupazione in banda

Inoltre, la misura viene estesa ad un range di frequenze molto maggiore di quello riportato nella maschera, si va infatti da 30 MHz a 12.75GHz con il fine di rilevare la presenza di eventuali armoniche, sia sopra che sotto la banda di utilizzo, dato che l'individuazione di possibili componenti fuoribanda anche a frequenze molto minori dei 2.44 GHz potrebbe andare a disturbare il microcontrollore installato sulla Main Board, che lavora a frequenze dell'ordine dei MHz.

Il setup di misura è riportato di seguito (Figura 93). Per la ricezione della potenza irradiata di utilizza un'antenna log periodica, scelta soprattutto per la notevole banda passante, caratteristica derivata dalla struttura stessa dell'antenna, formata da dipoli di diversa lunghezza posti uno accanto all'altro. I dipoli da una parte garantiscono un ampio intervallo di funzionamento in frequenza ma il loro diagramma di radiazione permette di ricevere solo componenti di campo parallele ai dipoli e non ortogonali; proprio per

questo con il fine di poter caratterizzare correttamente il campo irradiato da un apparecchio sono necessarie due misurazioni, ovvero due polarizzazioni dell'antenna: verticale ed orizzontale. In questo modo si ottengono le due componenti del campo elettrico e di conseguenza è possibile calcolare il campo elettromagnetico irradiato.

Figura 93 - Laboratorio UL

6. Cybersecurity

La sicurezza informatica (*computer security*), è l'insieme dei mezzi, delle tecnologie e delle procedure dedicate alla protezione dei sistemi informatici in termini di disponibilità, confidenzialità e integrità dei beni o asset informatici. Un sinonimo che trova talvolta impiego in questo contesto è cybersicurezza (dall'inglese C*ybersecurity*), termine che più precisamente ne rappresenta una sottoclasse, essendo quell'ambito della sicurezza informatica che dipende solo dalla tecnologia: con esso si enfatizzano spesso qualità di resilienza, robustezza e reattività che una tecnologia deve possedere per fronteggiare attacchi mirati a comprometterne il suo corretto funzionamento e le sue performance.

Dal momento che l'informazione è un bene aziendale, e che ormai la maggior parte delle informazioni sono custodite su supporti informatici, ogni organizzazione è interessata a garantire la sicurezza dei propri dati, in un contesto dove i rischi informatici causati dalle violazioni dei sistemi di sicurezza sono in continuo aumento. Per questo esistono precise norme in materia di privacy, tra cui ad esempio il Regolamento Generale sulla Protezione dei Dati (RGDP), regolamento (UE) n. 2016/679. La materia privacy è però limitativa, trattando essa unicamente il tema della protezione dei dati personali ed escludendo il resto; la legge sulla privacy, infatti, non impone alcuna protezione per informazioni prive di dati personali. Spesso si fa confusione tra tutela dei dati personali e sicurezza delle informazioni tout court (informazioni riservate e confidenziali ma che nulla hanno che vedere con dati personali).

Con il fine di concentrarsi sull'aspetto della protezione delle informazioni l'Unione Europea ha inizialmente rilasciato il regolamento (UE) n. 526/2013 e poi abrogato dal regolamento (UE) 2019/881 riguardante i requisiti di sicurezza delle informazioni dell'Unione Europea e il ruolo dell'Agenzia europea ENISA per la sicurezza delle informazioni. Il regolamento identifica diverse aree di rischio che incidono sull'intera industria manifatturiera come automobili connesse e climatizzate, dispositivi medici elettronici, sistemi di controllo dell'automazione industriale e reti intelligenti come esempi di aree in cui verrà utilizzata la certificazione nel prossimo futuro. La scelta della certificazione appropriata e dei relativi requisiti di sicurezza informatica si basa sull'analisi dei rischi associati all'utilizzo di un prodotto, servizio o processo. [20]

Nella sicurezza informatica sono coinvolti elementi tecnici, organizzativi, giuridici e umani. Per valutare la sicurezza solitamente è necessario individuare le minacce, le vulnerabilità e i rischi associati ai beni informatici, al fine di proteggerli da possibili attacchi (interni o esterni) che potrebbero provocare danni diretti o indiretti di impatto superiore a una determinata soglia di tollerabilità (es. economico, politico-sociale, di reputazione) a un'organizzazione. Oltre alle tre fondamentali proprietà (disponibilità, riservatezza, integrità) possono essere considerate anche: autenticità, non ripudiabilità, responsabilità, affidabilità.

Nei paragrafi successivi, oltre ad una descrizione di quelle che sono le minacce dirette alla sicurezza IoT più comuni vengono anche riportate le soluzioni applicate da Elica per contrastarle e per garantire la sicurezza dei propri elettrodomestici IoT.

6.1. Valutazione delle minacce alla sicurezza IoT

La maggior parte dei dispostivi IoT sono vulnerabili ad un ampio range di possibili minacce. Gli attacchi più comuni che possono essere eseguiti contro un dispositivo smart sono:

- *Man in the middle*

  Attacco man in the middle (spesso abbreviato in MITM, in italiano "uomo nel mezzo") è una terminologia impiegata nella crittografia e nella sicurezza informatica per indicare un attacco informatico in cui qualcuno segretamente ritrasmette o altera la comunicazione tra due parti che

credono di comunicare direttamente tra di loro. Questo attacco si concretizza durante il processo di scambio di chiave pubblica tra due utenti: supponiamo che Alice voglia comunicare con Bob e che Eve voglia spiare la conversazione e, se possibile, consegnare a Bob dei falsi messaggi. Per iniziare, Alice deve chiedere a Bob la sua chiave pubblica. Se Bob invia la sua chiave pubblica ad Alice, ma Eve è in grado di intercettarla, può iniziare un attacco Man in the middle. Eve può semplicemente inviare ad Alice una chiave pubblica della quale possiede la corrispondente chiave privata. Alice poi, credendo che questa sia la chiave pubblica di Bob, cifra i suoi messaggi con la chiave di Eve ed invia i suoi messaggi cifrati a Bob. Eve quindi li intercetta, li decifra, ne tiene una copia per sé, e li re-cifra (dopo averli alterati se lo desidera) usando la chiave pubblica che Bob aveva originariamente inviato ad Alice. Quando Bob riceverà il messaggio cifrato, crederà che questo provenga direttamente da Alice.

Quanto descritto mostra la necessità per Alice e Bob di avere un modo per garantire che essi stiano utilizzando le rispettive chiavi pubbliche, piuttosto che quella di un attaccante. L'attacco sfrutta quindi l'assenza di Autenticazione delle credenziali. [24]

Ad esempio, un attacco man in the middle è l'*eavesdropping*, in cui l'attaccante crea connessioni indipendenti con le vittime e ritrasmette i messaggi del mittente facendo credere loro che stiano comunicando direttamente tramite una connessione privata, con l'intera conversazione che è controllata invece dal malintenzionato in grado di intercettare tutti i messaggi importanti e/o iniettarne di nuovi.

- *Data and Identity theft*

Il furto di identità si verifica quando le informazioni personali vengono rubate e utilizzate da criminali informatici o truffatori per impersonare il proprietario dei dati. Le credenziali possono essere utilizzate per accedere a diverse aree della vita digitale.

Esistono diverse modalità per ottenere i dati sensibili di un utente, una tra queste il *phishing*: si tratta di un'attività illegale che sfrutta una tecnica di ingegneria sociale: il malintenzionato effettua un invio massivo di messaggi che imitano, nell'aspetto e nel contenuto, messaggi legittimi di fornitori di servizi; tali messaggi fraudolenti richiedono di fornire informazioni riservate come, ad esempio, il numero della carta di credito o la password per accedere ad un determinato servizio. Per la maggior parte è una truffa perpetrata usando messaggi di posta elettronica, ma non mancano casi simili che sfruttano altri mezzi, quali i messaggi SMS. [21]

- *Device hijacking*

Il termine hijacking indica una tecnica di attacco informatico che consiste nel modificare opportunamente dei pacchetti dei protocolli TCP/IP al fine di dirottare i collegamenti ai siti web e prenderne il controllo. In questo modo l'attaccante è in grado di controllare il dispositivo IoT. [21]

- *Distributed Denial of Service (DDoS)*

Denial of Service (in italiano "negazione del servizio", DOS), nel campo della sicurezza informatica, indica un malfunzionamento dovuto ad un attacco informatico in cui si fanno esaurire deliberatamente le risorse di un sistema informatico che fornisce un servizio ai client, ad esempio

un sito web su un web server, fino a renderlo non più in grado di erogare il servizio ai client richiedenti.

In un Denial of Service Distribuito (DDOS) il traffico dei dati in entrata che inonda la vittima proviene da molte fonti diverse. L'esempio in analogia è quello di un gruppo di persone che affollano la porta d'ingresso o il cancello di un negozio o di un'azienda, e non consentendo alle parti legittime di entrare nel negozio o nel business, interrompono le normali operazioni. Ciò rende effettivamente impossibile fermare l'attacco semplicemente bloccando una singola fonte [4].

Gli attacchi vengono abitualmente attuati inviando molti pacchetti di richieste, di solito ad un server web, FTP o di posta elettronica saturandone le risorse e rendendo tale sistema "instabile" e non disponibile agli altri utenti. Nel nostro caso, in presenza di un attacco DoS o DDoS al cloud, risulterebbe impossibile controllare gli elettrodomestici IoT tramite App. [21]

- *Permanent Denial of Service (PDoS)*

Il Permanent Denial-of-Service (PDoS), noto anche come *phlashing*, è un attacco che danneggia un sistema così gravemente da richiedere la sostituzione o la reinstallazione dell'hardware. A differenza dell'attacco Denial of Service distribuito, un attacco PDoS sfrutta i difetti di sicurezza che consentono l'amministrazione remota sulle interfacce di gestione dell'hardware della vittima, come router, stampanti o altro hardware di rete.

Un esempio di questo attacco è il *flashing*. Qui l'utente malintenzionato utilizza le vulnerabilità appena descritte per sostituire il firmware di un dispositivo con un'immagine del firmware modificata, corrotta o difettosa. L'intento è quello di bloccare il dispositivo, rendendolo inutilizzabile per il suo scopo originale fino a quando non viene riparato o sostituito. [21]

6.2. Analisi delle possibili contromisure per la sicurezza IoT

I dispositivi domestici intelligenti devono essere protetti da una contromisura per la sicurezza IoT che sia completa (cioè da dispositivo a cloud) e che non interferisca con il provider del servizio internet.

Una efficiente soluzione per la sicurezza IoT dovrebbe includere le seguenti funzionalità:

- *Mutual authentication*

L'autenticazione mutua o autenticazione bidirezionale si riferisce a due parti che si autenticano a vicenda contemporaneamente in un protocollo di autenticazione. È una modalità di autenticazione predefinita in alcuni protocolli (IKE, SSH) e facoltativa in altri (TLS). L'autenticazione mutua è una caratteristica desiderata negli schemi di verifica che trasmettono dati sensibili, al fine di garantire la sicurezza dei dati. L'autenticazione bidirezionale può essere eseguita con due tipi di credenziali: nomi utente e password e certificati a chiave pubblica. Gli schemi che hanno un passaggio di autenticazione mutua possono utilizzare diversi metodi di crittografia, comunicazione e verifica, ma tutti condividono una cosa in comune: ogni entità coinvolta nella comunicazione viene verificata. Se Alice vuole comunicare con Bob, entrambi autenticheranno l'altro e verificheranno che sia con chi si aspettano di comunicare prima che vengano trasmessi dati o messaggi. Questa soluzione elimina di fatto la possibilità che si verifichi un attacco del tipo Man in the Middle. [24]

- *Secure communication (Encryption)*

  La crittografia è il processo di codifica delle informazioni. Questo procedimento converte la rappresentazione originale delle informazioni, nota come testo in chiaro, in una forma alternativa nota come testo cifrato. Idealmente, solo le parti autorizzate possono decifrare un testo cifrato in testo normale e accedere alle informazioni originali. La crittografia di per sé non impedisce l'interferenza, ma nega il contenuto intelligibile a un potenziale intercettore.
  Uno schema di crittografia utilizza solitamente una chiave di crittografia pseudo-casuale generata da un algoritmo. È possibile decifrare il messaggio senza possedere la chiave ma, per uno schema di crittografia ben progettato, sono necessarie notevoli risorse e competenze computazionali. Un destinatario autorizzato invece può facilmente decifrare il messaggio con la chiave fornita dal trasmettitore.
  Le prime tecniche di crittografia sono state utilizzate nella messaggistica militare. Da allora, nuove tecniche sono emerse e sono diventate comuni in tutte le aree dell'informatica moderna. Gli attuali schemi di crittografia utilizzano i concetti di chiave pubblica e privata o di chiave simmetrica e la loro sicurezza si basa sull'utilizzo di primitive crittografiche che per essere invertite richiedono un tempo di elaborazione e potenza di calcolo troppo elevati per i computer moderni. È importante evidenziare come lo sviluppo dei quantum-computer stiano però mettendo in crisi queste funzioni crittografiche e di conseguenza il NIST ha bandito una gara con il fine di definire i prossimi standard di cifratura e firma in grado di resistere anche ad attacchi provenienti da computer quantistici. [24]

- *Security monitoring and analysis*

  Il monitoraggio della sicurezza è il processo automatizzato di raccolta e analisi degli indicatori di potenziali minacce alla sicurezza, quindi valutazione di questi avvisi con un'azione appropriata. Il monitoraggio della sicurezza, a volte indicato come "monitoraggio delle informazioni di sicurezza" (SIM) o "monitoraggio degli eventi di sicurezza" (SEM), comporta la raccolta e l'analisi di informazioni per rilevare comportamenti sospetti o modifiche non autorizzate del sistema sulla rete, la definizione dei tipi di comportamento che gli avvisi devono attivare e l'adozione di azioni in base alle esigenze. Il ciclo di monitorare-analizzare permette di identificare casi d'uso comuni e rilevare potenziali scenari d'attacco. [22]

- *Security lifecycle management*

  La funzionalità di gestione del ciclo di vita della sicurezza consente ai fornitori di servizi e agli OEM di controllare gli aspetti di sicurezza dei dispositivi IoT quando sono in funzione.
  Il ciclo fornisce un guida in grado di garantire che vengano compiuti continui progressi sulla sicurezza dei prodotti IoT. Il ciclo è generalmente diviso in quattro fasi:

  1. Identify (Identificazione)

     Il primo passaggio consiste nell'identificare cosa si sta cercando di proteggere. È quindi necessario mappare la rete, identificare i server e le applicazioni che stanno girando su di essi.

  2. Assess (Valutazione)

     Una volta mappata la tecnologia esistente nell'organizzazione attraverso il processo di identificazione, segue la fase di valutazione. In questa fase, i professionisti della sicurezza prendono le informazioni raccolte dal processo di identificazione ed eseguono una

valutazione della sicurezza su tutte le risorse. Questo processo è uno dei passaggi più estesi del ciclo di vita della sicurezza delle informazioni e copre diverse aree, tra cui revisioni di processi e sistemi, revisioni dei server e valutazioni delle vulnerabilità.

3. Design (Progettazione)

   Sulla base delle vulnerabilità e dei problemi specifici identificati nella fase di valutazione si definiscono possibili approcci per risolvere problemi specifici, tra cui minacce alla sicurezza informatica. Alcuni fattori specifici che i team prendono in considerazione durante la fase di progettazione sono: livello di sicurezza, conformità, continuità, area di effetto ed efficacia. Una volta sviluppati potenziali modi per risolvere problemi specifici, viene analizzata ogni soluzione nel dettaglio e vengono creati piani e progetti individuali per ogni modifica. Questi progetti possono includere modifiche alla configurazione del sistema, modifiche ai processi, strumenti e altri fattori, nonché il modo in cui verrà risolto il problema. Il progetto presenterà anche un'analisi degli effetti di questi cambiamenti, comprese le modifiche procedurali, gli impatti sui sistemi adiacenti e i costi di implementazione.

4. Implementation (Implementare)

   Dopo l'approvazione della progettazione di una soluzione, il passaggio successivo del ciclo di vita delle informazioni è l'implementazione. In questa fase del processo viene creato un piano di implementazione per la soluzione proposta. Questo piano contiene una serie di fasi: sviluppare un piano di modifica, acquisizione risorse e implementazione modifiche.

5. Protection (Proteggere)

   Questo passaggio è strettamente correlato alle fasi di progettazione e implementazione, ma copre un ambito leggermente diverso. L'obiettivo della fase di protezione, chiamata anche fase di mitigazione, è convalidare le misure di sicurezza per garantire che i sistemi corrispondano alle policy e agli standard di sicurezza stabiliti.

6. Monitor (Monitorare)

   La fase finale del ciclo di vita della sicurezza è la fase di monitoraggio. In questa fase viene monitorato il sistema e le eventuali modifiche apportate. Mentre le misure di sicurezza implementate possono proteggere dalle vulnerabilità, non vi è alcuna garanzia che rimarranno sicure in futuro. L'obiettivo della fase di monitoraggio è duplice: garantire che la sicurezza rafforzata rimanga in atto e identificare nuove vulnerabilità man mano che si presentano. [22]

- *Secure boot*

  Secure Boot è una parte di UEFI, acronimo di Unified Extensible Firmware Interface. Quest'ultima è un'interfaccia informatica tra il firmware e il sistema operativo di un PC progettata per sostituire il BIOS durante la procedura di avvio di un dispositivo. Secure Boot è una funzionalità che permette di eseguire sul computer (o altro dispositivo) solo ed esclusivamente software autorizzato dal produttore del sistema. In altre parole, consente il caricamento (all'avvio del computer) di quei soli moduli software dotati di una firma digitale autorizzata e riconosciuta, cioè dall'OEM del dispositivo o da terze parti ritenute sicure, le cui firme sono conservate nel firmware della scheda madre. Questo permette di evitare attacchi finalizzati alla sostituzione del firmware con versioni malevole. [22]

6.2.1. Contromisure implementate da Elica

Sulla base delle funzionalità descritte nel paragrafo precedente l'azienda Elica ha implementato una serie di soluzioni volte a garantire la sicurezza dei propri dispositivi IoT. Sono di seguito riportate le principali tecniche adottate.

I moduli *Espressif* per la connectivity utilizzati nei prodotti Elica implementano di fabbrica *Secure boot* e *Secure Flash*. In questo modo solo firmware firmato può essere eseguito ed il firmware immagazzinato nella memoria è criptato. L'aggiornamento FW avviene tramite OTA solo da fonti autorizzate.

Con l'hardware per la comunicazione end-to-end che implementa tecnologie software sviluppate da *Techedge* viene eseguito un processo di autenticazione del server basato su certificato e solo successivamente alla verifica dell'autenticità del cloud la cappa condivide le proprie credenziali di accesso al Broker MQTT. Ad ogni elettrodomestico è associato un ID e una password a 16 bit generati casualmente ed unici e la loro conoscenza prova l'autenticità del client.

Grazie alla consulenza offerta da *Techedge* e *Reply* le comunicazioni tra elettrodomestico, cloud e mobile App sono cifrate, basate su TLS (HTTPS e MQTTS)

I servizi Cloud risiedono su machine AWS. Grazie alla tecnologia messa a disposizione da *Amazon web services* stesso è possibile attuare un ciclo di Monitoraggio – Analisi – Azione per identificare casi d'uso comune e rilevare possibili scenari d'attacco

In corso di implementazione è il processo per il monitoraggio della sicurezza e del rischio, ovvero del Security lifecycle. [22]

Queste soluzioni garantiscono una riduzione del rischio associato alle varie minacce IoT, ovvero rappresentano mitigazioni a possibili attacchi o tecniche in grado di ridurre la probabilità che questi si verifichino. L'effetto di come queste contromisure si incroci con le possibili minacce è descritto dalla tabella di seguito riportata.

	Secure boot	Mutual Authentication	Secure communication (Encryption)	Security monitoring and analysis	Security lifecycle management
Man in the middle		✓	✓		✓
Data and identity theft		✓	✓		
Device hijacking	✓	✓			✓
DDoS	✓			✓	
PDoS	✓		✓	✓	✓

Tutte queste soluzioni e buone pratiche nascono dalla messa a disposizione di documenti rilasciati da organismi internazionali come il NIST o l'ETSI; basta infatti citare il NISTIR 8259 o l'ETSI TS 103 645. La necessità di documentazioni di questo tipo nasce dal fatto che la sicurezza informatica sta diventando un problema crescente dato che il numero dei dispositivi domestici che si connettono ad internet sta aumentando sempre più, con elettrodomestici o prodotto tradizionalmente offline ma che ora stanno diventando connessi devono essere progettati per resistere a minacce informatiche. I documenti appena citati riuniscono buone pratiche da utilizzare in materia di sicurezza e forniscono un sostegno a tutte le parti coinvolte nello sviluppo e produzione di IoT di consumo. Le disposizioni sono incentrate sui risultati, piuttosto che prescrittive, offrendo alle organizzazioni la flessibilità di innovare e implementare soluzioni di sicurezza appropriate per i loro prodotti.

A valutare il lavoro svolto da Elica nella fase di progettazione "sicura" e di sviluppo e sostegno continuo ai propri prodotti per gli aspetti legati alla cybersecurity è possibile prendere come riferimento l'IoT Security Rating di UL.

I documenti sono presi come linea guida e sono utilizzati sia dall'azienda Elica che da aziende collaboratrici come Reply e Techedge per lo sviluppo dei prodotti e servizi associati. Il lavoro svolto viene poi valutato da un ente esterno, l'Underwriters Laboratories appunto, che ha definito questo servizio di rating in grado di rappresentare una soluzione di verifica della sicurezza ed etichettatura per i prodotti IoT che classifica i prodotti in base a una scala ascendente a cinque livelli: Bronzo, Argento, Oro, Platino e Diamante (Figura 94). I prodotti verificati ricevono un'etichetta di sicurezza UL Verified Mark differenziata, che specifica il livello di sicurezza raggiunto, e vengono valutati su base continuativa da UL.

Figura 94 - UL verified mark

La soluzione di UL aiuta produttori e sviluppatori a dimostrare la loro diligenza nei confronti della sicurezza dei loro prodotti valutando il livello di sicurezza degli apparati IoT prodotti. La valutazione naturalmente non viene eseguita gratuitamente, ma a seconda del livello di certificazione che si vuole ottenere, e quindi di prove e valutazioni che l'UL deve fare, si ha un certo costo da pagare; in linea di massima il costo indicativo per la valutazione del livello GOLD, il terzo per importanza, è di circa 20.000€. Nonostante la somma possa sembrare proibitiva o comunque elevata questa rappresenta una certificazione riconosciuta a livello globale, e la sua presenza è sinonimo di garanzia e sicurezza, permettendo di sfruttare queste proprietà a proprio vantaggio attraverso un prezzo di vendita del prodotto finale più alto.

La Cybersecurity o più in generale la sicurezza informatica, fino a qualche anno fa sempre lasciata con priorità bassa, negli ultimi anni ha avuta un'ascesa molto rapida grazie allo sviluppo di prodotto connessi di tutti i tipi, che hanno garantito un aumento molto importante della domanda e di conseguenza delle risorse che un'azienda è interessata ad utilizzare per lo sviluppo di un nuovo prodotto, vista comunque la facilità di recupero del denaro investito.

7. Conclusioni e sviluppi futuri

L'elaborato realizzato ha permesso di fare una panoramica generale sull'attuale stato dell'arte, ovvero sulle soluzioni ora implementate e disponibili per garantire la connettività sui prodotti Elica. Quanto riportato ha un ruolo di formazione ed allineamento e permette di capire per quale motivo l'Azienda si è posta il progetto poi esaminato nella seconda parte della tesi.

Nei capitoli quattro e cinque si è cercato di determinare quale fosse la soluzione che meglio si adattasse agli obiettivi preposti- Realizzare una nuova user interface ed una nuova architettura di comunicazione tra smartphone e cappa richiede un confronto delle possibili tecnologie disponibili e, una volta definito il protocollo più adatto, implementarlo nella maniera più semplice possibile sia dal punto di vista produttivo che di consumo finale per l'utente.

Il contributo dato al progetto ha riguardato tutti i punti finora discussi, includendo anche la fase commerciale di contatto con il fornitore. Sotto la guida dell'Electronics & Connectivity Manager Meniconi Luca e con il contributo strutturale dell'azienda Elica ho potuto ideare, testare e simulare lo sviluppo discusso nei capitoli sopra citati, in particolare: studio delle tecnologie attualmente disponibili, definizione specifiche tecniche e funzionali della nuova interfaccia utente ed infine implementazione e testing del Bluetooth Low Energy.

I risultati raggiunti sono da considerare soddisfacenti e adatti per pianificare uno sviluppo industriale dato che sono stati raggiunti tutti gli obiettivi inizialmente prefissati.

L'apertura dell'azienda all'introduzione di una nuova tecnologia come il Bluetooth non si fermerà a questa singola applicazione, è in valutazione la possibilità di introdurre direttamente il comando remoto del dispositivo utilizzando questo protocollo, soluzione che permetterebbe di controllare a distanza l'elettrodomestico anche per tutte quelle persone che non dispongono di una connessione Wi-Fi a casa o in quelle regioni in cui l'elettrodomestico connesso ad internet non è presente nell'uso comune e prediligono dispositivi controllabili con tecnologie diverse dalla classica Smart Home.

Molto importante è anche l'aspetto Cybersecurity, fattore fondamentale sia per garantire il corretto funzionamento dell'apparato sia la privacy di informazioni e dati sensibili e che nel prossimo anno diventerà un requisito normativo dato che la RED introdurrà anche una serie di test e vincoli volti a verificare la cybersicurezza di un prodotto IoT. Lo studio e le migliorie anche in questo argomento dovranno continuare e seguire gli standard che di volta in volta verranno aggiornati e rilasciati.

Indice delle figure

Indice delle tabelle

Bibliografia

[1] Presentazione interna Elica - *Elica Corporate Profile*

[2] Fondazione E. Casoli, www.fondazionecasoli.org

[3] Presentazione interna EPL – *Elica Propulsion Laboratory*

[4] DIRETTIVA 2014/53/UE DEL PARLAMENTO EUROPEO E DEL CONSIGLIO, 16 Aprile 2014

[5] Presentazione interna Elica – *La cappa*

[6] Specifica Tecnica Funzionale (STF Elica) - *UI "Superplat" with esp32*

[7] Specifica Tecnica Funzionale (STF Elica) – *One-Wire Protocol*

[8] Wikipedia, www.wikipedia.org/wiki/Hypertext_Transfer_Protocol

[9] Wikipedia, www.wikipedia.org/wiki/MQTT

[10] Specifica Tecnica Funzionale (STF Elica) – *Elica MQTT Protocol*

[11] Specifica Tecnica Funzionale (STF Elica) – *Elica App, analisi tecnico funzionale*

[12] Wikipedia, www.wikipedia.org/wiki/IEEE_802.11

[13] Wikipedia, www.wikipedia.org/wiki/Near-field_communication

[14] Wikipedia, www.wikipedia.org/wiki/Z-Wave

[15] Wikipedia, www.wikipedia.org/wiki/Zigbee

[16] Wikipedia, www.wikipedia.org/wiki/Thread_(network_protocol)

[17] Wikipedia, www.wikipedia.org/wiki/LoRa

[18] EUROPEAN STANDARD, ETSI EN 303 446-1 v.1.0.2

[19] Test Report Dossier interno (Dossier EPL)

[20] REGOLAMENTO (UE) 2019/881 DEL PARLAMENTO EUROPEO E DEL CONSIGLIO, 17 aprile 2019

[21] Mitre, www.capec.mitre.org

[22] Presentazione interna Elica– *Cybersecurity IoT*