

Széchenyi István Egyetem
Gépészmérnöki, Informatikai és Villamosmérnöki Kar

IoT eszköz funkcionális és EMC tesztelése, mérése

Buzási László

**Villamosmérnök BSc VII. félév, Infokommunikációs szakirány
Konzulens: Liszi Máté
(egyetemi tanársegéd)**

Széchenyi István Egyetem
2021 November
Győr



Absztrakt

A TDK dolgozatom az Internet of Things technológia témakörében íródott. A dolgozatban egy kifejezetten IoT felhasználásra készült eszköznek a tesztelése, mérése kerül bemutatásra. Ez az eszköz, illetve a hozzá tartozó platform a Digitális Fejlesztési Központ keretein belül lett fejlesztve és megvalósítva egyaránt. Lényegében a készülék több különböző felhasználási területre alkalmazandó, szenzor adatokat feldolgozó és továbbító eszköz, amely az adatokat egyénileg kiválasztott rádiós technológián (GSM, 4G/5G, NB-IoT) továbbítja, ezeket egy szerver tárolja és szoftver segítségével megjeleníti a felhasználó számára. Ebben a projektben több résztvevő is közreműködött, személy szerint én az elektromágneses kompatibilitás mérésekkel, valamint funkcionális tesztelésekkel foglalkoztam.

EMC szempontjából vizsgálva lett többek között sugárzott emisszió, illetve sugárzott immunitás során az eszköz, amelyeknek az eredményét a dolgozat összefoglalja.

Funkcionális tesztelések alatt az eszköz helymeghatározási pontosságának vizsgálatára került sor, három különböző GNSS antenna segítségével. A fejlesztési fázisnak ez tulajdonképpen az első verziója, emiatt a mérések 4G LTE kommunikáció mellett lettek elvégezve, viszont a közel jövőben 5G és NB-IoT technológiák alkalmazásával is tesztelésre kerül majd ez az IoT eszköz.

„A dolgozat a Digitális Fejlesztési Központ támogatásával, a GINOP-3.1.1-VEKOP-15-2016-00001 azonosító számú „Oktatási intézmények és IKT vállalkozások közötti együttműködés ösztönzése és támogatása” –

Programozd a jövőd! projekt keretében valósult meg.

TARTALOM

BEVEZETÉS	6
1. IOT – INTERNET OF THINGS – „DOLGOK” INTERNETE	7
1.1. MIT JELENT AZ IOT KIFEJEZÉS?	7
1.1.1. IoT elterjedése	7
1.1.2. Ipari IoT	8
2. IOT MŰKÖDÉSI FOLYAMATA	9
2.1. ÉRZÉKELŐK (SENSORS)	10
2.1.1. Mit értünk érzékelő alatt?	10
2.1.2. Érzékelő típusok	11
2.1.3. Jelenlegi kihívások	12
2.2. VEZETÉKNÉLKÜLI HÁLÓZATI CSATLAKOZÁS (CONNECTIVITY)	13
2.2.1. Vezetéknélküli hálózati típusok lefedettség szerint	13
2.2.2. Vezetéknélküli kommunikációs technológiák	14
2.3. ADATFELDOLGOZÁS (DATA PROCESSING)	16
2.3.1. Adatfeldolgozási ciklus	17
2.3.2. Adatfeldolgozással kapcsolatos szempontok	18
2.4. FELHASZNÁLÓI FELÜLET (USER INTERFACE)	19
2.4.1. Mi az a felhasználói felület?	19
2.4.2. IoT - megoldásokkal való interakció módjai	20
2.4.3. Felhasználói felületi szempontok az IoT-hez	20
2.5. IOT - MUNKA FOLYAMAT ÖSSZEFOGLALVA	21
3. LTE TECHNOLÓGIÁK FELHASZNÁLÁSA IOT KERETEIN BELÜL	22
3.1. LTE-M	23
3.2. NB – IoT	23
3.3. 5G NR KITEKINTÉS	24
4. IOT ESZKÖZ BEMUTATÁSA	25
4.1. ESZKÖZ FUNKCIÓK, ALKOTÓRÉSZEK	26
4.2. EMC MÉRÉSI ELV	28
5. ELVÉGZETT MÉRÉSEK	30
5.1. SUGÁRZOTT IMMUNITÁS	30
5.1.1. Mérés leírása	31
5.1.2. Mérés menete	33

5.1.3.	<i>Eredmények</i>	34
5.2.	VEZETETT IMMUNITÁS	35
5.2.1.	<i>Mérés leírása</i>	35
5.2.2.	<i>Mérés menete</i>	36
5.2.3.	<i>Eredmények</i>	37
5.3.	ESD	37
5.3.1.	<i>Mérés leírása</i>	38
5.3.2.	<i>Mérés menete</i>	39
5.3.3.	<i>Eredmények</i>	40
5.4.	EFT.....	42
5.4.1.	<i>Mérés leírása</i>	42
5.4.2.	<i>Mérés menete</i>	43
5.4.3.	<i>Eredmények</i>	44
5.5.	SUGÁRZOTT EMISSZIÓ.....	45
5.5.1.	<i>Mérés leírása</i>	46
5.5.2.	<i>Mérés menete</i>	48
5.5.3.	<i>Eredmény</i>	49
6.	IOT PLATFORM FUNKCIONÁLIS TESZT	53
6.1.1.	<i>Eredmény</i>	54
7.	ÖSSZEFOGLALÁS.....	55
7.1.	KONKLÚZIÓ.....	55
8.	IRODALOMJEGYZÉK.....	56
9.	ÁBRAJEGYZÉK.....	57
10.	MELLÉKLETEK	59

BEVEZETÉS

Minden napos életünk során rengeteg helyzetben találkozhatunk az IoT technológiával, habár legtöbb esetben nem is gondolnánk ezt feltétlenül. Mindenki találkozhatott már úgynevezett „intelligens” eszközökkel, akár a munkahelyén vagy éppen a saját otthonában.

Nem kell messzire mennünk, hiszen egyszerű példa az „okos” telefonunk. A mobilkészülék ugyan nem kifejezetten tartozik az IoT eszközök sorába, viszont rengeteg lehetőséget kínál a felhasználó számára: internet kapcsolatra képes, naplózza a hívási előzményeket, rendelkezik beépített számológéppel, fényképet készít és ez a lista csak folytatódik tovább. Mindezek mellett állandó kapcsolatban áll a gyártóval, illetve a távközlési szolgáltatóval, szoftvere ezáltal képes önállóan frissülni - nem véletlen, hogy az okos jelzöt kapta ez az eszköz.

Ha belegondolunk, miért ne lehetnének a mobil készülékekhez hasonlóan intelligens eszközök akár a háztartási vagy az egészségügyi berendezések, különféle irodai, gyári eszközök, de akár testünkön viselhető készülékek is (pl.: okosóra).

Ugyanakkor ez már nem a jövő kérdése. Olyan technológiákkal rendelkezünk, melyeknek köszönhetően ezek az eszközök intelligensek, illetve összekapcsoltak. Intelligensek, hiszen szoftver dolgozik bennük, érzékelnek, adatokat gyűjtenek, valamint döntés hozatalra és ezek végrehajtására is képesek. Összekapcsoltak, ugyanis kommunikálnak a felhasználóval, gyártóval, ráadásul egymással is.

Egy statisztikai jelentés szerint 2024 végére közel 22 milliárd internethez csatlakozó okos telefon, okos óra, autó és egyéb eszköz lesz. Jelenleg ez a szám világszerte mintegy 14 milliárd. Ez alapján megállapítható, hogy exponenciálisan növekszik az IoT eszközök alkalmazása, illetve a hálózathoz csatlakoztatott egyéb készülékek száma.

A legtöbb eszközt jelenleg a WPAN¹ kategória tartalmazza, ilyenek akár az okos otthonok vagy Bluetooth készülékek. Ezen kívül természetesen még a Wi-Fi technológiát alkalmazó eszközök száma is nagy mértékben növekedett.

Azonban ezeknek az elektromos berendezéseknek alkotórészeit egyre kisebb méretekben gyártják a jelen iparban, ezáltal a fizikai térben közelebb kerülnek egymáshoz, ami veszélyt jelenthet interferencia szempontból. Emiatt különösen fontos, hogy elektromágneses kompatibilitási vizsgálatokat végezzünk el rajtuk, aminek segítségével meggyőződhetünk ezen elektromos eszközök zavarmentes együttműködéséről.

¹ Wireless Personal Area Network

1. IOT – INTERNET OF THINGS – „DOLGOK” INTERNETE

1.1. Mit jelent az IoT kifejezés?

Lényegében az IoT nem más, mint egy globális hálózati infrastruktúra [1]. Ezen a hálózaton keresztül különböző (egyedileg azonosítható) „intelligens” eszközök, tárgyak egymással kommunikálni tudnak. Valamint beépített érzékelők segítségével adatokat is képesek gyűjteni, amelyeket egyénileg kiválasztott vezeték nélküli technológiával egy szerverre ún. IoT platformra [2] továbbítanak adatfeldolgozás, illetve tárolás céljából.

Az IoT kifejezés magát az ökoszisztémát jelenti:

- Eszközök összekapcsolása, kommunikációja, reakciója
- Kommunikációs protokolltól függetlenül képesek kommunikálni egymással (Abban az esetben, ha kompatibilisek)

Pontosabban, az olyan élvonalbeli technológiák, mint a machine learning², a gép-gép (M2M) kommunikáció és a mesterséges intelligencia (AI) előnyeit kihasználva, az IoT célja, hogy a szabványos internet támogatású fizikai eszközökön (okos telefon, asztali számítógép, laptop) túlmutató internetkapcsolatot terjesszen ki az internettel nem rendelkező fizikai eszközök és mindennapi tárgyak széles spektrumára. Például kávéfőzőkre, mosógépekre, kamerákra, autókra stb., ezáltal képesek lehetünk távolról figyelni és vezérelni ezeket egy mobil vagy táblagép segítségével.

1.1.1. IoT elterjedése

Az IoT eszközök, alkalmazások elterjedésében több tényező is közreműködött, ezek többek között a következők:

- Az IP alapú rendszerek (IPv4, IPv6)
- Cloud Computing³
- Fejlett adat analitikai eszközök (Big Data)
- Olcsó, kis méretű IoT modulok (Raspberry Pi, Rádiófrekvenciás modulok)
- Fejlett vezeték nélküli technológiák, protokollok

² Gépi tanulás – mesterséges intelligencia egyik ága

³ Adatfeldolgozó és tároló funkciók ellátása, bárholonnan elérhetővé teszi az IoT-hez köthető szolgáltatásokat, valamint az általuk összegyűjtött adatok is könnyen hozzáférhetők.

1.1.2. Ipari IoT

Az Ipari IoT (IIoT) az IoT-technológia ipari környezetben történő alkalmazására utal, különös tekintettel a felhő technológiákat alkalmazó érzékelők és eszközök műszerezésére és vezérlésére. A közelmúltban az iparágak gép-gép kommunikációt (M2M) használtak a vezeték nélküli automatizálás és vezérlés eléréséhez (1. Táblázat). A felhőalapú és a kapcsolódó technológiák (például az analitika és a gépi tanulás) megjelenésével azonban az iparágak új automatizálási réteget érhetnek el, és ezzel új bevételi és üzleti modelleket hozhatnak létre. Az IIoT-t néha az ipari forradalom negyedik hullámának is nevezik (Ipari 4.0). Néhány gyakori felhasználási területe:

- Intelligens városok
- Megelőző és prediktív karbantartás
- Intelligens gyártás
- Intelligens digitális ellátási láncok
- Összekapcsolt és intelligens logisztika

M2M vs. IoT

M2M	IoT
• Az M2M a gépek közötti közvetlen kommunikációról szól • A pont-pont kommunikációt támogatja • Az eszközök nem feltétlenül támaszkodnak internetkapcsolatra • Az M2M többnyire hardveralapú technológia • A gépek általában egyszerre csak egy géppel kommunikálnak • A készülék mobilon vagy más hálózaton keresztül is csatlakoztatható	• Az IoT az érzékelők automatizálásáról és az internetes platformról szól • A felhőalapú kommunikációt támogatja • Az eszközök internetkapcsolatra támaszkodnak • Az IoT hardver és szoftveralapú technológia egyaránt • Sok felhasználó képes csatlakozni egy időben az interneten keresztül • Az adatkézés az internetprotokoll-hálózattól függ (IP)

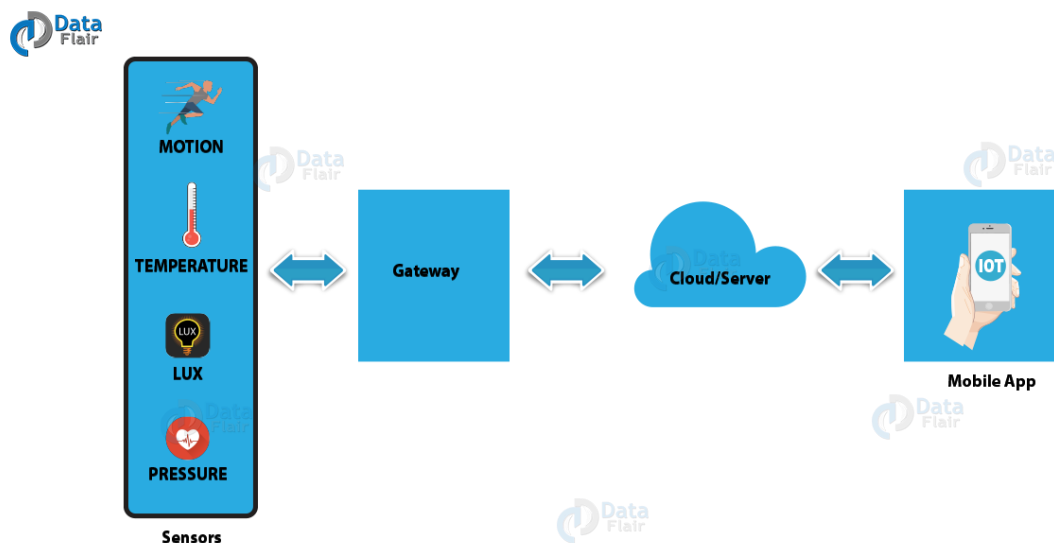
1. Táblázat: Gép – Gép kommunikáció (M2M) és IoT közötti különbségek

2. IOT MŰKÖDÉSI FOLYAMATA

Más rendszerekhez hasonlóan az Internet of Things is rendelkezik előre meghatározott folyamatokkal, illetve alkotórészekkel, melyek segítségével működő képes lesz ez a technológia (1. ábra). A teljes IoT - rendszer négy különböző komponensből épül fel, amelyek együttműködnek a kívánt eredmény megvalósításában:

- Érzékelők
- Vezetéknélküli hálózati csatlakozás
- Adatfeldolgozás
- Felhasználói felület

A következőkben részletesebben bemutatom, hogy ezek az alapvető IoT elemek milyen feladatokat látnak el és hogyan működnek [3].



1. ábra: IoT – architektúra (1)

Az IoT architektúrába tartozik az úgynevezett Node is. Ez általában egy kisméretű eszköz (például mikrokontroller, memória stb.), amely a különböző szenzorokkal van ellátva. Ezek a Node-ok pedig, valamilyen vezeték nélküli technológiával a Gateway-hez csatlakoznak. A Gateway pedig az internethez kapcsolódik, ezzel – a nevéből adódóan – egy átjárót hoz létre a Node-ok által gyűjtött adatok számára, melyek így képesek eljutni az adott felhőalapú szolgáltatásba.

2.1. Érzékelők (Sensors)

Az IoT - munkafolyamat érzékelő eszközökkel kezdődik. Az érzékelők nem újdonságok, hiszen a felhasználók már régóta alkalmazzák őket. Szerepük azonban óriási mértékben megnőtt az Internet of Things növekedésével.

2.1.1. Mit értünk érzékelő alatt?

Az érzékelő olyan eszköz, amely észleli a fizikai környezetből származó bizonyos típusú adatokat, és reagál azokra. A konkrét bemenet lehet fény, hő, mozgás, nedvesség, nyomás, vagy bármely más környezeti jelenség. A kimenet általában olyan jel, amelyet az érzékelő helyén ember által olvasható kijelzővé alakítanak át, vagy elektronikus úton továbbítanak a hálózaton keresztül olvasás vagy további feldolgozás céljából.

Tehát a munkafolyamat első lépéseként, az érzékelő eszközök néhány bites adatokat gyűjtenek az őket körülvevő környezetből. Az összegyűjtött adatok lehetnek olyan egyszerűek, mint egy földrajzi hely, vagy olyan összetettek, mint a beteg egészségügyi alapjai. Az adatok legérzékenyebb változásainak felvételéhez több érzékelőt is össze lehet adni, hogy egy olyan eszköz részei legyenek, amely képes többre, mint a környezeti változók érzékelése. Például, a telefon egy olyan készülék, amely több beépített érzékelőt tartalmaz - legyen az GNSS⁴, kamera, gyorsulásmérő - melyek nélkül a telefon nem képes érzékelni a dolgokat.

Így legyen szó önálló érzékelőről vagy több szenzorral rendelkező eszközzel, az első lépés a környező környezetből származó összes apró részlet összegyűjtését jelenti.

Az IoT platformok különböző típusú intelligenciát és adatokat használnak fel különféle érzékelők alkalmazásával. Mint már említésre került ezek arra szolgálnak, hogy adatokat gyűjtsenek és megosszák azokat a csatlakoztatott eszközök teljes hálózatával. Mindezek az összegyűjtött adatok lehetővé teszik az eszközök önálló, automata működését, ezáltal az egész ökoszisztéma napról napra "okosabb" lesz.

4 Global Navigation Satellite System – Közismertebb nevén GPS (Global Navigation System), amit az USA-ban alkalmaznak

2.1.2. Érzékelő típusok

Az IoT - érzékelő eszközök manapság gyakorlatilag bármihez csatlakoztathatók, de minden használati esethez egy adott típusú érzékelő szükséges. Íme, néhány példa a leggyakrabban használt szenzor típusokra (2. ábra) és azok használati eseteire:

- Hőmérséklet-érzékelők:

A hőmérséklet-érzékelők kritikus szerepet játszanak számos IoT - alkalmazásban. Például a megfelelő hőmérséklet fenntartása számos gyártási folyamat szempontjából kulcsfontosságú. A hőmérséklet távolról történő figyelése az érzékelőkkel prediktív karbantartást tesz lehetővé, és csökkenti a költséges állásidőt. A hőmérséklet-érzékelők másik felhasználási esete a hideglánc-megfigyelés az élelmiszer- és gyógyszeriparban.

- Szintérzékelők:

A szintérzékelők lehetővé teszik például a hulladékgyűjtő konténerek kiürítését a hulladékgazdálkodásban, amikor szükséges. A szintérzékelők másik felhasználási esete a tartályszintek (pl. üzemanyag) mérése a folyékony eszközök nyilvántartásában.

- Gyorsulásmérő érzékelők:

A gyorsulás mérése számos felhasználási esetben hasznos lehet, például a járművek monitorozása esetén. A gyorsulásmérő érzékelők hasznosak lehetnek a gyártógép túlzott rezgésének észlelésében vagy egy olyan tárgy jogosulatlan mozgásában is, amelynek nem szabadna elmozdulnia (lopáselleni védelem).

- GNSS nyomkövetők:

A GNSS nyomkövetők egy eszköz földrajzi helyzetének nyomon követésére szolgálnak. Használhatók például járművekben vagy konténerekben, akár személykövetésre is.

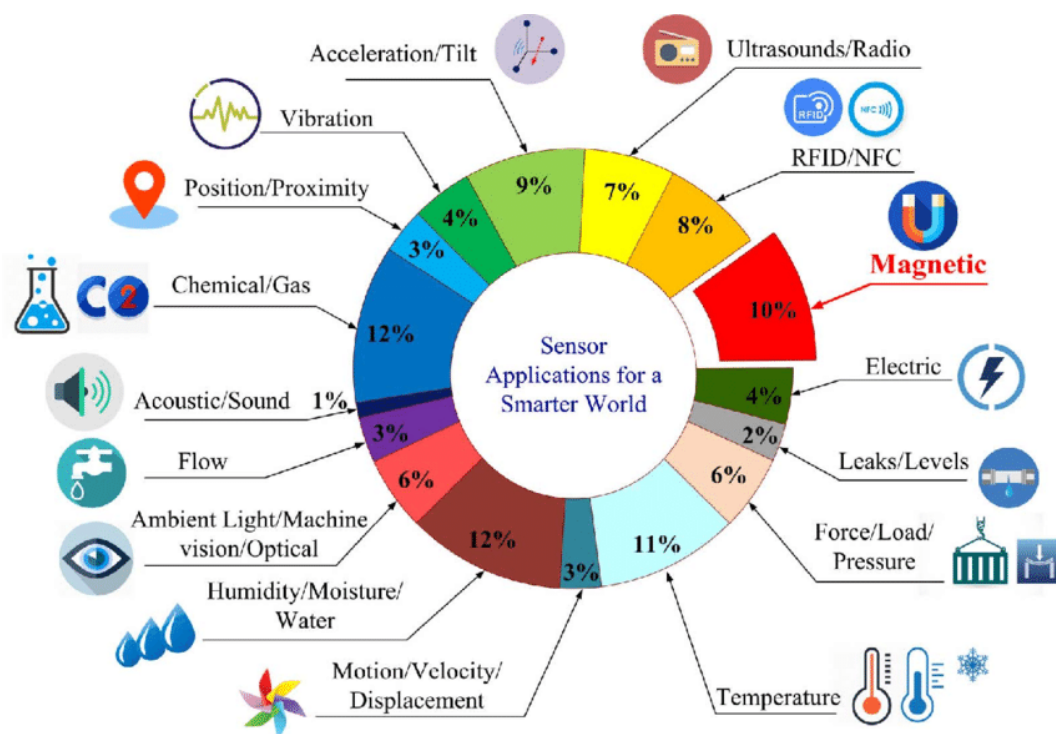
Az érzékelő eszközök kiválasztása fontos lépés egy tervezés során, mert más fontos döntéseket is meghatároz. A kamerák és mikrofonok sok energiát és nagy adatátviteli sebességet igényelnek a hatékony működéshez, Wi-Fi-t kell használniuk, és nagyobb akkumulátorra vagy hálózati táplálásra van szükségük. Ezzel szemben a mozgásérzékelők kisebb adatátviteli sebességet és csak készenléti energiát igényelnek. GNSS modulok esetén szinte mindig kell akkumulátor, különben ezeknek a működése nagymértékben korlátozott lesz.

2.1.3. Jelenlegi kihívások

Vannak olyan tényezők, amelyek korlátozzák az érzékelő eszközök használatát. A legfontosabbak a következők:

- a) Méret
- b) Ár
- c) Akkumulátor élettartam

Nehéz olyan érzékelő eszközt találni, amely kis méretű és olcsó a hosszú akkumulátor-élettartam mellett (pl. öt év). Sok érzékelő eszköz napjainkban még mindig elég terjedelmes a méretét tekintve: például egyes GNSS nyomkövető eszközök mérete hasonló lehet, mint egy mobilkészüléké. A méret összefügg az akkumulátor élettartamával is, minél nagyobb az akkumulátor, annál nagyobb az érzékelő eszköz egyaránt.



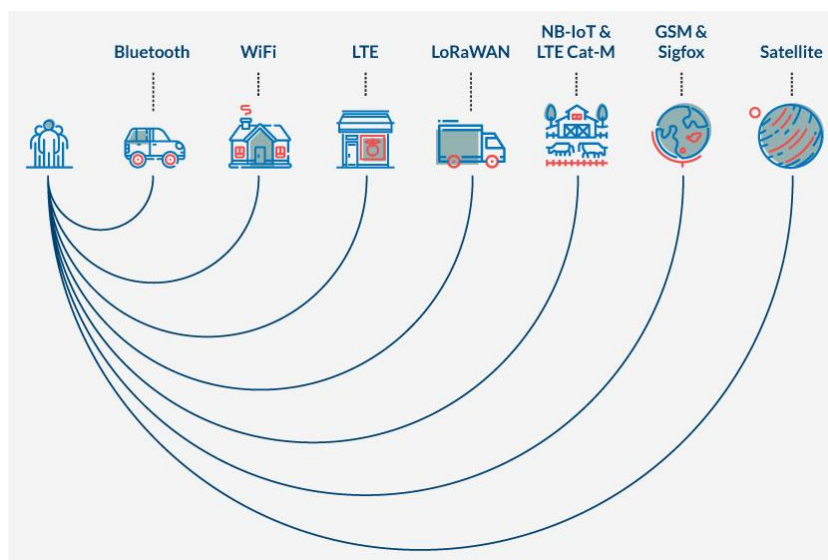
2. ábra: Alkalmazott szenzor típusok (2)

Az érzékelő eszközök méretének, árának és akkumulátor-élettartamának kombinációja azonban a közeljövőben javulni fog a technológia fejlődésével.

2.2. Vezetéknélküli Hálózati Csatlakozás (Connectivity)

Most, hogy az érzékelő eszközök a helyükre kerültek, a következő lépés az, hogy továbbítsuk az összegyűjtött adatokat. Az alkalmazásokban a szenzorok olyan hálózathoz (Wi-Fi, LPWAN⁵, Bluetooth stb.) csatlakoznak, amelyen keresztül az összegyűjtött adatok továbbításra kerülnek (ún. Gateway közreműködésével). A cél, ahová elszeretnénk őket juttatni egy felhőalapú szolgáltatás -ismertebb néven Cloud -, ahol az adatok feldolgozása történik.

Ez a hálózati csatlakozás az IoT azon része, amely lehetővé teszi a "dolgok" kommunikációját és adatcseréjét. A kapcsolat felépítése vezetékes vagy vezeték nélküli hálózaton keresztül valósítható meg. A vezetékes hálózat azonban nem alkalmas a legtöbb IoT - alkalmazáshoz, mivel a hatótávolsága csak addig érhető el, ameddig a vezeték is eljuthat. A legtöbb use case⁶ nagyobb hatótávolságot igényel ennél, ezért ebben a dolgozatban a vezeték nélküli kommunikációra (3. ábra) összpontosítottam.



3. ábra: Vezetéknélküli kommunikációs technológiák (3)

2.2.1. Vezetéknélküli hálózati típusok lefedettség szerint

- (LP)WAN (Wide Area Network) - Pl.: 4G, 5G, LoRa, Sigfox, NB-IoT
- MAN (Metropolitan Area Network) - Pl.: WiMax
- LAN (Local Area Network) - Pl.: Wi-Fi
- PAN (Personal Area Network) - Pl.: Bluetooth

⁵ Low-Power Wide Area Network

⁶ Felhasználási eset

2.2.2. Vezetéknélküli kommunikációs technológiák

Az IoT számos kapcsolódási lehetőséget kínál, például mobil (GSM⁷, LTE⁸), műholdas, Wi-Fi, LPWAN és Bluetooth. A hálózati lehetőség kiválasztásakor több tényezőt kell figyelembe venni: hatótávolság (maximális távolság, amelyen keresztül adatok küldhetők), adatátviteli sebesség (mennyi adat küldhető másodpercenként), energiafogyasztás (akkumulátor élettartam fontossága), költségek, megbízhatóság és lefedettség.

Az optimális hálózati technológia nagy hatótávolságot, nagy adatátviteli sebességet, alacsony költségeket és alacsony energiafogyasztást biztosítana. Sajnos, ez a fajta technológia a jelenben nem létezik. Például a hatótávolság növelése növeli az energiafogyasztást, és az adatátviteli sebesség növelése általában növeli a költségeket (vagy csökkenti a hatótávolságot).

A következőkben az IoT leggyakrabban használt csatlakozási lehetőségeit mutatom be:

- Alacsony fogyasztású, nagyterjedésű hálózat (LPWAN):

A nevéből értetődően, az LPWAN két fontos jellemzővel rendelkezik:

- Alacsony energiafogyasztás (évekig tartó kis akkumulátorokat használ)
- Kommunikáció nagy távolságokon (kilométerben mérve)

LPWAN technológiát az az ötlet alapozza meg, hogy szakaszosan küldjön kis mennyiségű adatot (pl. néhány alkalommal egy nap), amely ezáltal lehetővé teszi az alacsony energiafogyasztást, megnövelve ezzel az akkumulátor élettartamot.

Az egyik felhasználási területe az intelligens hulladékkezelés, ahol a konténerek szintérzékelőkkel vannak felszerelve, és csak szükség esetén ürítik ki őket. Egy ilyen használati esetben elegendő, ha az eszköz bizonyos időszakokban küld kis mennyiségű adatot a felhőbe. Ahelyett, hogy egy valós idejű felügyeleti rendszere lenne, sokkal fontosabb az, hogy az akkumulátor élettartama tovább tartson (pl. több év) és konténereként a költségek is vállalhatóbbak legyenek.

- Műhold (Satellite):

A műholdas kommunikáció nagy sáv szélességű és nagy hatótávolságú, de ez egy nagyon magas energiafogyasztással társul. Az alkalmazása nem gyakori IoT eszközöknél, azonban szinte az egyetlen mód melynek segítségével információt tudunk szerezni egy óceán közepén áthaladó konténerről.

⁷ Global System for Mobile Communications
⁸ Long Term Evolution

- Mobil hálózat (Cellular):

A mobilhálózati kapcsolatnak számos előnye van. Ez egy megbízható opció, amely nagy távolságokra biztosítja a kommunikációt a nagy adatátviteli sebesség mellett. Ráadásul a mobil hálózatok megfelelő lefedettséggel is rendelkeznek.

A mobil kapcsolat hátránya az, hogy viszonylag költséges és magas energiafogyasztás jellemzi. Azonban vannak olyan új mobilhálózatok, amelyeknek célja, hogy ezekkel a problémákkal foglalkozzon. Ezek közül az egyik az NB-IoT⁹, ez egy olyan LPWAN technológia, amely a meglévő mobilhálózati infrastruktúrát használja ki.

- Wi-Fi és Bluetooth:

A Bluetooth és a Wi-Fi jó lehetőség a rövid hatótávolságú kommunikációra. Nagyobb adatátviteli sebességgel rendelkeznek, mint az LPWAN-ok, és alacsonyabb az energiafogyasztásuk, mint a műholdas és a mobil kapcsolatnak.

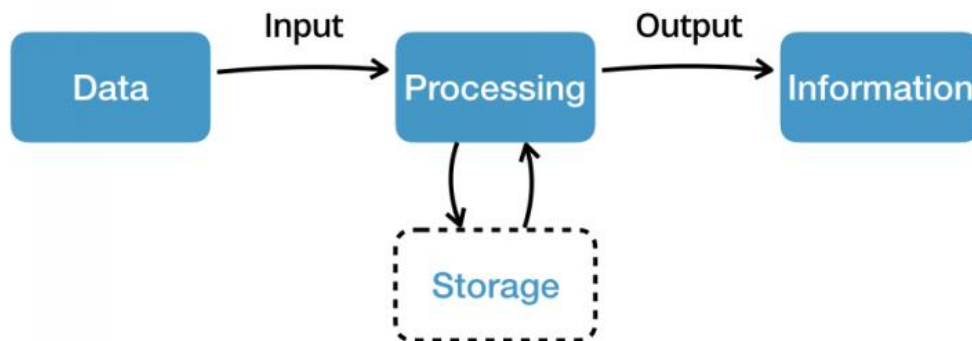
A hagyományos Bluetooth mellett, egy újabb verzió is rendelkezésre áll, ami az úgynevezett Bluetooth Low-Energy (BLE). A BLE-ben használt technológia még alacsonyabb energiafogyasztást tesz lehetővé: A hagyományos Bluetooth által igényelt energiának csak a töredékére van szüksége.

⁹ Narrowband-IoT

2.3. Adatfeldolgozás (Data Processing)

Előzőekben felvázoltam a munkafolyamat első, illetve második lépését, azt, hogy milyen módon gyűjtenek adatokat a szenzorok és ezeket milyen vezeték nélküli technológiák felhasználásával küldik tovább egy felhőalapú szolgáltatásba. Mindezek után a feladat nem más, mint az összegyűjtött adatok használhatóvá tétele, ez tulajdonképpen az adatfeldolgozás. Figyelembe kell vennünk az adatok és az információk közötti különbséget is. Az adatok nyers, szervezetlen tényekre vonatkoznak, és általában meglehetősen használhatatlanok, amíg fel nem dolgozzák őket. Miután az adatok feldolgozásra kerültek, információnak nevezzük.

Annak érdekében, hogy értelmet nyerjen az IoT - érzékelőink által gyűjtött hatalmas mennyiségű adat, fel kell dolgoznunk azokat.



4. ábra: Adatfeldolgozás ciklusa

Tehát az adatfeldolgozás célja, hogy a nyers adatokat valamilyen hasznos információvá alakítsa, amire a végfelhasználó reagálni képes (4. ábra).

Az adat jelen esetben nem más, mint az adatfeldolgozási folyamat bemenete vagy nyersanyaga. Az adatfeldolgozás kimenete pedig az információ. A kimenet különböző formákban, például egyszerű szöveges fájlokban, diagramokon, táblázatokban vagy képeken is megtekinthető a felhasználói felületen. Fontos, hogy az adatfeldolgozás kimenete tárolható (Storage¹⁰) későbbi használatra.

¹⁰ Információk tárolására szolgál

2.3.1. Adatfeldolgozási ciklus

A folyamat általában egy ciklust követ, amely három alapvető szakaszból áll: bemenet, feldolgozás és kimenet.

1. Bemenet:

A bevitel az adatfeldolgozási ciklus első szakasza, az eszköz és a Backend közti kapcsolat megteremtője. Ez egy olyan szakasz, amelyben az összegyűjtött adatokat géppel olvasható formává alakítják át, hogy a számítógép feldolgozhassa őket. Ez egy nagyon fontos folyamat, mivel az adatfeldolgozási kimenet teljes mértékben függ a bemeneti adatoktól.

2. Feldolgozás:

A feldolgozási fázisban a számítógép a nyers adatokat információvá alakítja. Az átalakítás különböző adatmanipulációs technikák alkalmazásával történik, mint például:

- Besorolás: Az adatok különböző csoportokba való beosztása.
- Rendezés: Az adatok valamilyen sorrendben vannak elrendezve (pl. betűrendben)
- Számítás: A numerikus adatokon számtani és logikai műveleteket hajtanak végre.

A besorolási, valamint a rendezési technikák tulajdonképpen az adatbázisnak az alapját alkotják.

3. Kimenet:

Az utolsó szakaszban kapjuk meg a kimenetet. Ez az a rész, ahol a feldolgozott adatokat ember által azonosítható formává alakítják, és hasznos információként mutatják be a végfelhasználónak, ez az úgynevezett Front-end.

A projekt keretein belül fejlesztett Front-end-ről még lesz szó a dolgozat későbbi részében, ugyanis ennek a platformnak, az elkészült eszköznek a helymeghatározási funkcióját teszteltem három különböző GNSS antenna felhasználásával. Ebben az esetben számomra a hasznos információ a felületen megjelenített GNSS koordináta volt.

2.3.2. Adatfeldolgozással kapcsolatos szempontok

Most, hogy már általánosságban ismertettem, hogyan működik az adatfeldolgozás, bevezethetünk néhány szempontot az IoT-ben történő adatfeldolgozással kapcsolatban.

- Kívánt kimenet:

Annak ellenére, hogy az adatfeldolgozási ciklus a bemeneti szakaszban kezdődik, először meg kell gondolni, milyen kimenetet szeretnénk kapni. Más szóval, mik azok a kérdések, amelyeket az IoT segítségével meg kell válaszolni? Milyen információk érdekelnek minket?

Egy példa ilyen esetre az, hogy riasztást szeretnénk kapni, amikor egy adott gyártó gép hőmérséklete meghaladja a küszöbértéket, ez esetben a hőmérséklet, mint információ áll a fókuszban. Ezeket esemény vezérelt technikának nevezzük.

- Adatok tárolása:

A szenzorok által gyűjtött potenciálisan nagy mennyiségű adat miatt általában be kell fektetni egy méretezhető felhőszolgáltatásba (Cloud), hogy képesek legyünk tárolni az adatokat. Ki kell dolgozni egy adatmegőrzési szabályt, tervet is és el kell fogadnunk, hogy nem ésszerű az összes IoT - adatot örökre megőrizni. Minél több adatunk van, és minél tovább tartjuk, annál költségesebb a tárolásuk. Viszont a kevesebb adat kisebb betekintést és csökkenő előzmény referenciát jelent számunkra. Így rangsorolni és egyensúlyban kell tartani a költségeket és a tárolni kívánt adatok mennyiségét.

- Frissítések gyakorisága:

Az adatfeldolgozás végrehajtása előtt fontos eldönteni, hogy mi a megfelelő egyensúly a frissítések gyakorisága és az erőforrások felhasználása (pl. számítási kapacitás, teljesítmény) között. A "jó egyensúly" teljes mértékben az IoT használati esettől függ.

Egyes használati esetekben elengedhetetlen, hogy azonnal tudjuk, hogyan befolyásolja az összegyűjtött adat a kimenetet. Ehhez azonban valós idejű adatfeldolgozásra van szükség, amely nagyon erőforrás-igényes lehet. Néhány más használati esetben elegendő akár naponta egyszer az összegyűjtött adatok feldolgozása.

- Adatfeldolgozó eszközök:

Egy teljes IoT rendszerhez szoftverre van szükség. Ezt a bizonyos szoftvert a Cloud tárolja. Feladata, hogy összegyűjtse az eszközök által küldött adatokat, elemzéseket végezzen rajtuk – különféle analitikai módszerek segítségével - és önálló döntéseket hozzon az IoT rendszeren belül végrehajtandó műveletekről.

2.4. Felhasználói felület (User Interface)

Az előzőekben azt tárgyaltam, hogyan gyűjtik az adatokat az érzékelő eszközök, hogyan küldik el ezeket egy felhő alapú szolgáltatásba valamilyen hálózati megoldáson keresztül, és milyen módon alakulnak át hasznos információkká az adatfeldolgozás során. Az utolsó lépés, amit meg kell tennünk, hogy az információt eljuttatjuk a végfelhasználónak (end-user). Ez pedig a felhasználói felületen keresztül valósítható meg (röviden UI¹¹).

2.4.1. Mi az a felhasználói felület?

A felhasználói felület azokat a szolgáltatásokat tartalmazza, amelyekkel a felhasználó interakcióba lép a számítógépes rendszerrel. Ez magában foglalja a képernyőt, oldalakat, gombokat, ikonokat, űrlapokat stb.



5. ábra: Felhasználói felület, „okos” otthon világítás vezérléshez (4)

A felhasználói felületek legkézenfekvőbb példái a számítógépeken és okostelefonokon található szoftverek és alkalmazások (5. ábra).

A felhasználói felület azonban nem feltétlenül igényel képernyőt. Például egy TV-távírányító felhasználói felülete különböző gombokból áll, és létezik olyan eszköz, amely hangparancsokkal vezérelhető.

¹¹ User Interface

2.4.2. IoT - megoldásokkal való interakció módjai

Többféle mód van, amellyel a felhasználó kommunikálhat egy IoT - megoldással. Akárcsak az érzékelő eszközöknél vagy a hálózati technológiáknál, a választás itt is a használati esettől függ. Vessünk egy pillantást néhány leggyakoribb lehetőségre:

a) Automatikus értesítések fogadása:

A legáltalánosabb eset az IoT - alkalmazásokban, hogy értesítéseket vagy riasztásokat szeretnénk kapni, ha valami szokatlan történik. Ha például egy gyártógép hőmérséklete túllépi a küszöbértéket, erről értesítést szeretnénk kapni. Az információ e-mailben, SMS-ben, telefonhívással vagy push értesítéssel is elérhető.

b) Információk proaktív figyelése:

Lehet, hogy proaktív módon szeretnénk figyelni az információkat. Például, ha lenne egy eszközkövető megoldásunk, amely nyomon követné a járműveinket, akkor is nyomon követhetnénk a járművek helyét, ha semmi szokatlan nem történik. Használhatunk egy mobil vagy számítógépes alkalmazást az információk megfigyelésére.

c) A rendszer távvezérlése:

Az UI azt is lehetővé teszi a felhasználó számára, hogy távolról vezérelje az IoT - rendszert. Például, a felhasználó képes lehet lámpák fényének állítására vagy akár a fűtés kikapcsolására mobil alkalmazás segítségével. Ezt az alkalmazás automatikusan is elvégezheti a neki adott iránymutatásoknak megfelelően.

2.4.3. Felhasználói felületi szempontok az IoT-hez

Kihívást jelent akár egyetlen alkalmazáshoz is létrehozni önálló felhasználói felületet, de az IoT - alkalmazások teljesen új szintre emelik a komplexitást. Nézzünk meg pár olyan kérdést, amelyet figyelembe kell venni az IoT felhasználói felületének tervezésekor:

- Vezetéknélküli hálózati csatlakozás:

Vannak különböző megközelítések afelől, hogy milyen gyakran küldünk adatokat a felhőbe (és hogy milyen gyakran dolgozzák fel azokat). Ezt figyelembe kell venni a felhasználói felület tervezésekor. Ha például egy helykövető három óránként küld adatokat a platformra, akkor a felhasználói felületnek egyértelműen tájékoztatnia kell a felhasználót arról, hogy nem valós idejű információkat lát. A felhasználói felület tudathatja a felhasználóval, hogy "Az utolsó üzenet 2 órával ezelőtt érkezett – a következő üzenet várhatóan 1 óra múlva lesz".

- Fizikai felhasználó felület:

El kell gondolkodni azon, hogy szükség van-e fizikai felhasználói felületre az IoT - eszközön. Egyes alkalmazásokban ez alapvető fontosságú lehet. Például, ha „okos” világítás lenne otthonunkban, azt szeretnénk, hogy képesek legyünk használni a rendszert akkor is, ha a Wi-Fi hálózat éppen nem elérhető. A fizikai UI azonban esztétikai okokból gyakran nagyon korlátozott, és azért is, mert meg akarjuk hosszabbítani eszközeink akkumulátorának élettartamát. A fizikai felhasználói felület olyan egyszerű is lehet, mint egy LED - es lámpa az érzékelő eszközön, ami megmondja a felhasználónak, hogy az eszköz be van kapcsolva.

- Teljesítmény:

Hatékony adatfeldolgozás mellett is hatalmas mennyiségű információ jelenhet meg a felhasználói felületen. Emellett nem szabad elmenni az UI tervezésekor, mert ellenkező esetben előfordulhat, hogy a felhasználói felület teljesítménye nem lesz méretezhető nagyobb szintű használatra. A grafikonok nagyszerű lehetőséget nyújtanak a nagy mennyiségű adat érthető módon való bemutatására, és segítenek az UI teljesítményében is.

2.5. IoT - Munkafolyamat összefoglalva

A következő ábra röviden összefoglalja (6. ábra) az előzőekben ismertetett folyamatot:



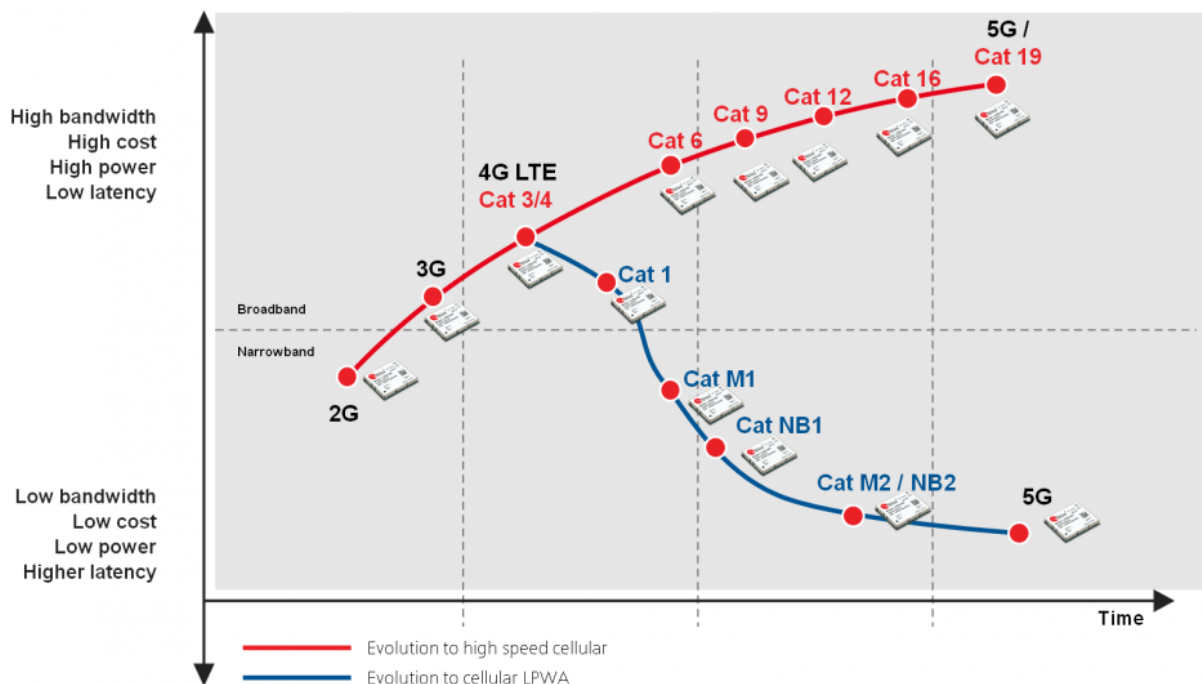
6. ábra: IoT – munkafolyamat összefoglalva (5)

Az egész folyamat a szenzorok adatgyűjtésével kezdődik, ezek a szenzorok valamilyen vezeték nélküli kommunikációs technológiával kapcsolódnak a hálózatra. A hálózat segítségével eléri a szervert vagy Cloud-ot, ahova az összegyűjtött adatokat továbbítják tárolás, valamint további feldolgozás céljából. Az utolsó lépés, hogy ezen feldolgozott információkat a végfelhasználónak egy User Interface-en keresztül megjelenítjük.

3. LTE TECHNOLÓGIÁK FELHASZNÁLÁSA IOT KERETEIN BELÜL

Az 5G technológiával a láthatáron, a 2G és a 3G hálózatok fokozatosan megszűnnek, és az LPWAN-t támogató új hálózati technológiák világszerte elérhetővé válnak LTE-M és NB-IoT, más néven Mobile IoT formájában (7. ábra). Mindkettő azzal a céllal jött létre, hogy különösen alkalmas legyen a globális IoT - kapcsolat engedélyezésére [4].

Az LTE-M és az NB-IoT egyaránt jó hálózati megoldást kínál az olyan iparágak számára, amelyek ki szeretnék használni az LPWAN technológiát, amely javítja az eszközök akkumulátorának élettartamát, és olyan eszközöket csatlakoztat a hálózathoz, melyeket korábban nehéz volt elérni. Mindkettő technológia ma elérhető, szabványosított és a 4G hálózatra épül, ami azt jelenti, hogy időtállóak, globális hálózati lefedettséggel rendelkeznek, illetve GSMA és a távközlési szabványok támasztják alá őket (Licencelt spektrum).



7. ábra: LTE-M és NB-IoT fejlődése

Az LTE-M és az NB-IoT olyan IoT - eszközöket támogat, melyek hosszú akkumulátor-üzemidőt igényelnek, vagy amelyeket olyan helyeken használnak, ahova a normál 4G technológiával nehéz elérni, például mély beltéri helyeken. Tehát miben különböznek, és milyen hatással lesznek a piacra [5]?

3.1. LTE-M

Az LTE-M (LTE-MTC¹² és LTE Cat M néven is ismert) egy LPWAN technológia, amely lehetővé teszi a meglévő LTE infrastruktúra újra felhasználását kiterjesztett lefedettséggel. Az LTE-M a 3GPP¹³ által kifejlesztett technológia, amely képessé teszi az eszközök és szolgáltatások használatát kifejezetten IoT - alkalmazásokhoz. Az LTE-M 1 Mbps adatátviteli sebességet kínál, amely maximálisan 4 Mbps sebességre emelkedik és 1,4-5 MHz sávszélességet használ.

Ez a technológia főleg az ipari felhasználásokra lett kifejlesztve. A késleltetése sokkal kisebb, mint az NB-IoT-nek, ezért jól alkalmazható már a gyártósorokon, szerelőrobotok, gépek adatkommunikációjához, közel valós idejű alkalmazásoknál is használható. Ugyanakkor a költsége jóval nagyobb, az energiafogyasztása szintén, viszont képes akár hangátvitelre is.

3.2. NB – IoT

A Narrowband-IoT (keskenysávú kapcsolaton keresztül működő) ugyancsak a 3GPP által kifejlesztett LPWAN rádiótechnológiai szabvány, amely az IoT- megoldásokra optimalizált és a meglévő mobilhálózatra épül, így a hagyományos mobilhálózatokkal szemben támasztott szigorú minőségi követelményeknek kell megfelelnie. Viszont az NB-IoT nagyságrendekkel alacsonyabb energiaigényű és jóval nagyobb hatótávolságú, mint a hagyományos mobilhálózatok.

Ez a technológia különösen olyan felhasználási módoknál optimális, ahol sok, vagy éppen nehezen hozzáférhető helyszínen működő szenzorokon keresztül kell kevés adatot begyűjteni (kis adatforgalom). Az eszközök nagy távolságból elérhetőek (10-20 km), kis energiafogyasztásúak, ezért megnövekedett akkumulátor élettartammal rendelkeznek (kb. 10 éves élettartamra tervezik őket). Maximum 127 Kbps adatátviteli sebességre képes, késleltetése nagy, tulajdonképpen naponta néhány üzenetküldésre lett méretezve (például intelligens mérőórák). Az NB-IoT a sávszélességet egyetlen 200 kHz-es keskeny sávra korlátozza. Ez a frekvenciaspektrum kihasználásának szempontjából előnyös tulajdonság.

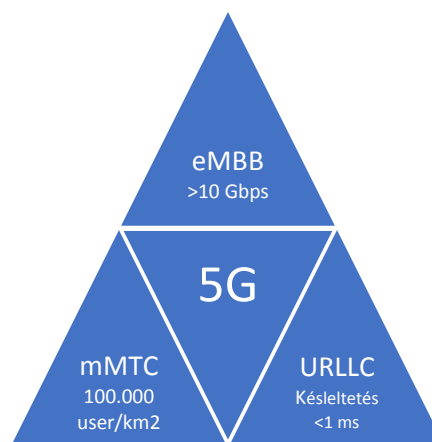
¹² Machine Type Communication

¹³ 3rd Generation Partnership Project

3.3. 5G NR Kitekintés

Az 5G nem más, mint az ötödik generációs mobilhálózat. Az 5G vezeték nélküli technológia célja, hogy nagyobb, több Gbps-os csúcs adatsebességet (10 Gbps), ultra alacsony késleltetést (~ 1 ms), nagyobb megbízhatóságot, masszív hálózati kapacitást (100.000 felhasználó/km²), nagyobb rendelkezésre állást és egységesebb felhasználói élményt nyújtson több felhasználónak [6].

5G hálózatoknál már elkülönítik a különböző felhasználási lehetőségeket, a különböző adattípusokat, adatforgalmakat. Ezek három fő kategóriába (8. ábra) sorolhatók:



8. ábra: 5G use case kategóriák

- eMBB (evolved Mobile Broad Band):

Nagy adatforgalmú mobil felhasználás, ami nem késleltetés kritikus. Az eMBB jelenleg azokat a területeket célozza meg, ahol egyre nagyobb adatátviteli sebességre van szükség. Emellett lehetővé teszi az új IoT- használati eseteket, amelyek nagy adatforgalmat igényelnek, például a video streamelést.

- mMTC (massive Machine Type Communication):

Massive IoT (mIoT) néven is ismert; a jelenlegi IoT- szolgáltatások kiterjesztése, amely magában foglal szinte minden gép-gép közötti kommunikációt. Ilyenek például: Okosváros, Intelligens közlekedési rendszerek.

- URLLC (Ultra Reliable Low Latency Communication):

Azok a felhasználási esetek tartoznak ebbe a kategóriába, amelyek késleltetéskritikusak és nagy rendelkezésre állást igényelnek. Fontos tehát a kis késleltetés és a kapcsolat stabilitása, valamint a megbízhatóság. Például ide tartoznak: önvezető autók, valós idejű megfigyelő rendszerek, távoli műtét.

4. IOT ESZKÖZ BEMUTATÁSA

Mindezen elméleti háttér azt a célt szolgálja, hogy jobban átláthatóbb és érthetőbb legyen az Internet of Things technológiának az alapelve és működési folyamata. Röviden visszautalva néhány részletre, amely fontos abból a szempontból, ha kifejezetten IoT felhasználásra szeretnénk eszközt fejleszteni: Legtöbb esetben az ilyen típusú eszközöket úgy tervezik, hogy összeszerelést, illetve tesztelést követően az adott felhasználási területen működésbe helyezik és ezek után tulajdonképpen több teendő nincsen az adott készülékkel. Ugyanakkor ez kizárólag csak akkor igaz, amennyiben az eszközben elhelyezett akkumulátor élettartama megfelelő, az az több éven keresztül képes működtetni egy eszközt. Ehhez természetesen hozzá segítenek azon LPWAN technológiák (LTE-M, NB-IoT) melyeket a dolgozat korábbi részében (3) megemlítettem.

Azonban nem minden esetben ezeket a kis adatátviteli sebességre tervezett technológiákat alkalmazzák, erre egy remek példa a projekt fejlesztése által megalkotott eszköz (9. ábra), amelynek a tesztelését, mérését 4G LTE kommunikáció mellett végeztem. Ennek következtében merültek is fel problémák a mérések során, ezekről a későbbiekben tesztek említést.



9. ábra: IoT Platform V1.0 eszköz panel

Fent látható ez az IoT eszköz, egyelőre tokozás és antenna nélkül. A panel alatt található az eszközt működtető akkumulátor. Maga a kapcsolási rajz, PCB¹⁴ terv elkészítése nem tartozott a saját feladatköreim közé, emiatt csak azokat az információkat, funkciókat ismertetem, amelyek számomra lényegesek voltak a vizsgálatok elvégzésének szempontjából.

¹⁴ Printed Circuit Board – Nyomtatott Áramkör

4.1. Eszköz Funkciók, Alkotórészek

Említésre került, hogy az eszközön való vizsgálatok elvégzéséhez nem feltétlen van szükség minden apró részlet ismeretére a nyomtatott áramkörrel kapcsolatban, ugyanakkor a mérések megkezdése előtt fontos utánajárni azoknak a funkcióknak, amelyek segíthetik adott esetben a vizsgálat folyamatát. Tipikusan ebbe a kategóriába tartoznak az állapot visszajelző LED¹⁵-ek.



10. ábra: Állapotjelző LED-ek (balról-jobbra haladva, LED1-LED6-ig bezárólag)

Első lépésként az ábrán látható (10. ábra) LED-ek működését kellett megismernem, annak érdekében, hogy a mérések során visszacsatolást kapjak az eszköz aktuális állapotáról.

Többféle LED közül a következők a lényegesebbek:

- LED1: A tápellátás bemenet csatlakoztatva van (CHG port-ra csatlakozó USB kábel)
- LED2: Úgynevezett „Heartbeat” LED, amely jelzi a mikroprocesszor működését
- LED3: Abban az esetben jelez, ha az eszköz töltés alatt van
- LED4: MQTT szerverrel való kommunikáció folyamatban van

Ez utóbbi funkciót a panel felső részén található „SW1” kapcsolóval lehet engedélyezni, a közvetlen mellette elhelyezkedő „SW2” pedig az eszközt Low-Power üzemmódba képes kapcsolni.

Ezekén kívül az mPCIe¹⁶ csatlakozó alatt egy kisebb méretű LED is van, melynek az a feladata, hogy jelezze a Rádiófrekvenciás modul helyes működését.

¹⁵ Light-emitting Diode

¹⁶ Mini-Peripheral Component Interconnect Express

Az eszközben alkalmazott Rádiófrekvenciás modul (11. ábra) maximális 150 Mbps downlink sebességet és 50 Mbps uplink sebességet biztosít LTE technológia alatt, és a meglévő 2G hálózatokkal való visszamenőleges kompatibilitás biztosítja a kapcsolatot még az olyan területeken is, ahol nincs 3G vagy 4G lefedettség. A hálózatra való csatlakozáshoz egy SIM kártya szükséges, amelynek elhelyezésére az alábbi ábrán látható módon van lehetőség.



11. ábra: Alkalmazott RF modul

A választás azért erre a Rádiófrekvenciás modulra [7] esett, mert a szabványos mPCIe csatlakozóra integrált modul nagymértékben megkönnyíti, illetve felgyorsítja a tervezési fázist. Ugyanis a panelre egy M.2 foglalat segítségével egyszerűen csatlakoztatható, valamint cserélhető is más típusú modulra szükség esetén. Továbbá ez az RF modul úgynevezett CE¹⁷ jelöléssel rendelkezik (12. ábra), ami annyit jelent, hogy a termékre vonatkozó – EU által támogatott - előírásoknak eleget tesz és az Európai Unión belül forgalmazható.



12. ábra: CE jelölés

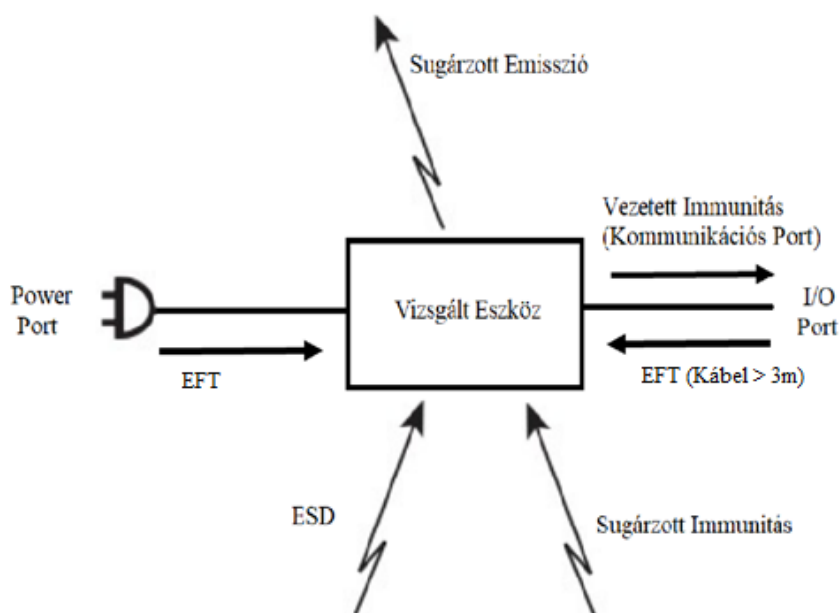
Ez a szempont pedig a méréseknél jelent előnyt, hiszen elektromágneses kompatibilitási teszteket kell elvégezni az eszközön, viszont maga a vezeték nélküli kommunikációért felelős modul ezeknek a vonatkozó szabványoknak megfelel. A következő fejezetben ismertetni fogom, hogy miért is van szükség elektromágneses kompatibilitás vizsgálatok elvégzésére.

17 Conformité Européenne

4.2. EMC Mérési Elv

Előzőekben szó esett arról, hogy elektromágneses összeférhetőségi, kompatibilitási, az az EMC¹⁸ vizsgálatokat kell elvégezni az eszközön. Természetesen ez nem kizárólag erre az egy készülékre vonatkozik:

Elektromágneses összeférhetőség mérésére azért van szükség, hogy megbizonyosodjunk arról, hogy egy adott elektromágneses elven működő eszköz, berendezés zavartalanul tudjon működni különböző elektromágneses zavarok környezetében (immunitás), illetve arról, hogy a vizsgált eszközünk elektromos zavarkibocsátása más készülékek működését nem akadályozza (emisszió).



13. ábra: EMC mérési összeállítás

Ezen az egyszerűsített ábrán illusztrálom (13. ábra), hogy általánosságban milyen típusú EMC vizsgálatokat kell elvégezni egy adott készüléken. Ezek mellett többféle teszt is létezik, ebben az esetben azokat szemléltetem, melyeket elvégeztem az IoT eszközön, ezen méréseket az erre vonatkozó fejezetben (5) részletesebben bemutatom.

Az EMC vizsgálatok helyes és pontos megvalósítása érdekében szabványokat hoztak létre, melyek szigorú előírásként, illetve útmutatóként szolgálnak minden mérés során.

18 Electromagnetic Compatibility

Az EMC szabványok [8] meghatározzák az elektromágneses kompatibilitás feltételeit, szabályait, vizsgálati módszereit, emissziós határértékeit és immunitási szintjeit. Ezeket eszköz specifikusan alkalmazzuk a mérések során.

Mielőtt a vizsgálati folyamatokat elkezdjük, szükség van a DUT¹⁹, az az a vizsgált eszköz besorolására egy fajta kategóriába, ugyanis ez alapján tudjuk kiválasztani a megfelelő szabványt, szabványokat. Ilyen kategória lehet például ipari felhasználású készülék, akár háztartási berendezés; elsődleges lépés tehát, hogy a vizsgálni kívánt eszközt besoroljuk valamely típusba. Miután ez megtörtént, a vonatkozó szabvány alapján el tudjuk kezdeni az abban meghatározott tesztek.

Az általam vizsgált IoT eszközt a Multimédia-készülék típusba soroltam, majd az ehhez kapcsolódó szabványokat kiválasztottam és tanulmányoztam:

- MSZ EN 55035:2017 - Ez a szabvány az immunitási követelményeket adja meg a Multimédia-készülékek elektromágneses összeférhetősége kapcsán
- MSZ EN 55032:2015 - Ez pedig az emisszióval kapcsolatos kritériumokat fogalmazza meg a Multimédia-készülékek EMC vizsgálata szempontjából

Minden szabvány tartalmaz úgynevezett záradékokat (14. ábra), amelyek táblázatba vannak foglalva különböző teszt pontokat tekintve (AC vagy DC port-ra értelmezendő előírások stb.)

Table 1 – Immunity requirements for enclosure ports

Table clause	Environmental phenomenon	Test specification	Units	Basic standard	Remarks	Performance criteria
1.1	Power frequency magnetic field	Frequency Field strength	50 or 60 1 Hz A/m	IEC 61000-4-8	See ^a	A
1.2	Continuous RF electromagnetic field disturbances, swept test	Frequency range Field strength	80 to 1 000 3 MHz V/m	IEC 61000-4-3 or IEC 61000-4-20 or IEC 61000-4-21	For modulation details see 4.2.2.1	A
1.3	Continuous RF electromagnetic field disturbances, spot test	Frequency (±1 %)	1 800, 2 600, 3 500, 5 000 MHz	IEC 61000-4-3 or IEC 61000-4-20 or IEC 61000-4-21	For modulation details see 4.2.2.1	A
		Field strength	3 V/m			
1.4	ESD	Contact discharge Air discharge	4 8 kV	IEC 61000-4-2		B

^a Applicable only to equipment containing devices intrinsically susceptible to magnetic fields, such as CRT monitors, Hall effect elements, electro-dynamic microphones, magnetic field sensors or audio frequency transformers. Refer to D.3.2 for determining the test level when the EUT contains a CRT display.

NOTE The applicable versions of the basic standards are IEC 61000-4-2:2008, IEC 61000-4-3:2006/AMD1:2007/AMD2:2010, IEC 61000-4-8:2009, IEC 61000-4-20:2010 and IEC 61000-4-21:2011. See Clause 2.

14. ábra: EMC szabvány záradék (Table Clause)

Ezen záradékok segítségével határoztam meg, hogy milyen vizsgálatokat kell elvégezni az eszközön, valamint azt is, hogy mely mérések alkalmazandók kizárólag egy adott feltétel teljesülése mellett (Pl. 3 m-nél nagyobb kábelhosszúságot támogató portok esetén).

¹⁹ Device Under Test (vagy EUT- Equipment Under Test)

5. ELVÉGZETT MÉRÉSEK

Az IoT eszköz különféle funkcióinak ismeretében és a vonatkozó szabványok tanulmányozását követően el tudtam kezdeni az EMC vizsgálatokat.

A méréseknél felhasznált eszközök egyes esetekben különböztek, ezeket az adott vizsgálat fejezetében részletezem. Továbbá az IoT eszköz megfelelő működéséről való visszacsatolás szerzésének a módszere is változó volt a mérések jellegétől függően.

A mérésekről jegyzőkönyveket készítettem (=20210624-1-1=; =20210624-1-2=), melyek a mellékletben elérhetők. Ezek tartalmazznak olyan többlet eredményeket, képeket, amelyek adott esetben a dolgozatban nem szerepelnek.

5.1. Sugárzott Immunitás

Az első vizsgálat, amelyet elvégeztem a Sugárzott immunitás volt, szabvány megnevezés alapján Continuous RF electromagnetic field disturbances.

A Sugárzott immunitás mérésének az a célja, hogy az adott villamos berendezés zavartűrő képességét vizsgáljuk olyan nagyfrekvenciás zavarokkal szemben, amelyek a levegő közegén keresztül terjednek és más villamos/elektromos készülék által keletkeztek.

Ezen vizsgálatokat minden esetben árnyékolt kamrában (FAC²⁰) kell elvégezni, hogy a mérés során a környezetet ne zavarjuk a sugárzással. Jelen esetben GTEM cellás megoldást használtam, mely kiváltja az antennát és az árnyékolt helyiséget. Erre az opcióra többek között az IoT eszköz méretéből és a vizsgálandó frekvencia tartományból adódóan volt lehetőségem.

A teszteléshez felhasznált mérő és segédeszközök a következők voltak:

- RF jelgenerátor – Agilent, RFG-3
- Erősítő – R&S, PA1G-2
- GTEM Cella
- RF kábel
- MQTT Explorer (Szoftver)
- Frequency Stepper (Szoftver)

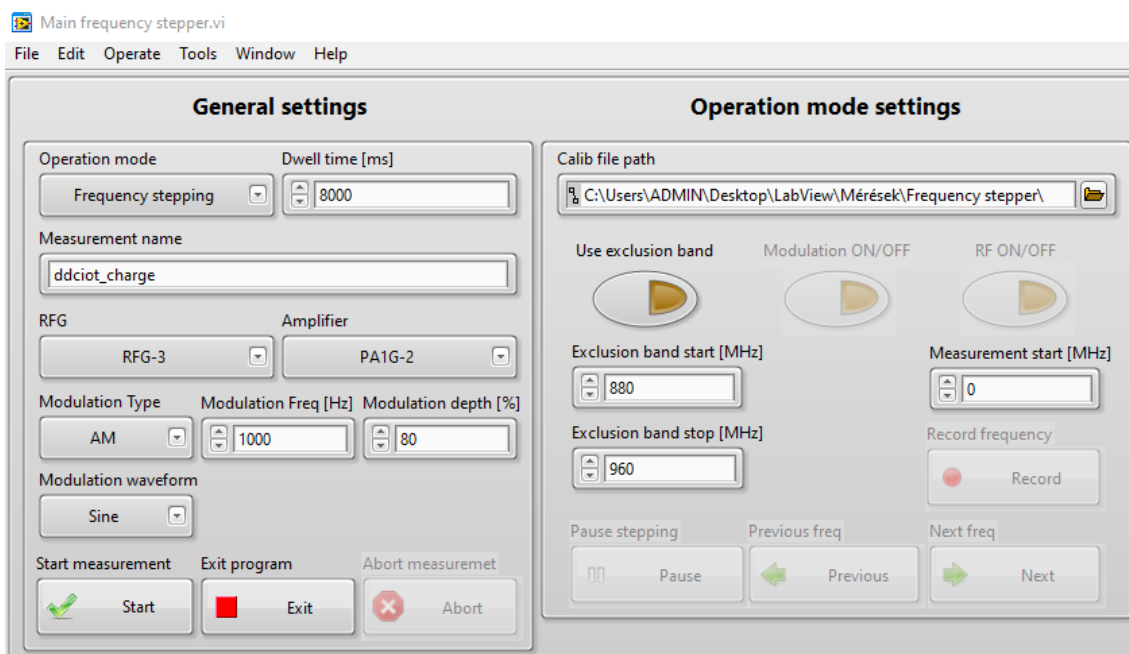
²⁰ Fully Anechoic Chamber

5.1.1. Mérés leírása

A mérés során az MSZ EN 55035 szabványban meghatározott „1.2” záradék szerint jártam el. Amelyben a következő előírások szerepelnek a vizsgálatra vonatkozóan:

- Frekvenciatartomány: 80-1000 MHz
- Térerősség: 3 V/m

Alapvetően a GTEM cellában elhelyezett eszközt a meghatározott frekvenciatartományon belül szükséges vizsgálni. Azonban, ha a frekvenciák közötti váltást manuálisan végeznénk, akkor a mérés ebből kifolyólag több időt venne igénybe. Ennek a problémának a kiküszöbölésére lett megalkotva a vizsgáló laboratórium által az úgynevezett Frequency Stepper (15. ábra) mérőprogram.

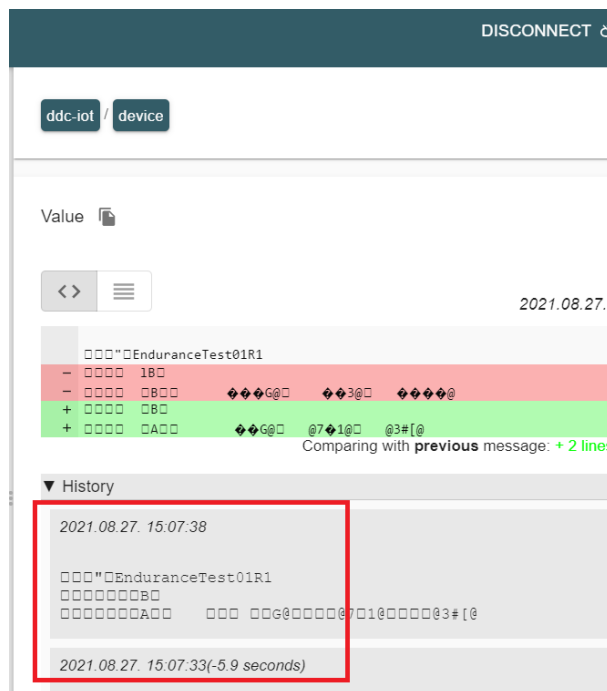


15. ábra: Frequency Stepper szoftver

A mérőprogram tulajdonképpen a jelgenerátort és az erősítőt vezérli, amelyeket egy RF kábel felhasználásával csatlakoztattam egymáshoz. A szoftverbe betöltöttem egy előre generált fájlt, aminek a segítségével megadtam, hogy mely frekvenciatartományon belül kell elvégezni a frekvencia léptetést és mekkora térerősség mellett.

Ezek mellett lehetőség van a moduláció beállítására is, melyet a szabvány határoz meg. Továbbá a léptetés időközének megadására is van opció (Dwell time), ez alapérték szerint 1 s. Ugyanakkor az egy másodperces frekvencia léptetés nem felel meg minden esetben, ahogy az IoT eszköz esetében sem. Ugyanis a SIM kártyával ellátott modul 6 s-es időközönként küld adatot egy MQTT szerverre.

A mérés során a GTEM cellában elhelyezett készülék működéséről, ennek a kommunikációnak a segítségével kaptam visszajelzést (16. ábra).



16. ábra: MQTT Explorer felület

A fenti ábrán látható bekeretezett rész mutatja a szerverre sikeresen kézbesített üzeneteket. Az előzmény felület két beérkezett adat között eltelt időt jeleníti meg (5,9 s), ennek köszönhetően tudtam vizsgálni az eszköz működésében esetlegesen fellépő hibákat.

Az eszköz és az MQTT szerver kommunikációjának a feltétele, hogy az RF modulba egy SIM kártyát helyezünk. Amennyiben az eszköz képes csatlakozni az adott 4G hálózatra, akkor sikeresen tud üzenetet küldeni az MQTT protokoll közreműködésével.

Viszont a GTEM cella egy árnyékolt berendezés, ennek következtében nincs megfelelő jelerősség a készülék és a mobilállomás közötti kapcsolathoz. Emiatt szükség volt egy alternatív megoldásra, mégpedig az antenna csatlakozót ki kellett vezetnem a cellából egy RF kábel felhasználásával. Így az eszköz antennája árnyékolt helyiségen kívül volt csatlakoztatva, ezáltal a bázisállomással való kommunikáció fel tudott épülni, aminek köszönhetően az MQTT szerver is fogadni tudta az adatfolyamot.

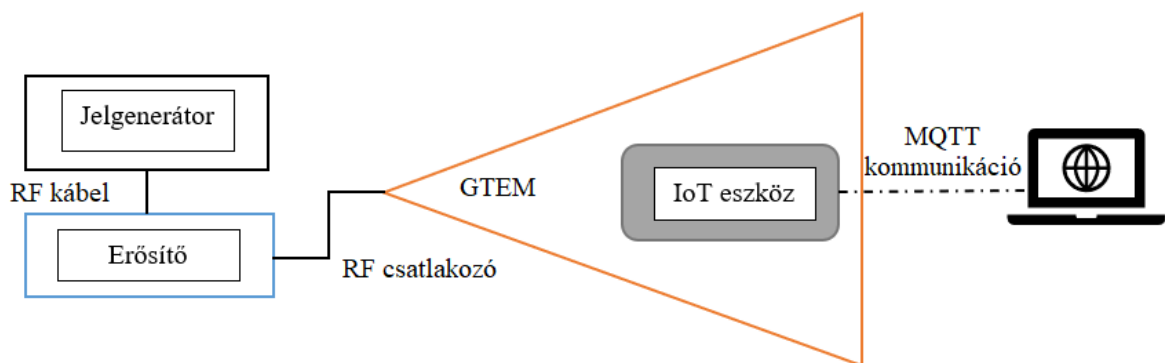
A vizsgálat elvégzéséhez szükség volt úgynevezett exclusion band megadására, ami annyit jelent, hogy az abban megadott frekvenciasávot a mérőprogram átlépi. Ezeket a kivétel frekvenciákat szintén szabványok határozzák meg, jelen esetben a 880-915/925-960 MHz-es mobilkommunikációs sávokat kellett kivenni a vizsgált tartományból.

5.1.2. Mérés menete

Az alapszabvány, amely meghatározza a Sugárzott immunitás vizsgálatának folyamatát: IEC 61000-4-3

A vizsgálat megkezdése előtt szükség van egy mérési összeállításra, majd ezek után a mérőprogram beállítására a vonatkozó előírásoknak megfelelően.

A mérési folyamatot a következő összeállítás (17. ábra) alapján végeztem:



17. ábra: Sugárzott immunitás mérési összeállítás

Elsődlegesen a jelgenerátor RF output kimenetét és az erősítő műszer bemenetét 1 m hosszúságú RF kábellel kötöttem össze, majd az erősítőt a GTEM cella csatlakozójára vezettem, utóbbi esetben 3 m hosszúságú kábelt használva. Ezek után az IoT eszközt a GTEM cellában kijelölt helyre helyeztem, majd ellenőriztem az MQTT szerverrel való kommunikáció felépülését.

A mérőprogramot beállítottam a szabványnak megfelelő módon. A szoftver egy kalibráció alapján elmenti a frekvenciasávokhoz tartozó teljesítményszintet a megfelelő térerősség szint tartása érdekében és ennek felhasználásával léptet a mérés közben. A beállításokat annyiban módosítottam, hogy a frekvencia léptetési idő 8 másodperc legyen, ezzel igazodva az eszköz 6 másodperces adatküldéséhez. Ez fontos lépés, hiszen hiba esetén ezzel a módszerrel tudtam pontosan megállapítani a zavart okozó frekvenciasávokat.

Ez viszont nagymértékben megnövelte a vizsgálat idejét, ami abból a szempontból okozott problémát, hogy a 4G hálózaton keresztül üzemelő eszköz akkumulátora a mérés során lemerült. Ugyanis ahogy az előző fejezetben (4) említettem, ezeket az eszközöket kis adatforgalomra tervezik, ez az IoT eszköz sem kivétel ez alól. Azonban a tesztelési fázisban ez a „végleges” működési állapot hasonló problémákhoz tud vezetni, mint például rövidebb akkumulátor élettartam.

5.1.3. Eredmények

A mérés összeállítása után és a mérőprogram beállítását elvégezve megtudtam kezdeni a tesztelési folyamatot.

Kétféle működési állapotban vizsgáltam az eszközt, tápellátás mellett, illetve csak a belső akkumulátor használatával. A mérés során feljegyzett eredményeket táblázatba foglaltam.

- Tápellátás (Charging) üzemmód:

Teszt Frekvencia [MHz]	Antenna Polarizáció	Felület (Oldal)	Térerősség [V/m]	Teljesítmény Kritérium	Eredmények	
80 - 1000	V és H	Elülső	3	A	A	Megfelelt
80 - 1000	V és H	Hátsó	3	A	A	Megfelelt
80 - 1000	V és H	Bal	3	A	A	Megfelelt
80 - 1000	V és H	Jobb	3	A	A	Megfelelt
80 - 1000	V és H	Felső	3	A	A	Megfelelt
80 - 1000	V és H	Alsó	3	A	A	Megfelelt

2. Táblázat: Sugárzott immunitás vizsgálati eredmény

A táblázatban látható „Felület” oszlop (2. Táblázat) az eszköznek a hat oldalára utal, ugyanis a vizsgálatot mind a hat elhelyezésben elkell végezni a GTEM cellában terjedő elektromágneses hullámok irányából adódóan. Ezek mellett feltüntettem még a teszt frekvenciatartományt, valamint a térerősséget, amelyeket a szabvány meghatározott a mérés elvégzéséhez.

A teljesítmény kritérium, az eszköz részéről elvárt működést jelenti minden vizsgálat esetében. Az „A” osztály pedig azt, hogy nem megengedett semmilyen hiba az eszköz működése során, ezt a kritériumot az IoT készülék teljesítette, mint az kiolvasható az elért eredményekből. Tápellátás alatti üzemmódban megfelelt az előírt követelményeknek.

- Belső akkumulátor üzemmód:

Belső akkumulátoros üzemmódban pontosan azok az eredmények születtek, amelyeket a fenti táblázat szemléltet. Attól eltekintve, hogy mérés során lemerült az akkumulátor, emiatt a mérési folyamat félbe szakadt. Ugyanakkor amelyik frekvencia ponton megszakadt a folyamat, attól az értéktől kezdve újra tudtam indítani a vizsgálatot a mérőprogram segítségével.

Ezek alapján elmondható, hogy ennek az IoT eszköznek a zavartűrőképessége a sugárzott zavarjelekkel szemben megfelelő mindkét üzemmódban.

5.2. Vezetett Immunitás

A következő vizsgálat a Vezetett immunitás volt, az az Continuous induced RF disturbance szabvány szerinti megnevezéssel. Ennek a mérésnek a célja az, hogy megvizsgáljuk az adott készülék immunitását az eszköz táp, illetve jelvezetékein érkező külső zavarokkal szemben.

A teszteléshez felhasznált mérő és segédeszközök a következők voltak:

- RF jelgenerátor – Agilent, RFG-3
- Erősítő – R&S, PA1G-2
- Clamp (Csatoló)
- Impedancia stabilizátor (LISN) – R&S
- RF kábel
- MQTT Explorer (Szoftver)
- Frequency Stepper (Szoftver)

5.2.1. Mérés leírása

A vizsgálat során az MSZ EN 55035 szabványban meghatározott „4.1” záradék szerint jártam el. Ami az alábbi követelményeket tartalmazza a mérés elvégzéséhez:

- Frekvenciatartomány: 0,15-10 MHz
10-30 MHz
30-80 MHz
- Térerősség: 3 V/m, illetve 1 V/m a legnagyobb frekvenciatartomány esetén

A méréshez a Frequency Stepper nevezetű mérőprogramot alkalmaztam, akárcsak a Sugárzott immunitás (5.1) vizsgálatánál. Ezúttal egy olyan fájlt töltöttem be a szoftverbe, amely a Vezetett immunitás - szabványban előírt - kritériumára vonatkozik. Az imént felsorolt követelmények ugyan három frekvenciatartományból állnak, viszont ez a fájl ezeket egy tartományra szűkíti. Emiatt elegendő volt egyszer elindítanom a programot, hiszen a vizsgálati tartomány az előírt 0,15-80 MHz-ig terjedő frekvenciasáv volt.

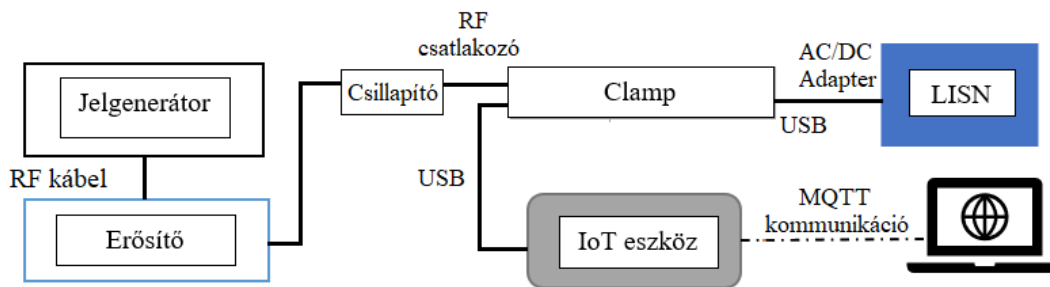
A térerősségre vonatkozóan a 3 V/m került beállításra. Ugyanakkor 30 MHz-től léptetve 1 V/m a meghatározott érték, de amennyiben 3 V/m esetén megfelelő működést mutat az eszköz, akkor jogosan feltételezhető, hogy 1 V/m esetén is ezt az eredményt kapnánk vissza.

További változtatásokra nem volt szükség, a beállítások többi része azonos a GTEM cellában végzett mérés során leírtakkal. (Moduláció, 8 s léptetés idő, exclusion band-ek)

5.2.2. Mérés menete

Az alapszabvány, amely meghatározza a Vezetett immunitás vizsgálatának folyamatát: IEC 61000-4-6

A vizsgálatok megkezdése előtt egy mérési összeállítást kellett előkészítenem, ezt a következő ábrán (18. ábra) illusztrálom:



18. ábra: Vezetett immunitás mérési összeállítás

Első lépésként - akárcsak az előző vizsgálat esetén – a jelgenerátort, valamint az erősítő műszert összekötöttem egy RF kábel használatával. Jelen helyzetben az erősítő kimenetét nem a GTEM cella csatlakozójára, hanem egy 10 dB-es csillapítóra veztettem. A csillapító kimenetét pedig egy úgynevezett Injection Clamp-re csatlakoztattam. Csillapítóra mérés technikai szempontból volt szükség, tulajdonképpen azért, hogy az erősítóből érkező nagy jelszinteket csillapított értékkel tudjam eljuttatni a vizsgált eszköz USB kábelére. Ugyanis ezt az USB kábelt, a már említett Clamp-be fogattam. Ez valójában egy csatoló, ami a besugárzás miatt használandó. Ezen a csatolón átvezetett kábelt pedig egy AC/DC adapter alkalmazásával a LISN nevezetű műszerre csatlakoztattam. Ennek a műszernek a feladata az, hogy a generátor által előállított zavaró jelek a villamos hálózatba ne juthassanak, csak a vizsgált IoT eszközre kerüljön zavarjel. Vizsgálat során a készülék működési állapotáról ismételten az MQTT kommunikáció adott visszajelzést számomra. Ezt követtem figyelemmel miközben a mérőprogram a frekvencia értékek léptetését végezte el szabványnak megfelelő módon.

5.2.3. Eredmények

A felvázolt mérési összeállítás előkészítése és mérőprogram beállítása után elvégeztem a tesztelést és ezeket illetően a következő eredményt kaptam (3. Táblázat):

Teszt Frekvencia [MHz]	Teszt mód	Teszt Port	Feszültség Szint (EMF) [dB μ V]	Teljesítmény Kritérium	Eredmények	
0.150 - 80	EM clamp	Power Port	3 Vrms	A	A	Megfelelt

3. Táblázat: Vezetett immunitás vizsgálati eredmény

A szabványban megadott teszt frekvenciatartományon belül elvégeztem a mérést. Tesztelési folyamat során az MQTT szerveren folyamatos volt az adatküldés, tehát 6 másodpercenként érkezett üzenet az eszközről hiba nélkül. Ennek következtében „A” osztályúnak nyilvánítottam vezetett immunitás szempontjából, ami azt jelenti, hogy az eszköz kábelcsatlakozójára vezetett zavarjelek nem akadályozták az elvárt működést.

5.3. ESD

Ezek után ESD²¹ tesztekkel végeztem el az eszközön, ami tulajdonképpen az elektrosztatikus kisülés megfelelője. Ez az elektrosztatikus kisülés viszonylag gyakori a hétköznapi életben, ugyanis a különféle tárgyak érintésekor keletkezik, akár szikra kíséretében is végbe mehet némely esetben.

Azonban a kisülési folyamat (ESD) a feltöltődött anyagok között olykor észrevétlenül is lezajlik, ennek következtében komoly gondokat tud okozni például az elektronikai iparban. Ennek megelőzése végett szükséges vizsgálni az eszköz immunitását az ESD folyamatokkal szemben.

A teszteléshez felhasznált mérő és segédeszközök a következők voltak:

- ESD szimulátor – Haefely, Onyx30
- Tápegység – EMC Partner, PS3
- Tranziens generátor – EMC Partner, Transient 3000
- MQTT Explorer (szoftver)

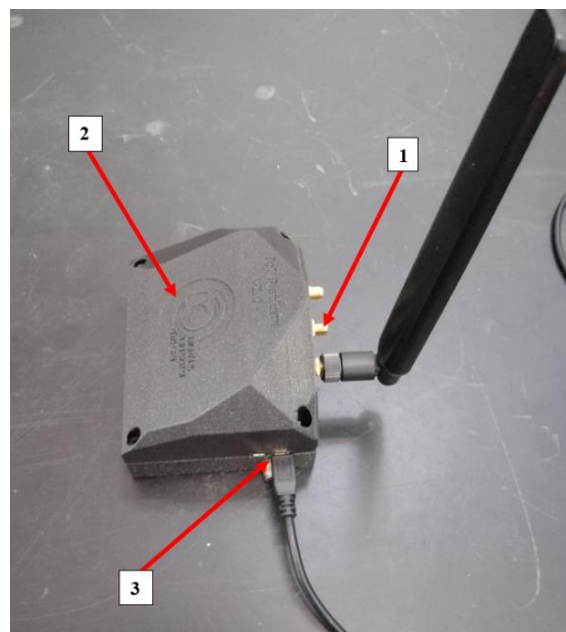
²¹ Electrostatic Discharge

5.3.1. Mérés leírása

A mérés során az MSZ EN 55035 szabványban meghatározott „1.4” záradék szerint jártam el. Ezen előírások alapján szükséges vizsgálatot végezni:

- Contact Discharge módban (4 kV, pozitív és negatív polarizáció)
- Air Discharge módban (8 kV, pozitív és negatív polarizáció)

ESD során megkülönböztetünk fémes, valamint műanyag felületet az eszközön. Fémes felületű pontokon Contact Discharge alkalmazandó, míg műanyag felületeken Air Discharge teszt módot kell alkalmaznunk. Ennek érdekében előre kiválasztottam azon teszt pontokat (19. ábra) az eszközön, amelyeken az ESD vizsgálatot végrehajtottam.



19. ábra: ESD teszt pontok

A fenti ábrán látható az IoT eszköz tokozásban és antennával felszerelve. Fontos szempont volt a tesztelési pontok kiválasztásánál az, hogy ESD vizsgálatot olyan felületeken kell elvégezni, amelyekre érvényes az érintés veszélyének a feltétele. Tehát az eszköz azon részeit kell figyelembe venni, melyeket bárki elérhet, megérinthet.

Ebben az esetben például a tokozáshoz használt csavarokat nem volt szükséges vizsgálni, hiszen maga a tokozás kialakítása védelmet nyújtott azokon a pontokon.

Az alábbi felületek láthatók számozással ellátva:

1. Antenna csatlakozó (fémes)
2. Tokozás (műanyag)
3. Tápellátás csatlakozó (fémes)

5.3.2. Mérés menete

Az alapszabvány, amely meghatározza az ESD vizsgálatának folyamatát: *IEC 61000-4-2*

Az ESD tesztelési folyamat alapvetően két fázisból áll:

- Közvetlen alkalmazás HCP²² használatával (Horizontális csatoló felület)
- Közvetett alkalmazás VCP²³ használatával (Vertikális csatoló felület)

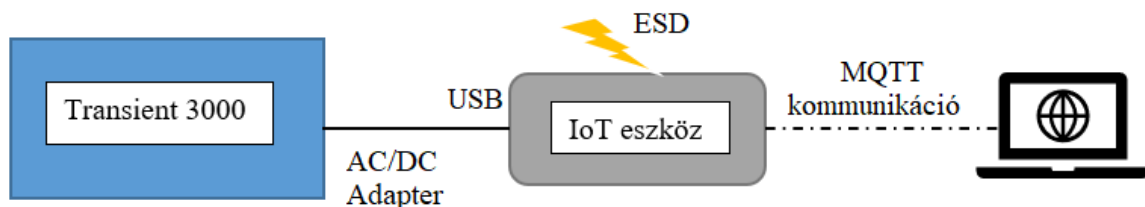
Mindkét esetben vizsgálni kell a kisülés hatását az ESD szimulátor segítségével, illetve mindegyik csatoló felületet földeléssel kell ellátni, ez utóbbi az ESD szimulátorra is igaz.



20. ábra: ESD szimulátor kijelző

Az ESD szimulátor kijelzőjén megjelenő beállítás menüben (20. ábra), szabványnak megfelelő feszültség értékeket és kisülési mennyiséget megadva el tudtam kezdeni az eszközön való tesztelést.

Az alábbi összeállításban (21. ábra) végeztem a mérést:



21. ábra: ESD mérési összeállítás

Az IoT eszközt egy USB kábel használatával lehet csatlakoztatni a Transient 3000 műszerhez, amelyből a tápellátást kapja egy AC/DC adapter segítségével. Az ESD szimulátor használatával elvégeztem a kisülési folyamatokat az előre kijelölt pontokon. Az eszköz működéséről a visszajelzést egy laptopon indított MQTT kommunikációs felületről kaptam, amelyre a készülék 6 másodpercenként küldött üzeneteket. Folyamatos kommunikáció az elvárt eredmény a vizsgálat során.

22 Horizontal Coupling Plane
23 Vertical Coupling Plane

5.3.3. Eredmények

A vizsgálatot elvégeztem a kijelölt tesztpontokon, HCP és VCP alkalmazásban egyaránt. Ezeknek az eredményeit táblázatba foglaltam:

- Közvetlen alkalmazási mód:



22. ábra: ESD vizsgálat, HCP használata

Közvetlen alkalmazás							
Kisülés Szint [kV]	Teszt Pontok	Polaritás	Contact Discharge	Air Discharge	Teljesítmény Kritérium	Eredmények	
4	1	+	X	-	B	A	Megfelelt
4	1	-	X	-	B	A	Megfelelt
8	2	+	-	X	B	A	Megfelelt
8	2	-	-	X	B	A	Megfelelt
4	3	+	X	-	B	A	Megfelelt
4	3	-	X	-	B	A	Megfelelt

4. Táblázat: ESD vizsgálati eredmény, HCP használatával

Feltüntettem a kisülési feszültség szinteket az egyes teszt pontokhoz pozitív, valamint negatív polarizációval egyaránt. Ezek mellett azt is megjelöltem, hogy milyen kisülési teszt módot alkalmaztam a vizsgálat során.

A táblázatból kiolvasható, hogy a szabványban elvárt teljesítmény kritérium az eszköz részéről „B” osztályzat volt (4. Táblázat). Ez annyit jelent, hogy megengedett a funkció veszteség vagy teljesítmény degradáció, amennyiben az eszköz megfelelő működése külső beavatkozás nélkül visszaáll. Azonban a vizsgálat során semmilyen hiba nem merült fel az eszközzel kapcsolatban, ezért „A” osztályba soroltam, tehát ezen a teszten megfelelt.

- Közvetett alkalmazási mód:



23. ábra: ESD vizsgálat, VCP használata

Ennél a vizsgálati módszernél, nem közvetlen az eszközön végeztem a kisülést. Egy földeléssel ellátott vertikális csatoló felületen (23. ábra) zajlott le az ESD folyamat és ennek hatására figyeltem a készülék működését.

Közvetett alkalmazás							
Kisülés Szint [kV]	Teszt Pontok (Oldal)	Polaritás	HCP	VCP	Teljesítmény Kritérium	Eredmények	
4	Elülső	+	X	X	B	A	Megfelelt
4	Elülső	-	X	X	B	A	Megfelelt
4	Hátsó	+	X	X	B	A	Megfelelt
4	Hátsó	-	X	X	B	A	Megfelelt
4	Bal	+	X	X	B	A	Megfelelt
4	Bal	-	X	X	B	A	Megfelelt
4	Jobb	+	X	X	B	A	Megfelelt
4	Jobb	-	X	X	B	A	Megfelelt
4	Felső	+	X	X	B	A	Megfelelt
4	Felső	-	X	X	B	A	Megfelelt
4	Alsó	+	X	X	B	A	Megfelelt
4	Alsó	-	X	X	B	A	Megfelelt

5. Táblázat: ESD vizsgálati eredmény, VCP használatával

A teszt pontok ebben az esetben az IoT eszköz hat oldalára utalnak, ugyanis a VCP-n végzett kisülési folyamatot mindegyik pozícióban tesztelni kell (5. Táblázat). A közvetlen alkalmazáshoz hasonlóan, ezen vizsgálat során is megfelelően teljesített a készülék. Következtetésképpen, ESD jelenségekkel szemben megfelelő immunitással rendelkezik az eszköz.

5.4. EFT

Az EFT²⁴, elektromos gyors tranziensek, illetve Burst néven is ismert. A tranziens jelenség egy rövid idő lefolyású burst, energialöket az adott rendszerben, amely hirtelen állapot változás következtében jön létre. Ezek a tranziensek általában a kábelcsatlakozón keresztül jutnak az adott elektronikai eszközbe. A mérés során az ezekkel szembeni immunitás vizsgálendő.

A teszteléshez felhasznált mérő és segédeszközök a következők voltak:

- Tápegység – EMC Partner, PS3
- Tranziens generátor – EMC Partner, Transient 3000
- MQTT Explorer
- Kapacitív csatoló (Capacitive Clamp)

5.4.1. Mérés leírása

A mérés során az MSZ EN 55035 szabványban meghatározott „2.5” és „4.5” záradék szerint jártam el.

Előbbi az eszköz Service port (COM) bemenetén vizsgálendő, abban az esetben, ha 3 m-nél nagyobb kábelhosszúságú csatlakozót alkalmazunk. Ehhez az alábbi előírások vonatkoznak:

- Kapacitív csatoló használata
- Teszt feszültség szint: 500 V (Pozitív és negatív polarizáció)
- Ismétlési frekvencia: 5 kHz

Utóbbi záradék pedig az eszköz tápellátási bemenetén (CHG) alkalmazandó. Alapvetően ez a záradék az AC tápellátású készülékekre vonatkozik, viszont a szabvány meghatározása szerint minden DC tápellátással rendelkező eszközt AC kategóriába kell sorolni, amennyiben az eszköz dedikált AC/DC konverterrel rendelkezik. Erre a pontra a következők az előírások:

- Közvetlenül az eszköz Power Port csatlakozóján vizsgáljuk (nincs szükség kapacitív csatolóra)
- Teszt feszültség szint: 1 kV (Pozitív és negatív polarizáció)
- Ismétlési frekvencia: 5 kHz

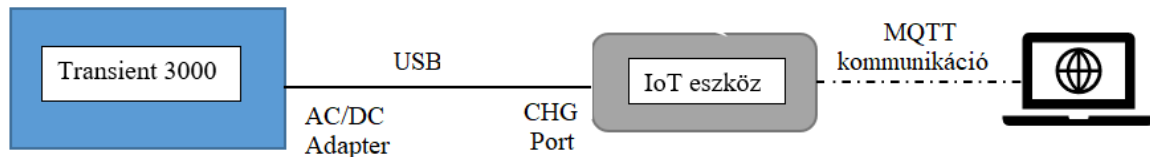
Mindkét esetben a szükséges beállításokat a Transient 3000 mérőműszeren végeztem el, az EFT tesztmódot kiválasztva.

24 Electrical Fast Transients

5.4.2. Mérés menete

Az alapszabvány, amely meghatározza az EFT vizsgálatának folyamatát: *IEC 61000-4-4*

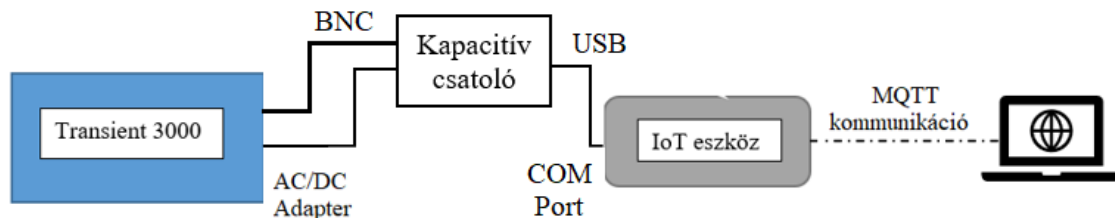
A vizsgálatok elvégzését elsősorban az eszköz CHG port bemenetén kezdtem (24. ábra), az alábbi mérési összeállítás szerint:



24. ábra: EFT mérési összeállítás (Power Port)

Az IoT eszköz CHG bemenetére egy USB kábelt csatlakoztattam, amelyet egy AC/DC adapter segítségével a Transient 3000 műszer EUT-Power bemenetére vezettem. Az eszköz működéséről a visszajelzést az eddigiekben alkalmazott MQTT kommunikációs felületről kaptam, amelyre a készülék továbbra is 6 másodpercenként küldött üzeneteket.

Ezek után az eszköz COM Port bemenetén végeztem el az előírt vizsgálatot, a következő ábrán látható összeállítás (25. ábra) alapján:



25. ábra: EFT mérési összeállítás (Service Port)

A vizsgálat összeállítása annyiban tér el az előzőekben felvázolt méréstől, hogy az eszköz COM Port bemenetére csatlakoztatom az USB kábelt, amelyet egy kapacitív csatolóba fogatva vezetek át a Transient 3000 mérőműszerre. Emellett a kapacitív csatoló BNC csatlakozóját szintén a tranziens generátorhoz vezetem, ezt az EFT „Impulse-Out” jelölésű kimenetére. A kommunikáció továbbra is az MQTT szerver segítségével történt.

Mindkét mérési összeállítás esetében a Transient 3000 műszeren elindított EFT teszt jelentette a vizsgálat kezdetét. A vizsgálatok során az elvárt eredmény a hibátlan kommunikáció volt az eszköz és a szerver között.

5.4.3. Eredmények

A két vizsgálati módszernek megfelelően elvégeztem a méréseket és a megfigyelt eredményeket táblázatba rögzítettem.

- CHG Port mérési mód:

Teszt Feszültség [kV]	Teszt Pont	Csatolási mód	Polaritás	Teljesítmény Kritérium	Eredmények	
1	Power Port	L	+	B	A	Megfelelt
		L	-	B	A	Megfelelt
		N	+	B	A	Megfelelt
		N	-	B	A	Megfelelt
		L+N	+	B	A	Megfelelt
		L+N	-	B	A	Megfelelt

6. Táblázat: EFT vizsgálati eredmény (Power Port)

A csatolási módokat a mérőműszeren futatott EFT teszt automatikusan változtatta a táblázatban látható pontok között (6. Táblázat). A teszt feszültség polaritását manuálisan kellett beállítanom a mérések során. Az eszköz kommunikációjában nem lépett fel semmilyen hiba, ennek a vizsgálatnak megfelelt.

- COM Port mérési mód:



26. ábra: EFT vizsgálat, kapacitív csatoló használata

Fentebb látható (26. ábra) a kapacitív csatolóval kialakított mérési összeállítás. A vizsgálat eredményét a következő táblázatban (7. Táblázat) foglaltam össze.

Teszt Feszültség [kV]	Teszt Pont	Csatolási mód	Polaritás	Teljesítmény Kritérium	Eredmények	
0,5	Service Port	Kapacitív csatoló	+	B	A	Megfelelt
			-	B	A	Megfelelt

7. Táblázat: EFT vizsgálati eredmény (Service Port)

Az előző méréssel ellentétben látható, hogy a csatolási módot a kapacitív csatoló jelentette, emiatt kevesebb mérési eredmény született. A teszt feszültséget ezzel az alkalommal is manuálisan állítottam be a tranziens generátoron, mindkét polarizációban. Az MQTT szerverrel való kommunikáció ebben az esetben is folyamatosnak bizonyult, tehát az előírt kritériumokkal szemben megfelelően teljesített az eszköz.

A két vizsgálati módszer eredménye alapján megállapítható, hogy a kábelcsatlakozón keresztül rendszerbe jutó tranziens hatásokkal szemben az IoT eszköz elegendő zavartűrőképességgel rendelkezik.

5.5. Sugárzott Emisszió

Az utolsó EMC vizsgálat, amelyet bemutatok az a Sugárzott emisszió, szabvány hivatkozások alapján Radiated emissions néven ismert.

Sugárzott emisszió mérése során a vizsgált eszköz által kibocsátott nagyfrekvenciás zavaroknak a szintjét mérjük és az eredmények alapján megállapítjuk, hogy ezek az emissziós szintek a szabványban meghatározott határértékek alatt vannak vagy sem. Sugárzott immunitáshoz hasonlóan ezen vizsgálatokat is minden esetben árnyékolt kamrában kell elvégezni, annak érdekében, hogy ténylegesen az eszköz által kibocsátott zavarjelek szintjét tudjuk vizsgálni.

A teszteléshez felhasznált mérő és segédeszközök a következők voltak:

- Spektrum analizátor - R&S, ESU8
- Bázisállomás szimulátor - R&S, CMW500
- Log-Per vevő antenna - ETS LINDGREN, 3142C
- Log-Per irányított antenna - R&S, HL050
- Árnyékolt kamra - Frankonia, FAC
- Forgóasztal - Frankonia, TTL
- Csillapító - Agilent, 8491B
- RF kábelek

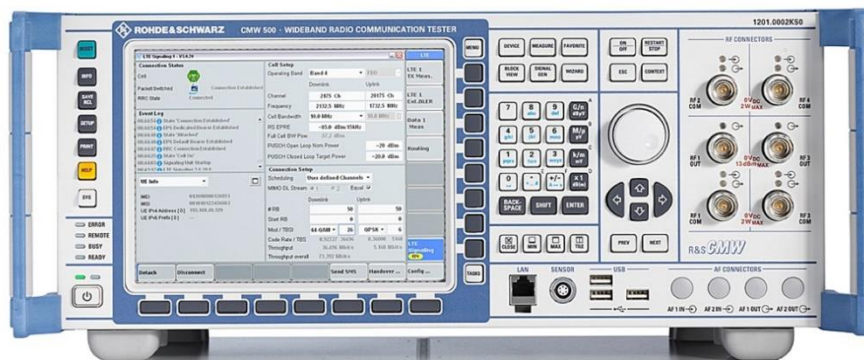
5.5.1. Mérés leírása

A mérés során az MSZ EN 55032 szabványban meghatározott „A4.4” záradék szerint jártam el. Az előírások, melyeket a záradék tartalmaz a következők:

- Frekvenciatartomány: 30-230 MHz, ehhez tartozó határérték $42-35 \text{ dB}(\mu\text{V/m})$
230-1000 MHz, ehhez tartozó határérték $42 \text{ dB}(\mu\text{V/m})$
- Mérési távolság: 3 m
- Méréshez használandó detektor típus/sávszélesség: Kvázi csúcs detektor (QP)/150 kHz

Említésre került, hogy az emisszió vizsgálatot árnyékolt kamrában kell elvégezni, ennek kapcsolatában felmerült egy probléma a mérés kezdetét megelőzően. A probléma forrása pedig az volt, hogy az eszköz nem tudott kapcsolatot létesíteni a bázisállomással, annak ellenére, hogy az antenna csatlakozóját RF kábel segítségével kivezettem az árnyékolt helyiségből. Ennek az oka lehetett a kábelhosszúságból adódó jel út csillapítás vagy az alkalmazott antenna nem megfelelő teljesítménye. Ennek következményeképpen az MQTT szerverrel való kommunikáció sem működött, emiatt szükségessé vált egy alternatív mérési módszernek az alkalmazása.

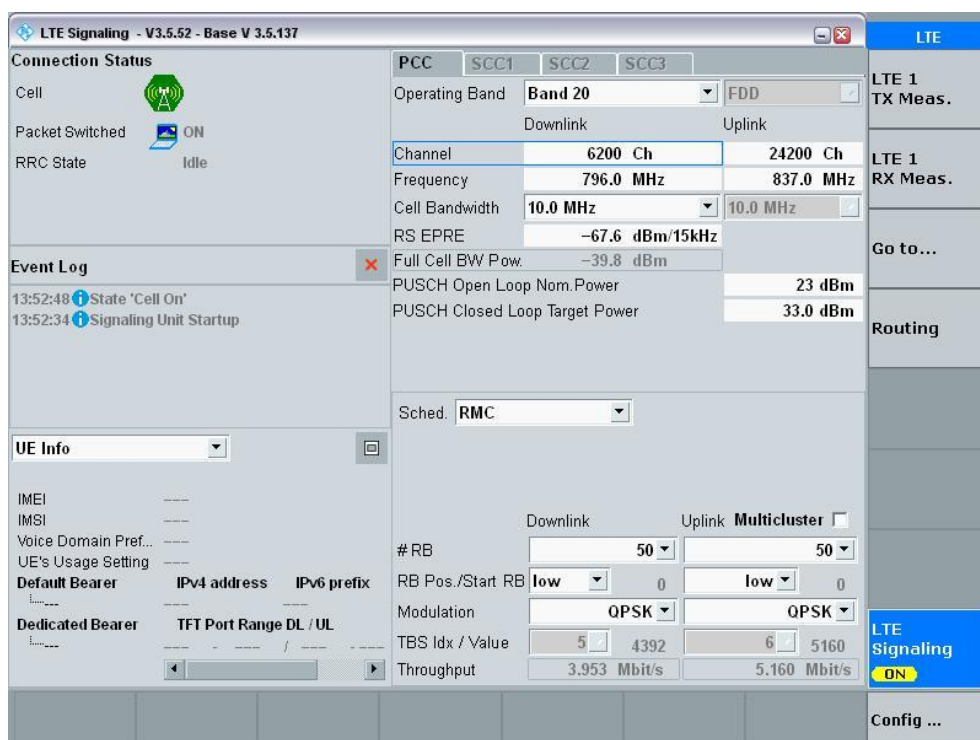
Az alternatív megoldást egy bázisállomás szimulátor berendezés (27. ábra) nyújtotta, amelynek használatával mobilhálózati kommunikációt tudtam létesíteni az IoT eszközzel.



27. ábra: CMW500 bázisállomás szimulátor (6)

Fent látható a műszer, amely egyrészt az eszköz 4G hálózattal való kapcsolatát biztosította a vizsgálat közben. Másrészt pedig az elvárt működésről való visszacsatolást is ez a készülék szolgáltatva számomra. A bázisállomás szimulátorhoz tartozik egy saját SIM kártya, amit szintén alkalmaznom kellett az eddigiekben használatos SIM helyett, a problémamentes kommunikáció érdekében.

A következőkben a műszeren beállított paramétereket (28. ábra) fogom ismertetni:



28. ábra: CMW500 mérési paraméterek

Első lépésként azt kellett kiválasztanom, hogy mely mobilkommunikációs technológián szeretném a kapcsolatot létrehozni a szimulátor és a vizsgált eszköz között. Mivel az eddigi összes vizsgálat során 4G LTE hálózaton kommunikált a modul, ezért jelen helyzetben is az LTE Signaling, illetve LTE Measurement opciókat választottam.

Ezek után a megfelelő Band paramétert kellett megadnom. Az operátor által adott SIM kártyát használva az RF modul minden esetben a Band 20-ra csatlakozott, emiatt a mostani mérés alkalmával is ezt a frekvencia csatornát állítottam be a mérés hitelessége érdekében. Ezzel a bázisállomás szimulátor automatikusan meg adta az ábrán látható Downlink és Uplink frekvenciasávokat, valamint az ezekhez tartozó kommunikációs csatornákat.

Következő lépésként a sávszélességet (Cell Bandwidth) adtam meg a műszernek, ez a vizsgálat folyamán három különböző érték volt: 5 MHz, 10 MHz, 20 MHz

Az RS EPRE tulajdonképpen a bázisállomás szimulátor referencia jelét adja meg, ezt alapértelmezett értéken hagytam. Ez utáni két paraméter a csatlakoztatott eszköz kommunikációs teljesítményét határozza meg. A fenti ábrán szemléltetett 23 dBm, valamint 33 dBm a maximális beállítható teljesítmény szinteket jelentik. A mérések folyamán nem csak a maximális teljesítmény mellett végeztem vizsgálatokat, hanem 50 % és 25 %-os értékkel egyaránt.

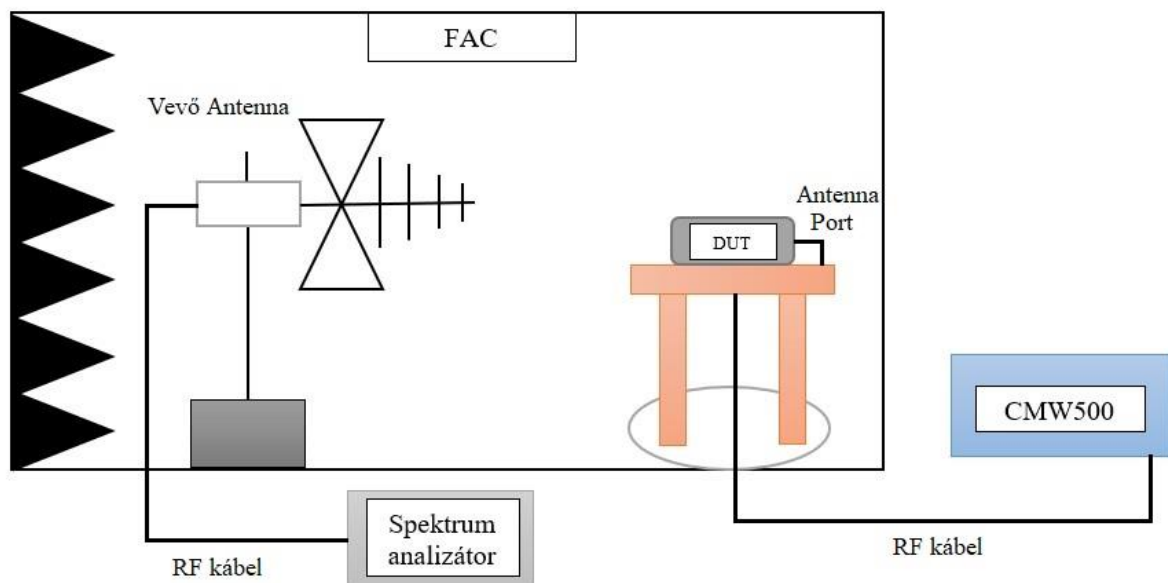
5.5.2. Mérés menete

Az emissziós vizsgálatok során két üzemmódban végeztem el méréseket:

- Belső akkumulátoros üzemmódban
- Tápellátás alatti (Charging) üzemmódban

Viszont a CMW500 műszerrel mindkettő esetben teszteltem vezetetten, illetve sugárzottan is az eszköz emissziós szintjeit.

Elsőként a vezetett mérésnek az összeállítását mutatom be a következő ábrán:



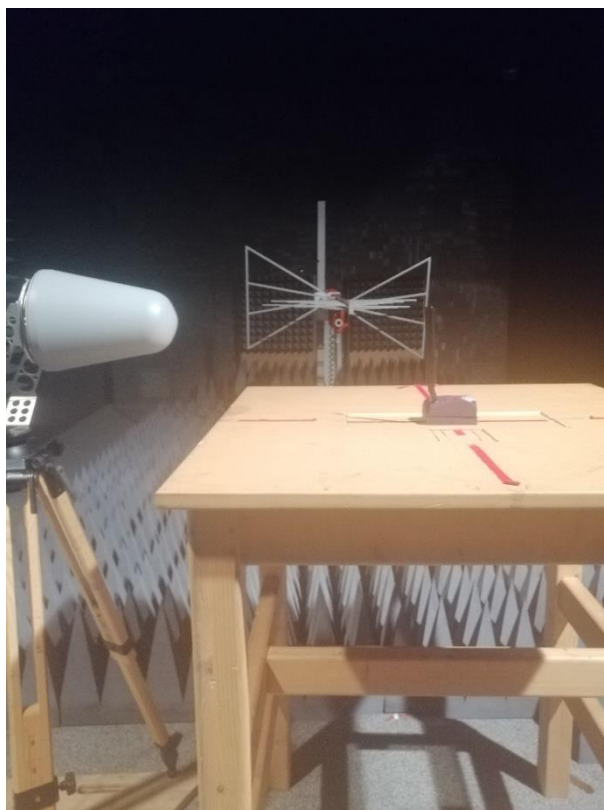
29. ábra: Sugárzott emisszió mérési összeállítás (CMW-vel vezetetten)

Itt látható az összeállítás (29. ábra) miszerint a vizsgálatot elvégeztem. A kamrában gúla alakú abszorberek vannak elhelyezve, amik biztosítják a reflektálódó elektromágneses hullámok elnyelését. A forgóasztalon elhelyezett IoT eszköz antenna csatlakozóját az asztal alatt vezettem el egészen a kamra csatlakozójáig egy RF kábelt használva, innen pedig a bázisállomás szimulátor bementére kötöttem a kábelcsatlakozót.

Az eszköz által kibocsátott zavarjelek szintjét az ábrán látható log-per antenna vette, ami egy spektrum analízátorral (ún. EMI Test Receiver) volt összekötve, így az árnyékolt kamrán kívülről figyelni tudtam a spektrumképet.

A mérést egy PC-n futatott mérőprogram segítette, amely a szabványoknak megfelelő beállításokkal (pl. emissziós határérték, mérési bizonytalanság) rendelkezett. Az antennával horizontális és vertikális polarizációban is készült mérés és ezen emissziós szinteknek az eredményét egy diagramon kaptam meg.

A következő ábrán a sugárzott mérés látható (30. ábra):



30. ábra: Sugárzott emisszió mérési összeállítás (CMW-vel sugárzottan)

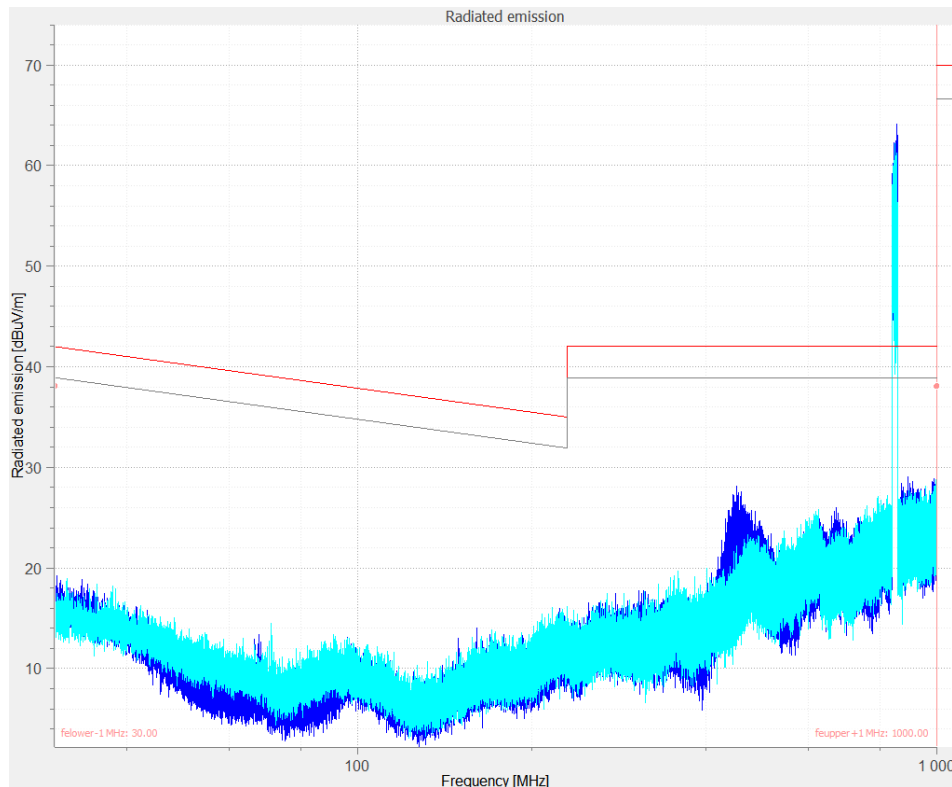
Az előző mérési összeállítástól annyiban különbözik a fent látható vizsgálat, hogy a bázisállomás szimulátor nem közvetlenül az eszköz antenna csatlakozójára van vezetve, ebben az esetben egy tripod-ra felszerelt irányított antennára van csatlakoztatva a műszer. A tokozás, valamint az eszköz kábeleiből is eredhet nemkívánt sugárzás, amely az RF csatlakozón nem feltétlenül jelenik meg. Emiatt sugárzott méréseket végeztem, hogy megbizonyosodjak arról, hogy a vezetett és sugárzott mérési eredmények között nincs különbség.

5.5.3. Eredmény

A mérési összeállítások előkészítését és az eszköz bázisállomás szimulátorral való kommunikációját követően elvégeztem a méréseket. Elsősorban vezetetten, majd utána sugárzottan is a leírt két üzemmódban. A dolgozatban kizárólag a maximális teljesítményen mért emissziós értékeket mutatom be, 20 MHz-es sávszélesség mellett. Ugyanis sok eredmény született a tesztelés során, ezért ezek a mellékletben található (=20210624-1-2=) jegyzőkönyvben megtekinthetők.

- Vezetett mérési eredmények

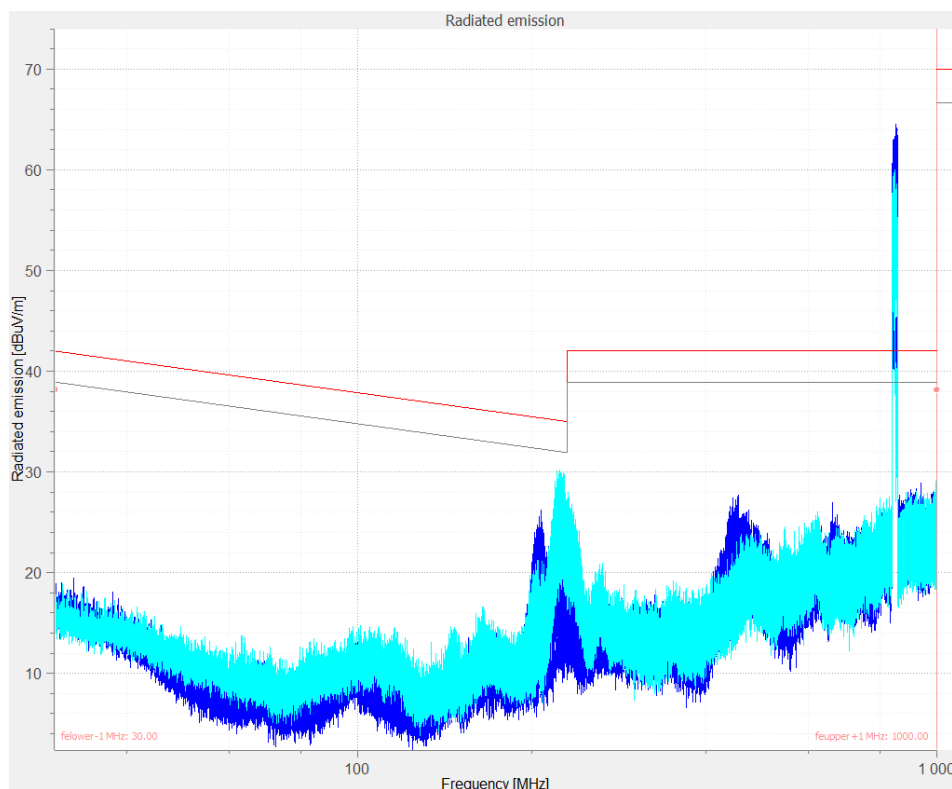
Belső akkumulátoros üzemmódban a következő eredményt kaptam 23 dBm kimeneti teljesítmény és 20 MHz sávszélesség mellett:



31. ábra: Sugárzott emisszió vizsgálati eredmény (CMW-vel vezetetten)

A diagram függőleges tengelye az emisszió értékét ábrázolja, a vízszintes tengely a vizsgált frekvenciatartományt (30-1000 MHz). Az ábrán a kék szín mutatja a horizontális, a cián pedig a vertikális antenna állásban mért emissziós szintet (31. ábra). A pirossal jelölt vonal a szabványban meghatározott határértékeket jelöli, míg a szürke vonal a mérési bizonytalanságból adódó limitet ábrázolja. A kiugró érték az IoT eszköznek a kommunikációját jelzi a Band 20-as 4G csatornán. A mérések során az emissziós diagram jelölései nem változtak. Ezen eredményből azt kellett megállapítanom, hogy az eszköz által kibocsátott zavarsszintek az előírt limit alatt vannak-e. Egyértelműen látszik, hogy az eszköz emissziós szintjei mind a szabványos határértékek, mind a mérési bizonytalanságból adódó határértékek alatt helyezkednek el. Ennél a tesztnél megfelelt a készülék.

Tápellátás alatti (Charging) üzemmódban a következő eredményt kaptam 23 dBm kimeneti teljesítmény és 20 MHz sáv szélesség mellett:



32. ábra: Sugárzott emisszió vizsgálati eredmény-2 (CMW-vel vezetetten)

A kapott eredményben észrevehető egy nagyobb eltérés, mégpedig a 200 MHz-es frekvenciasávok környékén (32. ábra). Itt a tápellátás alatti üzemmód miatt az eszköz DC-DC konvertere megnövekedett zavar szinteket produkált. Mivel ezek az értékek megközelítik a limitet ezért szükséges volt egy ellenőrző mérést végezni kvázi csúcs detektorral.

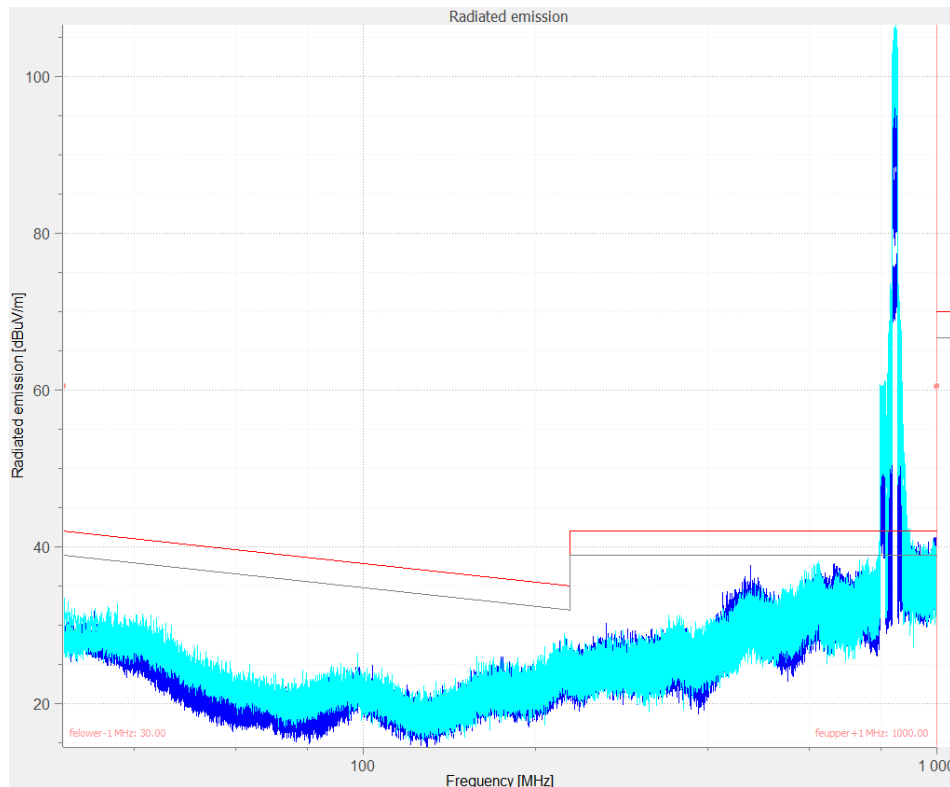
Teszt Frekvencia [MHz]	Detektor Típus	Sugárzott Zavar szint [dBμV]	Sugárzott Határérték (QP) [dBμV]	Eltérés [dBμV]	Eredmények
221.16	QP	24.83	35.13	10.30	Megfelelt
223.99	QP	23.63	35.09	11.46	Megfelelt
227.92	QP	23.16	35.03	11.87	Megfelelt
Mérési bizonytalanság:			3.08 dB		

8. Táblázat: Sugárzott emisszió eredmény-2, kvázi csúcs detektor mérés

A sugárzott zavar szint ugyan megközelíti a határértékeket, de jól látható a kvázi csúcs detektoros mérés (8. Táblázat) alapján, hogy az eltérés több, mint 10 dB. Tehát tápellátás alatt is megfelelő emissziós szinteket mutatott a vizsgált eszköz.

- Sugárzott mérési eredmények

Belső akkumulátoros üzemmódban a következő eredményt kaptam 23 dBm kimeneti teljesítmény és 20 MHz sávszélesség mellett:



33. ábra: Sugárzott emisszió vizsgálati eredmény (CMW-vel sugárzottan)

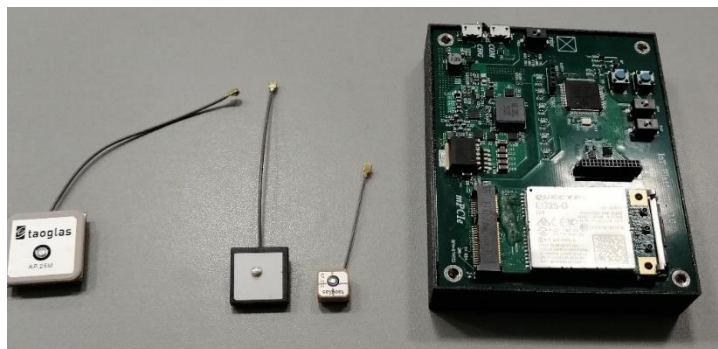
Első ránézésre úgy tűnik az eredményből (33. ábra), hogy az eszköz emissziós zavar szintje eléri a szabványban meghatározott limitet. Azonban ez annak a következménye, hogy a nagyszintű jeleket csillapítók segítségével mérhető szintre kellett csökkenteni, emiatt a sugárzott mérés dinamikatarományja kisebb, mint a vezetett mérés esetében. Mondhatni a kiemelkedő zavar szinteket a csillapítók eredményezték, maga az eszköz emissziós értékei megfelelőek voltak.

Tápellátás alatti (Charging) üzemmódban is hasonló eredményeket kaptam, ugyanezen okokból kifolyólag. Annyi különbséggel, hogy töltés következtében a korábban említett DC-DC konverter miatt 200 MHz környékén emelkedett az emissziós zajszint, de ebben az esetben is az előírt határértékek alatt helyezkedett el.

Összesítve a Sugárzott emisszió vizsgálat eredményeit az IoT eszközre vonatkozóan, elmondható az, hogy az eszköz által sugárzott nagyfrekvenciás zavarok mindegyik esetben a szabvány által meghatározott határértékek alatt voltak. Környezetére nincsen zavaró hatással.

6. IOT PLATFORM FUNKCIONÁLIS TESZT

Az EMC megfelelőségi vizsgálatokat követően az volt a feladatom, hogy teszteljem az IoT eszköz helymeghatározó funkcióját három különböző GNSS antenna segítségével. Mindeközben az eszközhöz fejlesztett platform front-end felületét is használtam, szintén tesztelési okok miatt. A lenti ábrán láthatók az alkalmazott antennák:

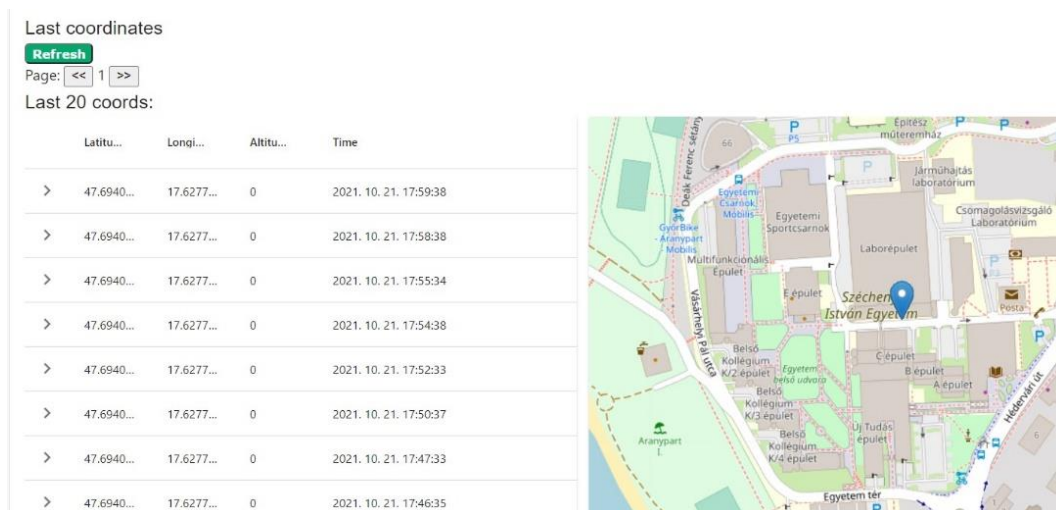


34. ábra: GNSS antennák

Az alábbi GNSS antenna típusokat (34. ábra) használtam fel a méréshez (balról-jobbra haladva):

- taoglas AP25M
- ACTPAT182-01-IP
- taoglas AP10E

Az IoT platform felületén (35. ábra) vizsgáltam az eszközről beérkező helyadat információkat, mindegyik antenna esetében.

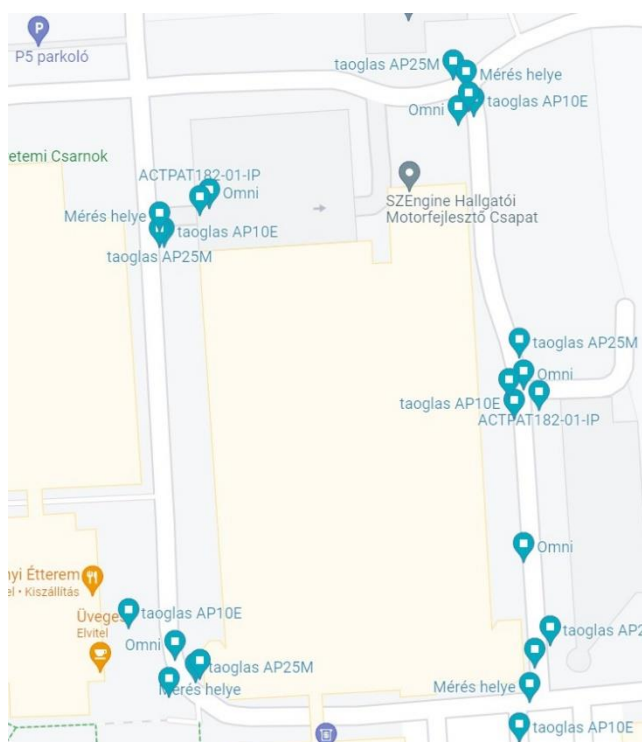


35. ábra: IoT platform front-end felület

A platform folyamatos frissítéssel írta ki az ideiglenes pozíciót, ahol éppen az eszközzel tartózkodtam. A megjelenített Latitude és Longitude értékek alapján határoztam meg az antennák pontosságát.

6.1.1. Eredmény

Egy előre kijelölt útvonalon haladtam végig a Széchenyi István Egyetem labor épülete körül. Adott pontokon megállva összegyűjtöttem egy táblázatba az egyes antennák által mutatott koordinátákat, majd ezeket a koordinátákat a Google Maps applikáció (36. ábra) segítségével ábrázoltam egy vizuális térképen.



36. ábra: Funkcionális teszt eredmény

A teszt során felhasználtam egy negyedik antennát is (EMC vizsgálatoknál alkalmazott), ami nem kifejezetten GNSS antenna, viszont a pontosság szempontjából segítette az összehasonlítást. Jól látható a kapott eredményekből, hogy az antennák pontossága között némely esetben elég nagy a szórás. A legpontosabb helymeghatározás a taoglas AP25M típusú antennával történt, a három antenna méretét tekintve ez volt a legnagyobb, ezzel magyarázható a pontosabb koordináció.

A funkcionális tesztek alapján megállapítható, hogy az IoT eszköz helymeghatározó funkciója kiválóan működik. Emellett a fejlesztett platform is megfelelő módon adta meg a számomra hasznos helyadat információkat.

7. ÖSSZEFOGLALÁS

A dolgozatomban ismertettem az Internet of Things technológia alapelveit és működési folyamatát, illetve azon LTE technológiákat melyeket kifejezetten IoT felhasználásra terveztek. Ezek után bemutattam egy olyan IoT eszközt, amely a Digitális Fejlesztési Központ keretein belül lett fejlesztve. Felvázoltam, hogy milyen okok miatt van szükség elektromágneses kompatibilitási mérésekre minden elektromágneses elven működő eszköz esetében. Ez alól a bemutatott, újonnan fejlesztett eszköz sem volt kivétel. Ennek érdekében, a vonatkozó szabványok alapján EMC vizsgálatokat végeztem el a készüléken, melyek során rendre a követelményeknek megfelelően teljesített. Végezetül az eszköz és a hozzá tartozó platform funkcionális tesztelését hajtottam végre.

7.1. Konklúzió

Ritka eset amikor egy első verziós eszköz EMC vizsgálatok szempontjából megfelel, ugyanakkor ennek már a tervezés során fontos szempontnak kell lennie minden elektromos/villamos készülék esetén. Ugyanis, ha a tervezési fázisban számításba kerül az EMC megfelelésség, akkor a vizsgálatok során már csupán ennek a tesztelése szükséges, hogy valójában sikerült-e megfelelően megtervezni az adott rendszert. Természetesen az ilyen tervezés nagyobb költségekkel is jár, viszont adott esetben lerövidítheti a fejlesztési folyamatot. Jelen esetben az IoT eszközénél alkalmazott RF modul jó példa ebből a nézőpontból, hiszen CE jelöléssel rendelkezett és ráadásul mPCIe csatlakozóra integrálták. Előbbi EMC mérésekre vonatkozóan jelentett előnyt, az utóbbi pedig amiatt, hogy ez a szabványos csatlakozó könnyen illeszthető volt az eszköz paneljéhez. A funkcionális teszteket tekintve is felmerült két opció, ami a GNSS antennákat illeti. Járható út lett volna, hogy ezeket az antennákat a projekt keretén belül tervezzék, ellenben ez rengeteg időt vett volna igénybe. Emiatt ugyan többlet költség mellett, de gyorsabban hozzájutottam a bemutatott antennákhoz, melyek nem utolsó sorban remekül működtek és hozzásegítettek a tesztek elvégzéséhez.

Nem elsődleges szempont tehát, hogy minden egyes elemét az adott rendszernek saját fejlesztés által oldjunk meg, ez ugyan nagyobb költségeket vonhat maga után, viszont végezetül egy rövidebb tervezési fázist és egy működőképes, illetve szabvány követelményeknek megfelelő eszközt kapunk eredményül.

8. IRODALOMJEGYZÉK

- [1] Buzási László „IoT Platform Fejlesztés”, 2021.04
- [2] IoT platform ismertető:
[What is an Internet of Things Platform? What is an IoT Platform? \(avsystem.com\)](https://avsystem.com) 2020.03.17
- [3] IoT működés:
<https://trackinno.com/2018/04/26/how-iot-works-part-1-sensors/> 2018.04.26
- [4] LTE technológia IoT témakörben:
[A legmegfelelőbb LTE IoT szabvány kiválasztása \(intelliport.hu\)](https://intelliport.hu) 2020.06.02
- [5] LTE-M és NB-IoT:
[LTE-M vs NB-IoT – A guide exploring the differences between them | Telenor Connexion](https://telenorconnexion.com)
- [6] 5G – IoT: [5G and the IoT \(What is IoT in 5G?\) - Thales \(thalesgroup.com\)](https://thalesgroup.com)
- [7] RF Modul: [LTE EG25-G Mini PCIe | Quectel](https://quectel.com)
- [8] EMC szabványok: [Magyar Szabványügyi Testület \(mszt.hu\)](https://mszt.hu)
- [9] IoT trendek: [The IOT Magazine](https://theiotmagazine.com)
- [10] IoT folyóirat: [IoT/M2M/V2V Channel \(microwavejournal.com\)](https://microwavejournal.com)
- [11] [The Top 10 IoT Segments in 2018 – based on 1,600 real IoT projects - IoT Analytics \(iot-analytics.com\)](https://iot-analytics.com) Knud Lasse Lueth 2018.02.22
- [12] [MQTT - The Standard for IoT Messaging](https://mqtt.org)
- [13] Understanding the Internet of Things (IoT) – GSMA 2014.07

9. ÁBRAJEGYZÉK

1. ábra: IoT – architektúra (1)	9
(1) How IoT Works - 4 Main Components of IoT System - DataFlair (data-flair.training)	
2. ábra: Alkalmazott szenzor típusok (2)	12
(2) Common sensor categories including magnetic sensors in IoT... Download Scientific Diagram (researchgate.net)	
3. ábra: Vezetéknélküli kommunikációs technológiák (3).....	13
(3) IoT News IOT decision-making tree (part 2): When to employ LoRaWAN/Sigfox/NB-IoT IoT Business News	
4. ábra: Adatfeldolgozás ciklusa	16
5. ábra: Felhasználói felület, „okos” otthon világítás vezérléshez (4)	19
(4) Control smart lights with the Hue app Philips Hue (philips-hue.com)	
6. ábra: IoT – munkafolyamat összefoglalva (5).....	21
(5) How IoT Works – Part 4: User Interface Trackinno	
7. ábra: LTE-M és NB-IoT fejlődése	22
8. ábra: 5G use case kategóriák	24
9. ábra: IoT Platform V1.0 eszköz panel.....	25
10. ábra: Állapotjelző LED-ek (balról-jobbra haladva, LED1-LED6-ig bezárólag)	26
11. ábra: Alkalmazott RF modul	27
12. ábra: CE jelölés	27
13. ábra: EMC mérési összeállítás	28
14. ábra: EMC szabvány záradék (Table Clause)	29
15. ábra: Frequency Stepper szoftver	31
16. ábra: MQTT Explorer felület	32
17. ábra: Sugárzott immunitás mérési összeállítás.....	33
18. ábra: Vezetett immunitás mérési összeállítás.....	36
19. ábra: ESD teszt pontok.....	38
20. ábra: ESD szimulátor kijelző.....	39
21. ábra: ESD mérési összeállítás	39
22. ábra: ESD vizsgálat, HCP használata.....	40
23. ábra: ESD vizsgálat, VCP használata.....	41
24. ábra: EFT mérési összeállítás (Power Port)	43

25. ábra: EFT mérési összeállítás (Service Port).....	43
26. ábra: EFT vizsgálat, kapacitív csatoló használata	44
27. ábra: CMW500 bázisállomás szimulátor (6).....	46
(6) CMW500-wideband-radio-communication-tester-rohde-schwarz- solution_front_46670_05_1440x_w1280_hX.jpg (1280×720)	
28. ábra: CMW500 mérési paraméterek	47
29. ábra: Sugárzott emisszió mérési összeállítás (CMW-vel vezetetten).....	48
30. ábra: Sugárzott emisszió mérési összeállítás (CMW-vel sugárzottan)	49
31. ábra: Sugárzott emisszió vizsgálati eredmény (CMW-vel vezetetten)	50
32. ábra: Sugárzott emisszió vizsgálati eredmény-2 (CMW-vel vezetetten)	51
33. ábra: Sugárzott emisszió vizsgálati eredmény (CMW-vel sugárzottan)	52
34. ábra: GNSS antennák	53
35. ábra: IoT platform front-end felület	53
36. ábra: Funkcionális teszt eredmény	54

10. MELLÉKLETEK

1. EMC immunitás jegyzőkönyv: =20210624-1-1=
2. EMC emisszió jegyzőkönyv: =20210624-1-2=