

ÓBUDAI EGYETEM
KANDÓ KÁLMÁN VILLAMOSMÉRNÖKI KAR
AUTOMATIKA INTÉZET

TDK dolgozat

Rádiófrekvenciás vezeték nélküli hálózat tervezése

Konzulens:
Kopják József
tanársegéd

Készítette:
Sebestyén Gergely

2013

Tartalomjegyzék

1.	BEVEZETÉS.....	2
2.	BELÉPTETŐ RENDSZEREK.....	3
3.	A BELÉPTETŐ RENDSZERREL SZEMBEN TÁMASZTOTT KÖVETELMÉNYEK.....	5
4.	JELENLEG ELTERJEDT KIS HATÓTÁVOLSÁGÚ RÁDIÓFREKVENCIÁS HÁLÓZATOK BEMUTATÁSA.....	7
4.1	WiFi.....	7
4.2	BLUETOOTH.....	8
4.3	ZIGBEE.....	8
4.4	IQRF.....	8
4.5	MiWi.....	9
5.	RÁDIÓFREKVENCIÁS HÁLÓZATI TOPOLOGIÁK ISMERTETÉSE.....	10
5.1	PONT-PONT KAPCSOLAT.....	10
5.2	PONT-MULTIPONT TOPOLOGIA.....	10
5.3	CSILLAG TOPOLOGIA.....	11
5.4	SZÖVEVÉNYES (MESH) HÁLÓZAT.....	11
6.	RFID ALAPÚ AZONOSÍTÁS.....	13
7.	FELHASZNÁLT TECHNOLÓGIÁK ÉS ESZKÖZÖK KIVÁLASZTÁSA.....	14
7.1.1.	<i>IQRF.....</i>	<i>15</i>
7.1.2.	<i>IQMESH.....</i>	<i>16</i>
8.	FIZIKAI RÉTEG TERVEZÉSE.....	18
8.1	OLVASÓ ESZKÖZÖK.....	20
8.2	VEZÉRLŐ ESZKÖZÖK.....	21
8.3	USB ÁTJÁRÓ.....	24
9.	SZOFTVERTERVEZÉS.....	25
9.1	FELHASZNÁLÓI RÉTEG PROTOKOLLJA.....	26
9.2	IQRF MODULOK SZOFTVERE.....	26
9.2.1.	<i>Koordinátor szoftvere.....</i>	<i>27</i>
9.2.2.	<i>Olvasó modul szoftvere.....</i>	<i>28</i>
9.2.3.	<i>Vezérlő egységek szoftvere.....</i>	<i>29</i>
9.3	USB-ÁTJÁRÓ.....	30
9.4	SZERVER.....	30
9.4.1.	<i>Monitor program.....</i>	<i>31</i>
9.4.2.	<i>Grafikus felhasználói felület.....</i>	<i>33</i>
10.	BELÉPTETŐ RENDSZER MŰKÖDÉSÉNEK BEMUTATÁSA.....	39
10.1	TITKOSÍTOTT KOMMUNIKÁCIÓ.....	39
10.2	CSOMAGOK ÜTKÖZÉSE.....	40
10.2.1.	<i>Beléptetés folyamata.....</i>	<i>41</i>
10.2.2.	<i>Épületautomatizálás és épület felügyelet.....</i>	<i>42</i>
11.	IRODALOMJEGYZÉK.....	45

1. Bevezetés

A dolgozatom célja bemutatni egy vezeték nélküli kommunikáción alapuló beléptető rendszer tervezését. A beléptető rendszer tervezésének ötlete onnan származik, hogy az egyetem egyik épülete még nem rendelkezik hasonló rendszerrel és lehetne egy saját fejlesztésű, alacsony költségű rendszert fejleszteni és kiépíteni.

A beléptető rendszer tervezésénél a cél a jelenleg használt rendszerek kommunikációs megoldásainak leváltása, költség hatékony vezeték nélküli hálózat kiépítése, az alkalmazott megoldások integrálása és az új megoldásokkal járó előnyök kihasználása valamint kiegészítő funkciók implementálása volt.

A beléptető rendszer tervezésekor az egyszerűség, könnyen használhatóság és funkcionalitás játszott döntő szerepet. A rendszer telepítésétől használatán át az egyes módosításokig minden egyszerű legyen, a lehető legmagasabb biztonság mellett.

A dolgozat első fő pontjaként, a *Beléptető rendszerek* fejezetében egy rövid leírás olvasható a beléptető rendszerek általános felépítéséről és működéséről. Ezt követően a rendszer tervezését meghatározó elvárások és ennek megfelelő tervezett rendszer kialakítás kerül bemutatásra *A beléptető rendszerrel szemben támasztott követelmények* fejezetben.

A tervezéskor *Felhasznált technológiák és eszközök kiválasztása* fejezetben a beléptető rendszerrel szemben támasztott követelményeknek megfelelő eszközök és technológiák kiválasztása kerül bemutatásra. A kiválasztáskor a felmerülő eszközök és technológiák rövid bemutatásával és ezek alapján melyek kerültek kiválasztásra a beléptető rendszerhez.

A dolgozat következő fejezete a *Fizika réteg tervezése*. Ez a fejezet mutatja be a rendszerhez tervezett eszközök felépítését, és áramköri kialakítását. Ezt követően a rendszerben használt eszközökre megírt és használt szoftverek kerülnek bemutatásra a Szoftvertervezés fejezetben. A fejezet elsőként a rendszerben használt kommunikációs protokollt majd az eszközök szoftver megoldásait mutatja be. A dolgozat végén a *Beléptető rendszer működésének bemutatása* fejezetben a rendszer működésekor végbemenő folyamatok és eljárások kerülnek bemutatásra. Végezetül az elkészített és telepített rendszer tesztelésével kapcsolatos tapasztalatok és észrevételek kerülnek leírásra.

2. Beléptető rendszerek

A beléptető rendszerekre általánosan az MSZ-EN 50133 szabványsorozat rendelkezik[1]. A szabványsorozatban a rendszer-és funkcionális követelmények, a rendszer részegységei, valamint a beléptető rendszereknél használt fogalmak találhatóak. A beléptető rendszer egy „komplex elektromechanikai-informatikai rendszer, amely telepített ellenőrző pontok segítségével lehetővé teszi az objektumokban történő személy- és járműmozgások hely-, idő- és irány szerinti engedélyezését vagy tiltását, az események nyilvántartását, visszakeresését.” „A szerkezeti elemeken túl tartalmazza azokat az intézkedéseket és apparátusokat melyek az üzemeltetéshez és a beléptetés felügyeletéhez szükségesek!” [1].

A beléptető rendszerek olvasókból, vezérlőkből, az áthaladást szabályozó eszközökből és érzékelőkből(APAS) valamint a felügyeletet végző rendszerből állnak. Az olvasók feladata az azonosításra alkalmas adatok továbbítása a rendszer felé. A vezérlők az olvasóktól érkező adatok alapján döntenek el (a rendszer kialakításától függően a felügyeleti rendszertől kapott információk alapján vagy offline adatbázisból), hogy az adott felhasználó jogosult-e az áthaladásra (hely,idő,irány) és ennek megfelelően működtesse az APAS-t. Az áthaladást szabályozó és érzékelők (APAS, az angol Access Point Actuators and Sensors meghatározásból) feladata, hogy csak a jogosultak áthaladását tegye lehetővé, illetve a jogosulatlanok áthaladását akadályozza mechanikusan vagy elektromechanikusan valamint ezek állapotát képes legyen meghatározni [2].

A felügyeleti rendszer feladata a jogosultságok eldöntése, a vezérlő egységek felügyelete, az események rögzítése és naplózása, hogy később visszakereshető, listázható legyen.

A beléptető rendszereknél megkülönböztetünk online és offline rendszereket. Az online rendszerek esetében a jogosultságok lekérdezése minden esetben a felügyeleti rendszertől történik, még az offline rendszerek esetében a jogosultságok a vezérlő egységekben vannak letárolva a rendszer üzemeltetői ezeket módosíthatják illetve kiolvashatják a naplózott eseményeket.

Az áthaladási szabályozó eszközök működésük szempontjából lehetnek életvédelmi (fail safe) vagy vagyonvédelmi (fail secure). Életvédelmi abban az esetben ha tápkimaradáskor az eszközök állapota nyitott, vagyis szabaddá válik a menekülési útvonal. Vagyonvédelmi abban az esetben ha tápkimaradáskor állapota zárt.

A beléptető rendszereknél használt fogalom az antipassback. Ennek lényege a beléptető azonosító visszaadásának megakadályozása. Az antipassback lehet logikai (egymás után tiltja az azonos irányú áthaladást), időzített (adott időn belül nem engedélyez áthaladást), területi ellenőrzött (csak a rendszer által nyilvántartott helyről engedélyezi az áthaladást) valamint ezek kombinációja.

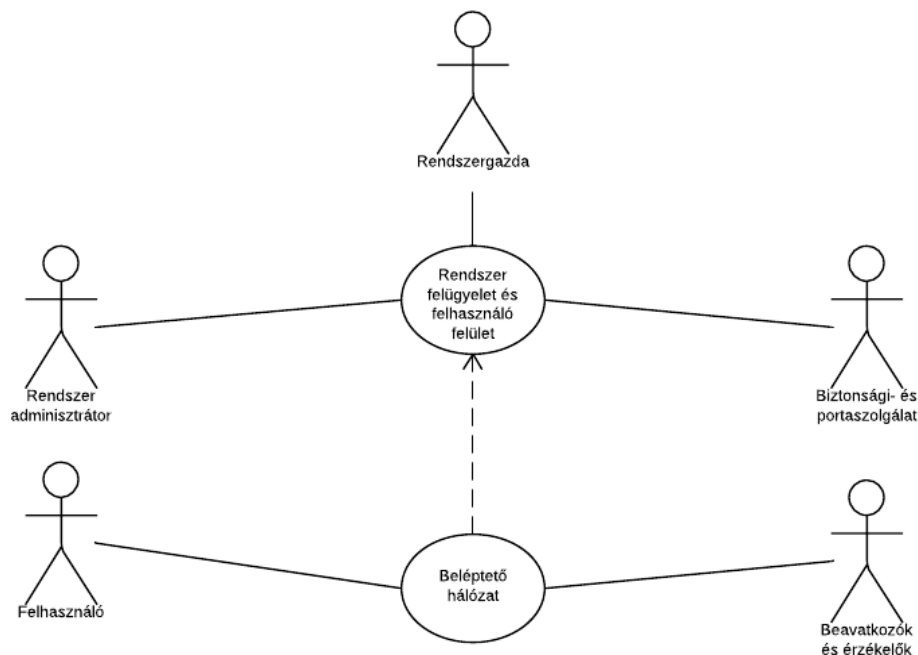
A beléptetés folyamata az azonosítást (személy,gépjármű, stb.) követően a belépési jogosultságok eldöntése, ennek megfelelő bavatkozás (APAS működtetése), áthaladás és visszazárás. A rendszer kialakításának megfelelő további funkciók feladatainak elvégzése (naplózás, rendszerfelügyelet, stb.).

3. A beléptető rendszerrel szemben támasztott követelmények

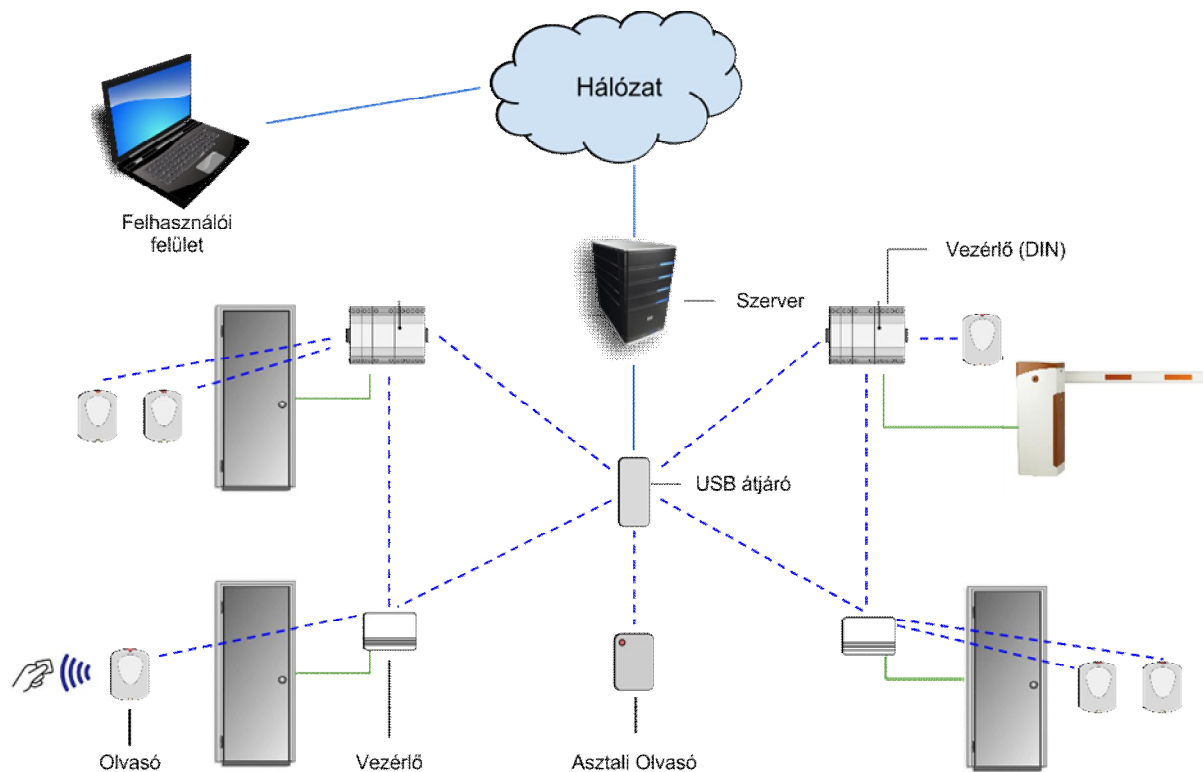
A tervezett beléptető rendszer meglévő biztonságtechnikai rendszerek kiegészítő rendszereként kell működnie de, fenn kell tartani a továbbfejlesztés lehetőségét. Az elsődleges biztonsági rendszerek a portaszolgálat, a riasztó és kamera rendszer. Ezek kiegészítőjeként a beléptető rendszernek alkalmasnak kell lennie az adott átjáróknál csak az arra jogosultak mozgását engedélyezni, illetve a mozgásuk naplózását, valamint nem akadályozhatja veszély esetén a menekülést.

A beléptető rendszer kialakításának meg kell felelni a beléptető rendszerek általános felépítésének. A rendszerben az azonosítandó felhasználók és az átjárók a beléptető hálózat.

A felügyeleti rendszerhez hozzáférést kell biztosítani a rendszergazdán kívül különböző hozzáférési jogosultsággal a rendszer adminisztrátorainak, valamint biztonsági és portaszolgálatnak. A beléptető rendszer szerepköreit az 1. ábra mutatja.



1. ábra A beléptető rendszer szerepkörei



2. ábra Beléptető rendszer felépítése

A beléptető rendszerben az azonosítást az alacsony költségek elérése érdekében RFID alapú technológiával kell megoldani. Az RFID alapú azonosítás biztosítja az elvárt biztonsági szintet és a technológia alkalmazásához szükséges eszközök ára is megfelelő.

A beléptető rendszer kommunikációjának vezeték nélküli megoldásnak kell lennie. A vezeték nélküli kommunikációval csökkenthetőek a telepítési költségek és a rendszer módosítása is egyszerűbbé válhat.

A beléptető rendszer vezeték nélküli hálózatát alkotó olvasó és vezérlő eszközöknek alacsony költségűnek, a megbízható működésűnek és az egyszerűen telepíthetőnek kell lennie.

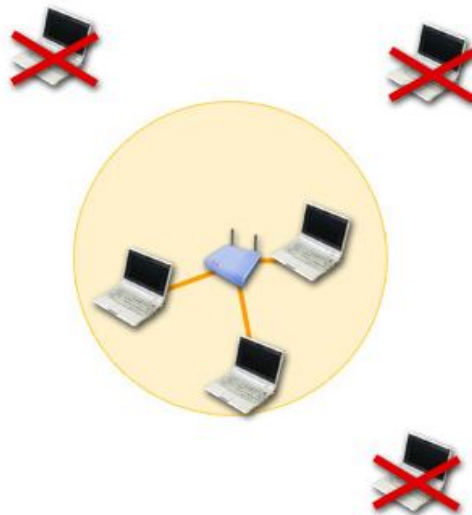
A felügyeleti rendszer központi szervét alkotó szerver szintén lehető legkisebb költségekkel megvalósító legyen. A szervernek rendelkezni kell USB porttal és Ethernet csatlakozóval a hálózathoz történő csatlakozás miatt, valamint alkalmas legyen LINUX operációs rendszer futtatására.

4. Jelenleg elterjedt kis hatótávolságú rádiófrekvenciás hálózatok bemutatása

4.1 WiFi

A WiFi (Wireless Fidelity) nagy sávszélességű vezeték nélküli adatátvitelre fejlesztették ki. A WiFi főleg számítógépek, játék konzolok rádiós összeköttetésére használható azaz, olyan eszközök melyek nagy adatátviteli sebességet igényelnek. A WiFi is mint sok más rádiós hálózat a 2.4 GHz-es szabad frekvenciasávot használja [11].

A hálózat csillag topológia szerint épül fel. A hálózatnak szüksége van egy hozzáférési pontra (Access Point) amelyhez a végpontok kapcsolódhatnak. A [802.11](#) család egyes szabványai szerint ezek 20-60 méteres hatótávolságúak lehetnek.



3. ábra WiFi

A hálózat kialakításából adódik, hogy azok az eszközök, amik a hatósugáron kívül esnek, nem tudnak csatlakozni a hálózathoz. Ekkor újabb hozzáférési pontot vagy pontokat kell elhelyezni. A WiFi előnyeikhez sorolható a titkosítás lehetősége, ez által könnyen létrehozható mások által nem hozzáférhető zárt hálózat.

A WiFi talán legnagyobb hátránya az igen nagy energiafogyasztás, amit ha nagy adatátviteli sebességre van szükség, könnyen lenyel az ember. Továbbá az új WiFi eszközöket csak akkor lehet ellátni a "Wi-Fi CERTIFIED" jelöléssel, ha sikeresen átmentek egy teszten, amelyet az ún. WiFi Szövetség ír elő és ennek komoly költségei vannak.

4.2 Bluetooth

A Bluetooth rövid hatótávolságú adatcseréhez használt, nyílt, vezeték nélküli szabvány. Alkalmazásával számítógépek, mobiltelefonok és más elektronikus eszközök között alakítható ki kapcsolat. A hálózat pont-pont kapcsolatot alakít ki, legtöbb esetben pár méteres hatótávolsággal, de létezik egy változata (Class1) amely akár 100 méteren is képes kapcsolatot kialakítani. A hálózat nagy előnye, hogy kis energiafogyasztást igényel ez által terjedt el hordozható eszközökben, például a mobiltelefonokban.

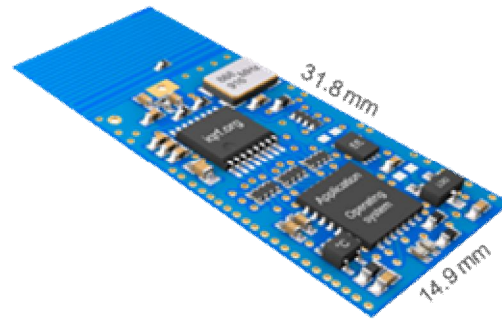
4.3 ZigBee

A ZigBee esetében, mint sok más rendszernél, az alap szabvány az IEEE által lett lefektetve. A ZigBee célja alacsony adatráta több hónapos vagy éves telep élettartalmú, kis komplexitású nem engedély köteles rádió szabvány megalkotása. A működési frekvenciája 868-916MHz vagy 2.4 GHz is lehet. A potenciális felhasználási terület a ház-automatizálástól az ipari szenzor hálózatokig terjed. Egy hálózaton belül maximálisan 65535 csomópont lehet. A ZigBee lehet koordinátor és router is, támogatja a szövevényes (mesh) topológiát, a hatótáv két eszköz között 10-500 méter lehet a környezet függvényében [4].

Az egyetlen hátránya a ZigBee hálózatoknak, hogy a protokoll zárt és licenrdíjas.

4.4 IQRF

Az IQRF a ZigBee-hez nagyban hasonló megoldás. A hálózati topológiát tekintve pont-multipont vagy szövevényes hálózat alakítható ki. A rendszer a Sub-GHz tartományban, 868MHz-es szabad frekvencia sávban működik. A rendszer maximális adatátviteli sebessége ~115kb/s lehet és egyszerre 32 bájtos csomag küldhető. Egy szövevényes hálózatot 239 csomópont és egy koordinátor alkothatja, de lehetőség van a csomópontokon keresztül további hálózatok kapcsolására, ez által akár 65000 eszközre terjeszthető ki egy komplex hálózat. A hálózatban egy modul lehet koordinátor vagy csomópont, de mindkét esetben elláthat speciális funkciókat is úgy, mint gateway vagy router.



4. ábra IQRF modul (TR52-BA)

Az IQRF modulok C nyelven programozhatóak. A modulokat a gyártó saját operációs rendszerével látja el, mely a felhasználói programot függvényhívásokkal támogat. A fejlesztés ez által igen egyszerűvé válik és a modulok komplex kialakításának köszönhetően nagymértékben csökkenthető az áramköri elemek száma, illetve kis mérete is kedvező.

Az IQRF biztosít egy általa fejlesztett, IQMESH elnevezésű ingyenes, nyílt protokollt, melyet az IQRF modulokban található operációs rendszer függvényhívások segítségével támogatja. Az IQRF további előnye a modulok alacsony fogyasztása. Üzem módtól függően áramfelvétele 3V-ról működtetve, 13mA-tól 35uA-ig, illetve alvó módban 380nA-ig csökkenthető. Ez ideális megoldást jelent elemes, vagy akkumulátoros tápellátás esetén.

4.5 MiWi

A MiWi a Microchip cég által fejlesztett vezeték nélküli megoldás, mely nagyban hasonlít az IQRF-hez. A MiWi szintén biztosít szövevényes hálózati kialakítást (MiWi PRO), viszont csak 8000 eszközre bővíthető. A MiWi kommunikációs protokollt és a hozzá biztosított könyvtárakból áll. A Microchip MiWi modulok 2.4 GHz illetve 868MHz-es frekvencia tartományban működnek. A modulhoz illeszteni kell egy mikrokontrollert, melyre a könyvtári függvényekkel megírt program kerül. A MiWi rendelkezik számos szolgáltatással a hálózati működést tekintve. Ide tartozik a szavazásos eljárás alapuló csatornaválasztás, a titkosítható kommunikáció és az automatikus hálózathoz történő csatlakozás [7].

5. Rádiófrekvenciás hálózati topológiák ismertetése

5.1 Pont-Pont kapcsolat

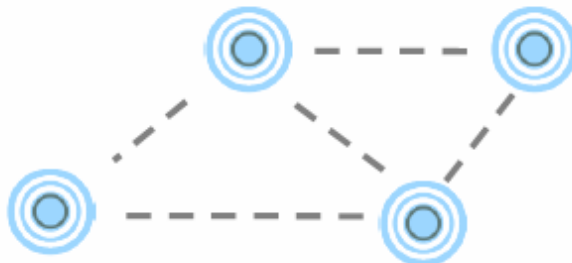
A pont-pont kapcsolat a legegyszerűbb hálózati forma két végpont között. A pont-pont kialakítás nem igényel valódi hálózati struktúrát az egyes eszközök közvetlen kapcsolatban állnak egymással, nincs kitüntetett elem a hálózatban, a végpontok egyenértékűek egymással. Ez a kialakítás olyan rendszereknél előnyös, ahol csak két kommunikációs eszköz szerepel a hálózatban, ilyen például a távirányítású kapunyitó.



5. ábra Pont-Pont kapcsolat

5.2 Pont-Multipont topológia

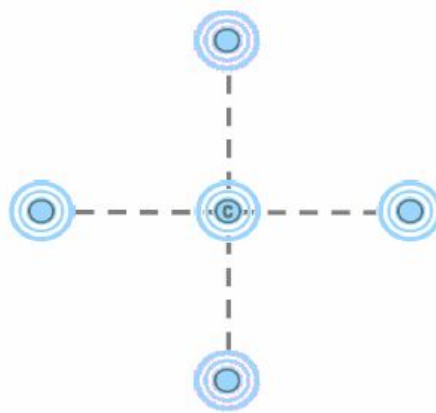
A pont-multipont kapcsolat esetében az eszközök adott hatótávolságon belül minden más végponttal közvetlen kapcsolatban állnak és azok egyenértékűek egymással. Ez a kialakítás már tekinthető valódi hálózatnak, de ebben az esetben sem igényel a rendszer központi egységet. Az adatok küldésekor nincsen lehetőség címzésre, tehát azt minden hatósugáron belül lévő eszköz megkapja.



6. ábra Pont-Multipont topológia

5.3 Csillag topológia

A csillag topológia a legelterjedtebb vezeték nélküli hálózati topológia (pl. WiFi). Ez olyan hálózatot jelent, ami egy központi bázisállomás, vagy más néven hozzáférési pont köré épül. Ez a központi egység tart kapcsolatot az egyes végpontok között, tehát azok csak ezen a bázisállomáson keresztül tudnak egymással kommunikálni. A csillag topológia esetében a küldött információ címezhető, megadott végponthoz rendelhető. A központi egységen keresztül lehetőség van más hálózatokkal történő kapcsolatteremtésre.

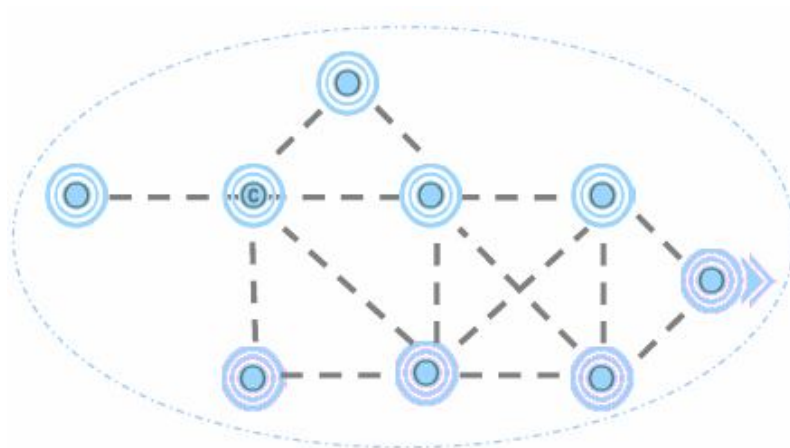


7. ábra Csillag topológia

5.4 Szövevényes (MESH) hálózat

Vezeték nélküli rádiós kapcsolatok kialakításához a legmegfelelőbb hálózati kiépítés az úgynevezett MESH topológia (ábra). Ennek lényege, hogy nincs központi berendezés, a hálózat elemei között kölcsönös kapcsolat van, a hálózat szerteágazó. Egy munkaállomás több másikkal is kapcsolatban állhat és több hálózathoz is kapcsolódhat egyidejűleg. A hálózati csomópontok - az úgynevezett node-ok - routerként viselkednek. Ezek olyan berendezések, melyek meghatározzák az elérési útvonalakat és továbbítják az üzeneteket. Nagyobb hálózatot úgy érhetünk el, hogy megnöveljük az egymáshoz kapcsolódó csomópontok számát. Ha egy berendezés meghibásodik, akkor mindig van alternatív útvonal az adatok továbbítására, ezért nem okoz fennakadást a kiesés. Ennek következtében a hálózat rendkívül megbízható, mert több úton is el lehet jutni a forrástól a célig. Úgy tűnhet ez a lehető legelőnyösebb hálózat

kiépítési forma, de azért ennek is megvannak a maga hátrányai. Például az, hogy korlátozott az átviteli sebesség illetve az adatok mennyisége.



8. ábra Szövevényes hálózat

6. RFID alapú azonosítás

A felhasználó azonosítás célja az adott személy kilétének megállapítása. Az erre kidolgozott eljárások lehetnek tudás(információ) alapúak, birtokolt tárgy illetve biometrikus tulajdonság alapúak. A biztonság fokozásához lehetőség van ezek kombinálására is. Az MSZ- (EN 50133:2006 négy felismerési osztályt határoz meg: 0- azonosítás nélküli, 1- tudás alapú, 2- tárgy alapú vagy biometrikus, 3- kombinált) [3].

Az RFID (Radio Frequency Identification) az automatizálásban igen széles körben használt azonosítási technológia. A lényege az RFID eszközön tárolt egyedi adatok olvasásával szerzett információk alapján történő azonosítás. Az RFID tag-ek (transzponderek) egy microchip-ből és egy antennából állnak. Működési elve szerint lehet passzív, aktív és fél-aktív. A legelterjedtebb ezek közül a passzív tag mely nem rendelkezik önálló tápellátással, a működéshez szükséges energiát az olvasó által gerjesztett elektromágneses térből nyeri, a fél-aktív tag rendelkezik önálló tápforrással, de ezt csak a microchip működéséhez szükséges a kommunikációhoz szintén az olvasó által gerjesztett mezőt használja. Ezen eszközök jellemző működési frekvenciatartománya 125kHz(LF), 13,56MHz(HF) és 860-960Mhz(UHF) [3][12].

A kommunikáció úgy jön létre, hogy az olvasó és a transzponder antánnaja között induktív kapcsolat keletkezik, az olvasó egység által gerjesztett tér energiájából a tag energiát nyer, a microchip ekkor „felébred”, majd a rajta tárolt adatoknak megfelelően változtatja az antenna terhelését, ezt az olvasó érzékeli és dekódolja.

7. Felhasznált technológiák és eszközök kiválasztása

A vezeték nélküli kommunikációt biztosító technológia és eszközök kiválasztásának fő szempontja, hogy támogassa a szövevényes hálózatot és védett vagy védhető legyen a hálózat a támadásokkal szemben. A másodlagos, de szintén fontos szempont az alacsony költség elérése és komplexitás. A WiFi több szempontból sem felel meg ezen elvárásoknak. A titkosítás ugyan egyszerűen megvalósítható vele de hálózati kialakítása nem megfelelő. A ZigBee-vel elérhetőek lehetnének a követelmények de zárt protokollja és költségei miatt szintén nem megfelelő.

A két legjobb megoldás a MiWi és az IQRF látszott. A két rendszer főbb tulajdonágait az alábbi táblázat mutatja.

	IQRF (IQMESH)	MiWi (Pro)
Hardver kialakítás	Modul	Modul+Mikrokontroller+kiegészítő elemek
Hálózati pontok maximális száma	239 (65000)	64*127(8192)
Hálózat kialakítása	Full Mesh- az egyes csomópontok elhelyezkedése tetszőleges, routoláskor nincsenek kitüntetett eszközök	Mesh- Routolás csak a 64 "koordinátor"+ egy végpont között
Hálózathoz való csatlakozás	Manuális	Automatikus
Csomagvesztés megakadályozása	Nincs	"Handshake" eljárással
Címzés	Hálózathoz való csatlakozáskor kiosztott cím	MAC cím alapján
Csatorna választás	Manuális	Automatikus
Titkosítás	Nincs implementálva- felhasználónak kell gondoskodni róla	Implementálva- AES vagy XTEA (64bit)
Szoftver támogatás	Operációs rendszer Fejlesztő környezet Gyári függvények Korlátozott memória terület EEPROM	Fejlesztő környezet Személyre szabható könyvtári függvények Tetszőleges mikrovezérlő illeszthető

A két rendszer között az általánosan fennálló kettősség okozott problémát a döntésben, mi szerint az egyszerű, de sok megkötést tartalmazó megoldást vagy a bonyolultabb, de személyre szabható megoldást válasszam.

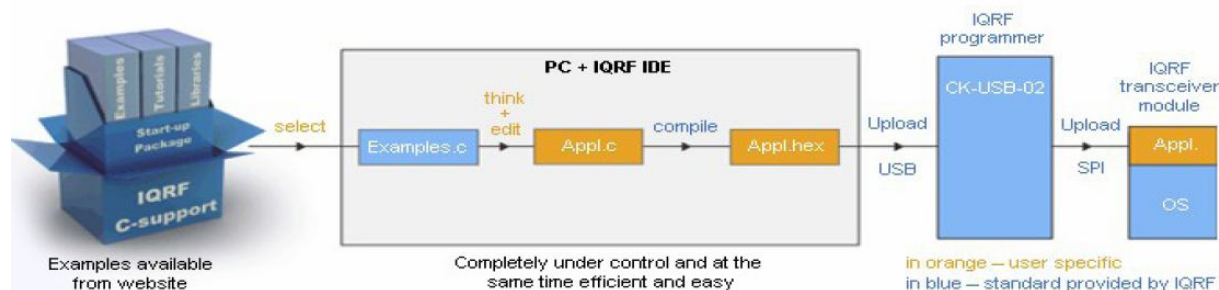
A végső döntés az egyszerűbbre esett. Azok a funkciók, ami szerint az IQRF gyengébb rendszernek tűnhet, az a felhasználói programban szinte mind implementálható.

Az egyes eszközökben az IQRF egy modulos kialakításának köszönhetően az áramköri tervezés is egyszerűbbé vált. Továbbá az IQRF rendelkezik egy megbízható operációs rendszerrel, ami növeli a rendszer stabilitását és csökkenti a fejlesztésre fordított időt. Az IQRF rendszerrel történő fejlesztés további előnye a gyors és átfogó gyártói támogatás.

A szerver kiválasztásakor több eszköz is felmerült. A biztos pont panel PC vagy ipari PC használata volt. A BeagleBoard-XM panel PC minden szempontból, jó megoldásnak tűnt de viszonylag magas költségű. Egy másik a Raspberry-PI panel PC mely rendkívül olcsó és szintén minden szempontból megfelelő eszköz. A rendszerben véglegesítve a Raspberry-PI került kiválasztásra, viszont a tesztüzemhez már rendelkezésre álló Advantech gyártmányú ipari PC került beépítésre.

7.1.1. IQRF

Az operációs rendszerhez alkalmazási program írható meg, amelyben az általunk szoftvert írhatjuk meg. A szoftverek fejlesztéséhez a gyártó minden szükséges programot és dokumentációt, illetve példaprogramokat elérhetővé tett. A programfejlesztést a saját integrált fejlesztői környezetük (IQRF IDE) segítségével végezhető. A fejlesztő környezethez a CC5X nyílt C fordító használható, tehát az alkalmazási program forráskódja bármely szövegszerkesztővel C nyelven megírható. A fordító optimalizálja a lefordított programot, viszont emiatt a szoftver írásakor több megkötést is megfogalmaztak.



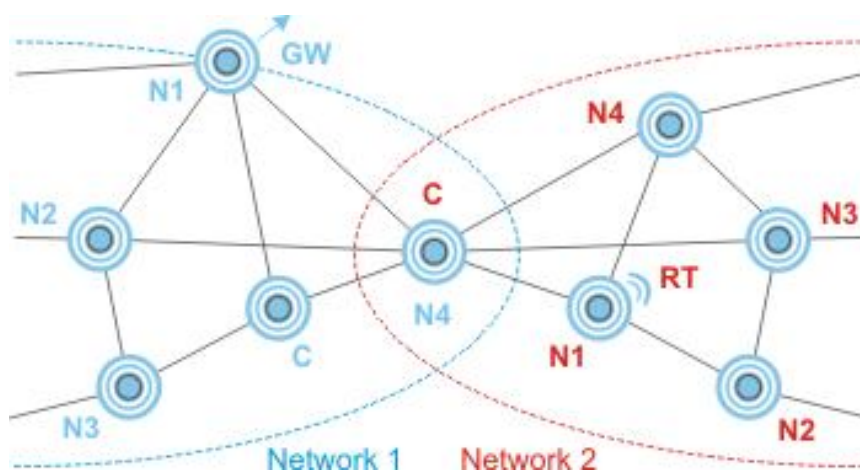
9. ábra IQRF szoftverek fejlesztésének folyamata

Az IQRF modulok egyes funkciói függvényhívásokkal valósíthatók meg. Ezekkel a függvényekkel érhetőek az egyes beállítási, adatküldési, időzítési és más lehetőségek. Ez

nagyban megkönnyíti a fejlesztői munkát. A fejlesztői környezet egyetlen hátránya, hogy a hibakeresési funkciók erősen korlátozottak.

7.1.2. IQMESH

Az IQMESH hálózat az IQRF készítői által fejlesztett nyílt protokoll. Az IQMESH hálózat egy ún. koordinátor és maximum 239 node-ból, csomópontból épül fel. A teljes hálózat tovább bővíthető, ha egy csomópont egy másik hálózatban a koordinátor szerepét tölti be(ábra). Így a teljes hálózat akár 65000 eszközre is kibővíthető, csak az eszköz azonosító címének hossza korlátozza az elemek számát. A hálózatban beállítható a hálózati szűrés, ami arra szolgál, hogy ha két különálló rendszer működik egymás közelében, akkor sem zavarják egymás működését. A hálózathoz tartozhatnak átjárók (gateway), amelyekkel csatlakozhatnak más hálózatokhoz (pl. internet) [5][6][9].



10. ábra IQMESH hálózat

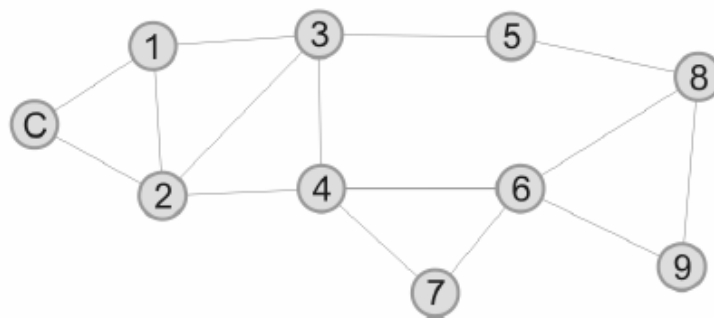
Az IQMESH hálózatokban kitüntetett szerepű a koordinátor, ez többek között ellátja a hálózat adminisztratív feladatait. A hálózat felépítésekor a csomópontokat (node) párosítani kell a hálózathoz (bonding), ekkor a koordinátor kioszt egy statikus címet, amelyre a további kommunikáció során hivatkozni tud.

Minden koordinátorhoz maximum 239 node tartozhat, ezek együttese alkot egy hálózatot melynek egy külön hálózati azonosítója van, és a hálózatok közötti kommunikáció ez alapján címezhető.

A csomópontok az operációs rendszernek köszönhetően a háttérben képesek routerként is működni. Ez által koordinátor hatótávolságán kívül is elhelyezhetők csomópontok, tehát a hálózat hatótávolsága nagyban növelhető anélkül, hogy el kellene helyezni külön eszközöket a jel továbbítására, szemben más hálózatokkal.

A hálózatnak egy fontos tulajdonsága a routolási idő. A küldött csomag minden egyes ugráshoz (hops) megközelítőleg 10ms időre van szüksége standard üzemmódban. A routolási időt tehát az ugrások száma határozza meg, ami a növekvő eszközszámmal arányosan nő.

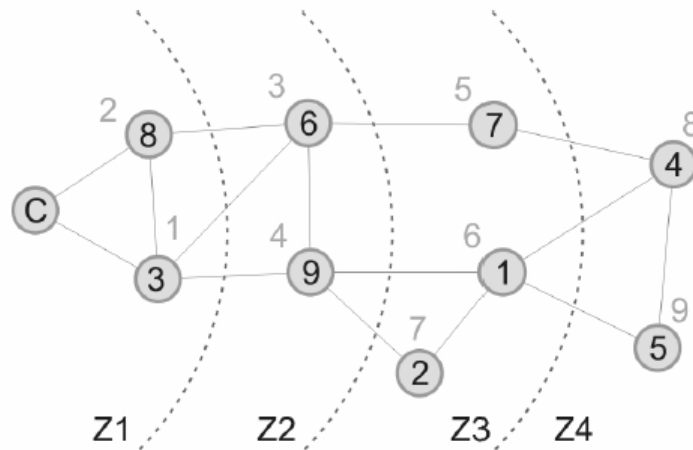
A csomagok továbbítására az IQMESH hálózatban két kialakítás áll rendelkezésre, a DFM (Discovered Full Mesh) és SFM (Static Full Mesh). A SFM esetében a hálózati párosításkor a kiosztott címek alapján növekvő sorrendben kell a csomópontokat elhelyezni (ábra) a koordinátortól („C”). A csomagok küldéséhez, ha szükség van továbbításra, meg kell adni a maximális ugrások számát [9].



11. ábra Static Full Mesh (SFM)

A DFM esetében tetszőleges sorrendben helyezhetők el az eszközök (ábra). Ez esetben a hálózatot használat előtt fel kell térképezni (discovery), melynek során a koordinátor minden eszközhöz hozzárendel egy VRN (Virtual Routing Number) számot és a rendszert több zónára osztja. A zónák kialakításának a mért jelerősség szolgál alapul. A VRN szám csak az operációs rendszernek szolgáltató információt az elküldött csomagok routolási sorrendjéhez. A csomópontok továbbra is a statikus címükkel címezhetők.

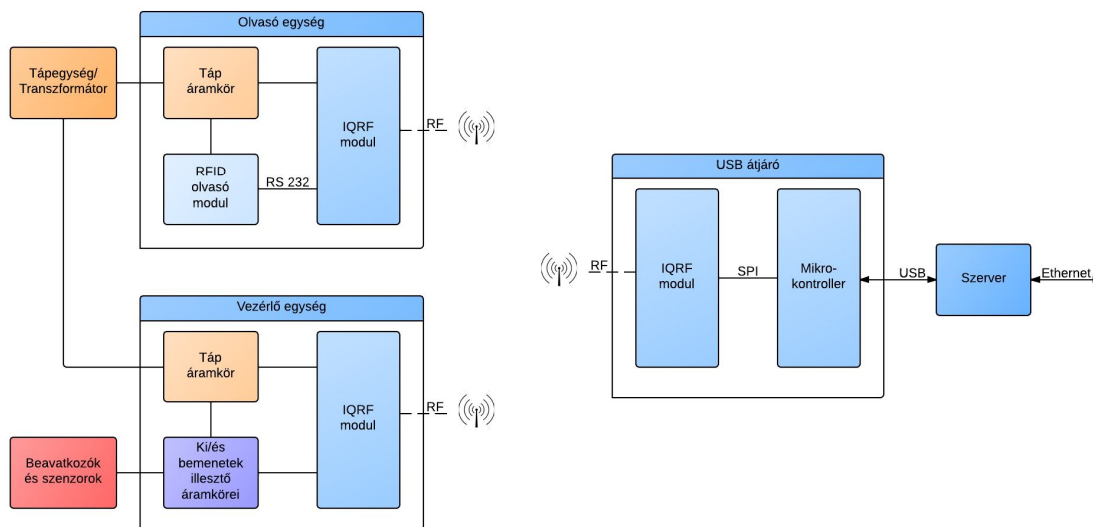
A DFM kialakítás egy speciális lehetősége az ugrások számának optimalizálására, ez az ún. DOM (Discoveres Optimized MESH). Az optimalizálást az operációs rendszer végzi el a háttérben. Ez a kialakítás nagymértékben megkönnyíti a hálózat telepítését.



12. ábra Discovered Full Mesh

8. Fizikai réteg tervezése

A beléptető rendszer két főbb egységre bontható, a vezeték nélküli hálózatot alkotó egységekre valamint a felügyeleti rendszerre. A vezeték nélküli hálózat egységei az olvasó, vezérlő valamint az USB-átjáró. Az olvasók feladata a felhasználók RFID azonosítójának olvasása és továbbítása a hozzá tartozó vezérlőhöz. A rendszerhez tartozik egy asztali olvasó is, mely a hálózathoz csatlakozva könnyíti meg az RFID azonosítók adminisztrációját. A vezérlők feladata az olvasóktól érkező adatok továbbítása a szerver felé és az átjárók működtetése. A vezérlők másodlagos feladata az épületautomatizálási feladat ellátása, az ehhez tartozó ki-és bemenetek felügyelete.



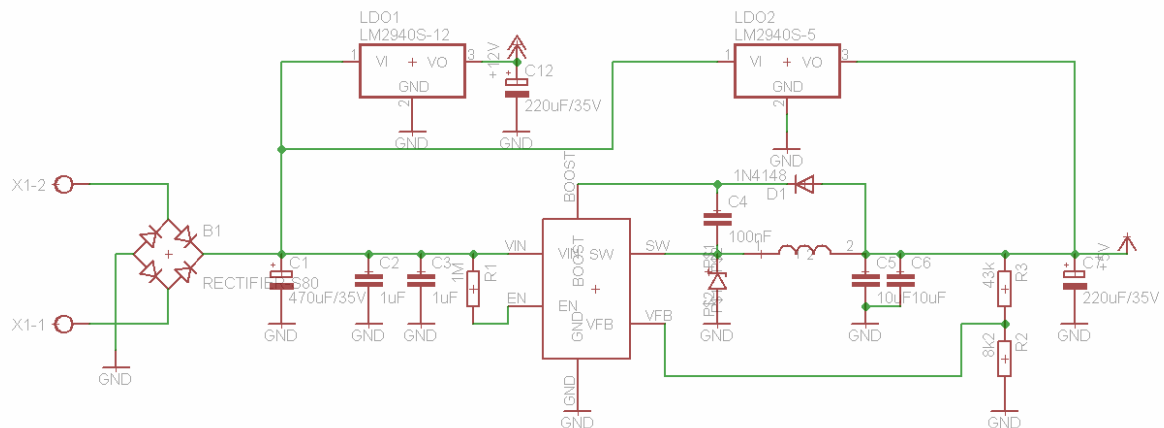
13. ábra Beléptető rendszer kialakítása

A beléptető rendszer vezeték nélküli hálózata és a felügyeleti rendszer között az USB-átjáró teremt kapcsolatot, mely USB-n keresztül csatlakozik a szerverhez. A rendszer felügyeletét a szerveren futó monitor program végzi a szintén a szerveren lévő adatbázis használatával. A rendszer web-alapú adminisztrációs, grafikus felhasználói felületének eléréséhez a szervernek Ethernet hálózathoz kell csatlakoznia.

A grafikus felület elérése bármilyen, böngészővel rendelkező eszközzel lehetséges. Ennek a megoldásnak köszönhetően a felhasználói felület bármely operációs rendszerről speciális program telepítése nélkül elérhetővé válik.

A tervezésnél fontos szempont volt, hogy az egyes eszközök lehetőleg kevés áramköri elemet tartsanak, ezzel is csökkentve a meghibásodás lehetőségét és a gyártási költségeket. Minden egységben megtalálható az IQRF rádiós modul, amely biztosítja a kommunikációt. Az egyszerű áramkörhöz történő illesztés és hibajavítás érdekében a 8 pólusú SIM tokba helyezhető modul lett választva az eszközökhöz.

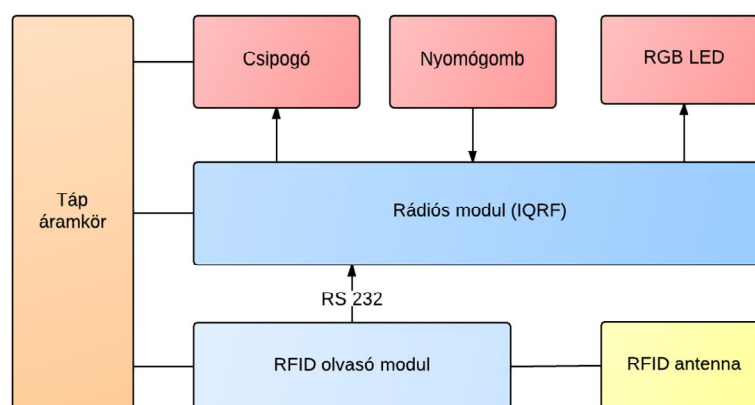
Az olvasó és vezérlő egységekben azonos tápáramkör került kialakításra. A tápellátásért felelős áramkör úgy lett kialakítva, hogy 7-30V-os váltakozó vagy egyenfeszültséggel is táplálható legyen. A feszültség stabilizálást egy olcsóbb lineáris IC vagy a magasabb hatásfok eléréséhez egy kapcsoló üzemű IC (MCP16301) is helyet kapott, ami valamivel nagyobb költségű.



14. ábra Táp áramkör

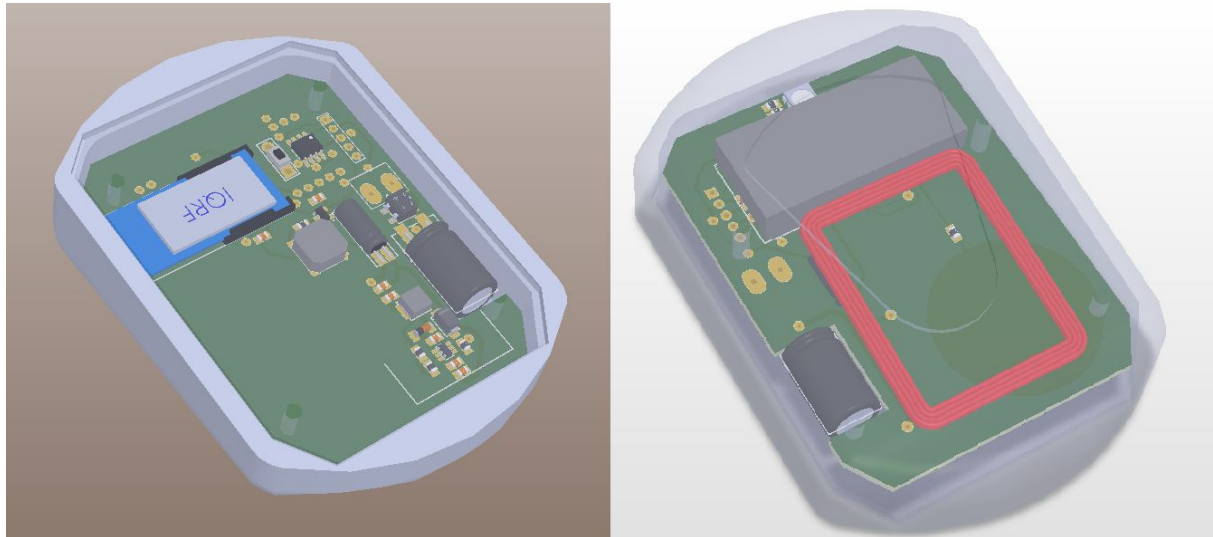
8.1 Olvasó eszközök

Az olvasó egység a tápáramkör és a rádiós modulon felül tartalmazza az RFID azonosítók olvasására alkalmas modult, egy RGB LED-et megjelenítő elemként valamint egy csipogót.



15. ábra Olvasó eszközök felépítése

Az RFID olvasó UART-on keresztül kommunikál így azt csak egy vezetékkel kellett összekötni a rádiós modullal. Az egységben található még egy csipogó is, ami a LED-el együtt a felhasználó tájékoztatására szolgál. A csipogót külső meghajtóval kellett ellátni, amit egy céláramkör és kettő meghajtó FET alkot.

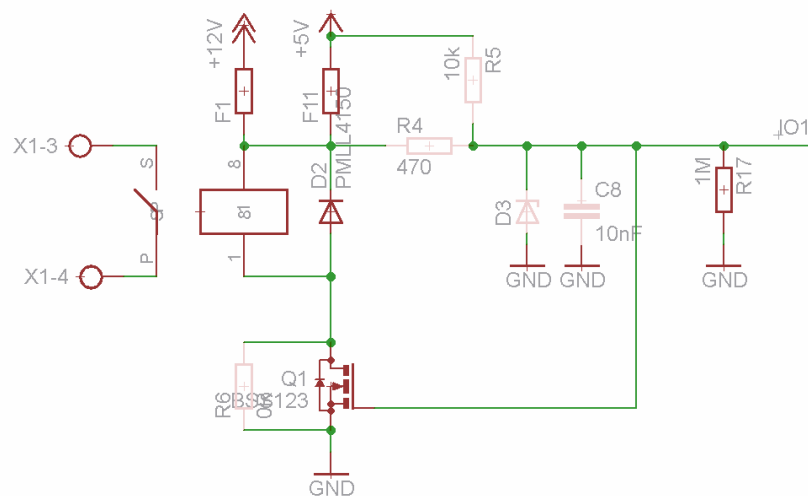


16. ábra Olvasó egység 3D-s képe

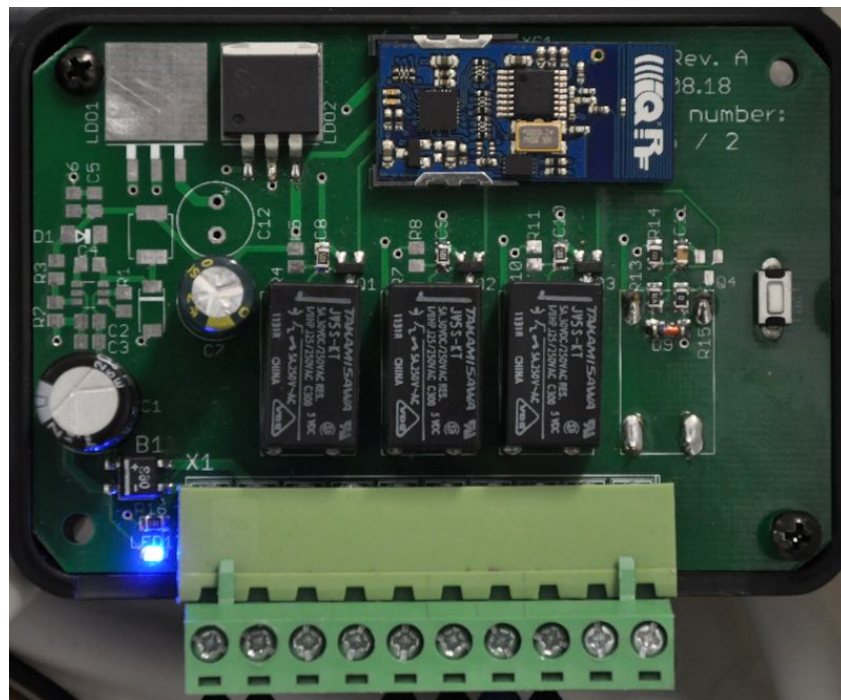
8.2 Vezérlő eszközök

A vezérlőbe integrálásra kerültek a szabályozó és érzékelő feladatok, ez által csökkenhetett a hálózat elemeinek száma. A vezérlőben az IQRF modulnak köszönhetően kevés áramköri elemre van szükség. A vezérlő áramköri kialakításánál a fő feladat a ki- és bemenetek illesztése volt. A költség hatékony kialakítás elérése érdekében a vezérlő multifunkciós kialakítással rendelkezik. Az egységben 4 be- illetve kimenet található, melyek a beültetett áramköri elemektől függően lehetnek be vagy kimenetek.

Kimenet kialakításakor két megoldás is alkalmazható. Passzív kimenetként egy relé gondoskodik a kapcsolásról. Ekkor csak a logikai FET-et, a hozzá tartozó lehúzó ellenállást, a relét és visszáram diódát, valamint az 5V-os tápfeszültséghez tartozó biztosítékot kell beültetni, vagy helyettesíteni egy 0 Ohm-os ellenállással. Aktív kimenet esetében a bemenethez hasonlóan a relét átkötéssel kell helyettesíteni és a visszáram diódát elhagyni. Aktív kimeneteknél lehetőség van a regenerálódó biztosíték 5V vagy 12V-ra történő kötésével kimeneti feszültség választására. A 12V-os feszültség használatakor a 12V-os lineáris feszültség stabilizátor IC-t is az egységbe kell ültetni.



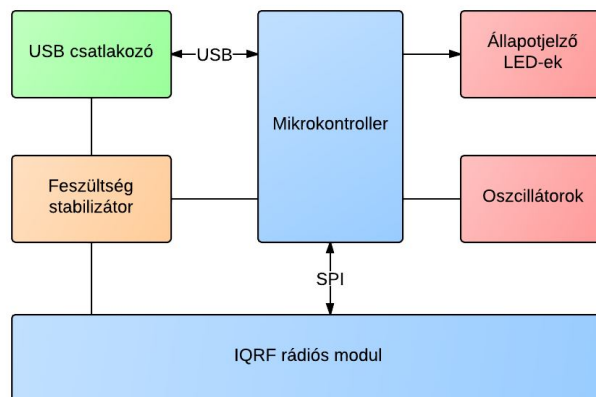
19. ábra Kimenetek



20. ábra Az üzembe helyezett vezérlő egység

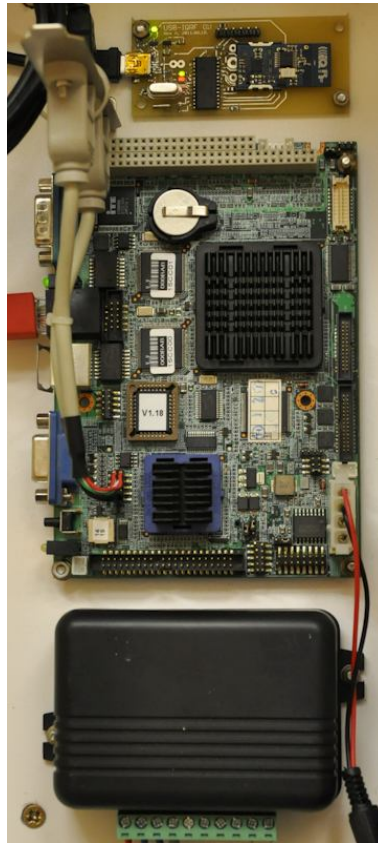
8.3 USB átvjáró

Az USB átvjáró szintén tartalmazza az IQRF rádiós modult, valamint egy PIC24FJ64GB002 Microchip gyártmányú mikrokontrollert. A mikrokontroller 3,3V-os tápfeszültséget használ, az USB port 5V-os feszültsége miatt egy feszültség stabilizátor IC kellett elhelyezni.



21. ábra USB-átjáró felépítése

Az USB kommunikációhoz pontos órajel elérésének érdekében külső oszcillátor kellett illeszteni. Az USB eszköz állapotának kijelzéséhez az eszköz tartalmaz egy piros és egy zöld LED-et is.



22. ábra Szerver (középen), USB-átjáró (fent) és vezérlő egység (lent)

9. Szoftvertervezés

A rendszer sajátosságai miatt szoftverfejlesztést több részre kellett bontani. Első lépés a hálózat felhasználói rétegének protokollját kellett kialakítani, úgy hogy minden funkció ellátására alkalmas legyen az egyszerűség fenntartásával. A következő lépésként a vezeték nélküli hálózatot alkotó IQRF modulok programjainak megírása volt. Végezetül a szerver kialakítása, valamint a monitorprogram és a web-alapú grafikus felhasználói felület szoftver tervezése következhetett.

9.1 Felhasználói réteg protokollja

A következőekben leírt protokoll a felhasználói réteghez tartozik. A protokoll a rendszer sajátosságainak megfelelően került kialakításra. A protokoll végső kialakításában 8 bájtos hosszúságú lett, ez lefedi valamennyi funkcióhoz tartozó küldendő adatokat.

A protokoll nulladik bájtja tartalmazza a parancsokat. A parancs bájt alsó 4 bitje tartalmazza a főparancsot, a felső 4 pedig a főparancshoz tartozó egyes alparancsokat.

0. Bájt		1. Bájt	2. Bájt	3-7 Bájt				
Alparancs	Főparancs	Vezérlő	Olvasó					
Parancs		Cím		Adat				

Az első és második bájtja a vezérlők és a hozzájuk tartozó olvasók címeinek van fenntartva. A monitor program ez alapján azonosítja be, hogy mely olvasó modultól érkezett a kérelem. Az utolsó 5 bájt alkotja a protokoll adat blokkját. Ebben az 5 bájtban kerülnek továbbításra az RFID azonosítók, valamint az egyéb funkciókhoz tartozó információk.

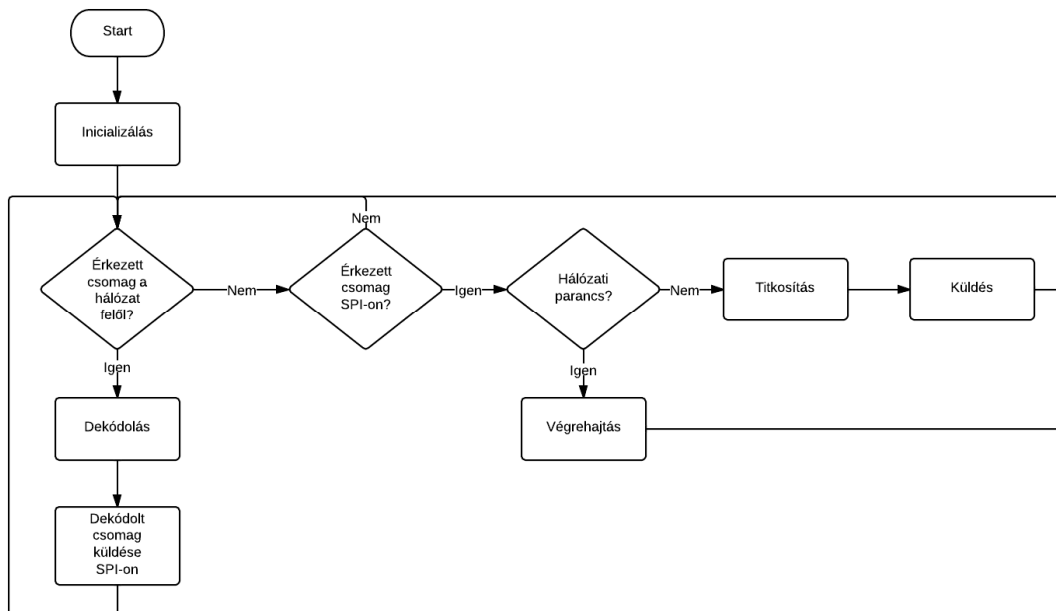
9.2 IQRF modulok szoftvere

Az IQRF-ek programjainak elkészítése a korábban leírt specifikációknak megfelelően került elvégzésre. A programoknak tartalmaznia kell az IQRF IQMESH hálózat kialakításához szükséges függvényhívásokat és programrészleteket, a felhasználó réteg protokolljának implementálását, az eszköz specifikus eljárásokat illetve rendszer hiányosságából adódó funkciók helyettesítő megoldásait.

Az eszköz kiválasztás bekezdésben leírt hiányosságokat a felhasználói programban kellett megvalósítani. Ezek a csomagvesztések megakadályozása és a titkosítás.

9.2.1. Koordinátor szoftvere

A szervernél elhelyezkedő USB-átjáróban található IQRF modul a vezeték nélküli hálózat koordinátora. A koordinátorban, első sorban meg kellett valósítani az SPI kommunikációt, hogy képes legyen kapcsolatot teremteni a mikrovezérlővel. Az SPI kezelését az operációs rendszer a háttérben végzi, bizonyos függvényhívásokkal van lehetőségünk annak használatára. A használat előtt engedélyezni kell az SPI kommunikációt. Adatok fogadásakor le kell kérdezni az SPI állapotát, hogy érkezett-e adat. Ha érkezett adat és a CRC ellenőrző összeg rendben volt, megkezdődhet az adatok kiolvasása a buffer-ből.



23. ábra IQRF koordinátor modul programjának folyamatábrája

Amikor a koordinátor csomagot fogad SPI-on megvizsgálja a protokoll szerinti nulladik bájtot, hogy neki érkezett-e a csomag, vagy tovább kell-e küldenie a hálózat felé, tehát itt valósul meg az átjáró szerepe.

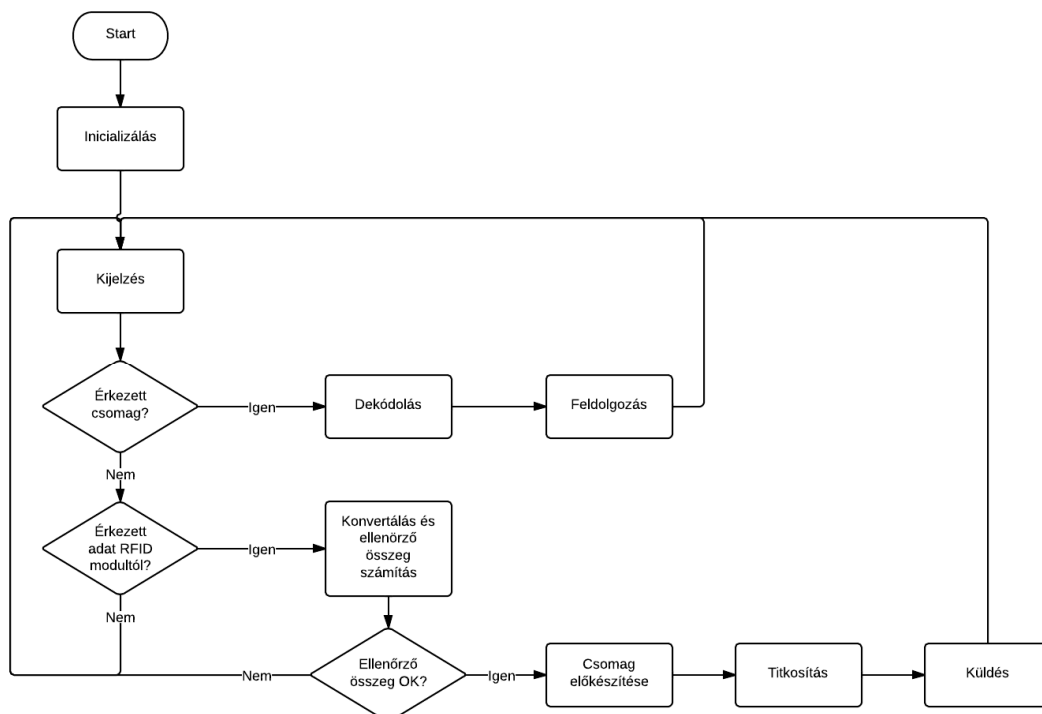
Amennyiben a koordinátor számára érkezett csomag, akkor csak az első kettő bájtot veszi figyelembe. Az első bájt határozza meg a hálózati parancsot, a funkció kiválasztását, a második bájtban pedig a parancsokhoz tartozó beállításokhoz tartozó információ található.

A hálózat felől érkező titkosított csomagokat először a program dekódolja és érvénytelen csomag esetén eldobja. Ellenkező esetben SPI-on küldi a mikrokontrollernek.

9.2.2. Olvasó modul szoftvere

Az olvasó modulok fő feladata az RFID tag-ek olvasása. Ennek megfelelően a program várakozik az RFID modultól érkező adatokra, valamint a hálózat felől érkező csomagokra. A hálózat felől csak hálózati információ illetve a kijelzéssel kapcsolatos adatok érkehetnek.

Az RFID modultól érkező adatok esetén szükséges dekódolni a beérkező információt. Az RFID modul 13 bájtban küldi el a beolvasott tag azonosítót és az ellenőrző összeget. Az 5 bájtos azonosító ASCII karakterekben kódolt hexadecimális számokként érkezik. A konvertálás és az ellenőrző összeg vizsgálata és egyezése után jogosultságok lekérdező csomagot küld a vezérlő modul felé.

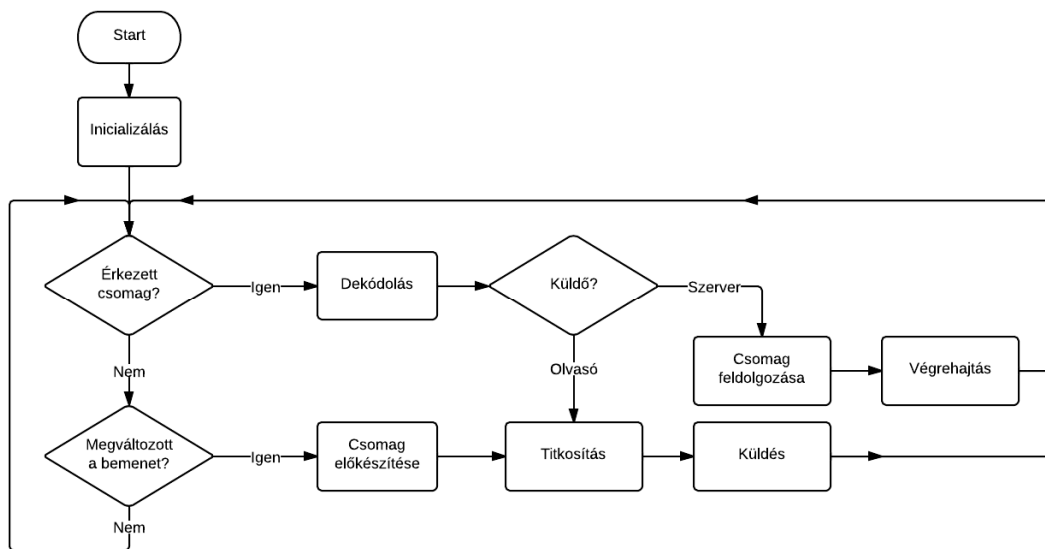


24. ábra Olvasó modul programjának folyamatábrája

9.2.3. Vezérlő egységek szoftvere

A vezérlő egységek feladata az olvasók felől érkező azonosítási kérelem valamint a bemeneteken történő változások detektálása és továbbítása a szerver felé és a szerver felől érkező beavatkozási parancsok végrehajtása.

A be-és kimenetek, valamint az átjárót működtető kimenet és az áthaladás érzékelő bemenet a programban előre definiálva van, így a különböző kialakítású egységeknél csak ezeket kell megfelelően meghatározni a továbbiakban azonosan működnek. A vezérlők automatikusan határozzák meg a hozzájuk tartozó olvasókat a hálózati azonosítójuk alapján.



25. ábra Vezérlő egység folyamatábrája

9.3 USB-átjáró

A korábbiakban már említésre került, hogy az USB átjáró egy korábbi projekt egyik hallgatójának munkája. Az USB-átjárón található Microchip PIC mikrovezérlő a Microchip USB könyvtárait használja. A könyvtárban található előre elkészített mintaprogramok egyedi igények szerint alakítható. Az átjáró USB HID könyvtárát használja, így az eszköz USB HID eszközként ül be. Az USB eszköz másik oldalán az IQRF modullal SPI-on keresztül kommunikál. Az IQRF egyedi protokollt használ. Az IQRF modul nem kezdeményez kommunikációt, minden esetben a mikrovezérlő feladata lekérdezni a modult. A modul előre meghatározott információval tudatja a mikrokontrollert aktuális állapotáról. Ezzel a megoldással valósítható meg a hibakezelés.

9.4 Szerver

A beléptető rendszer felügyeletét a szerver látja el. A szerver az USB-átjárón keresztül tart kapcsolatot a hálózattal.

Az alacsony gépigény miatt szinte bármilyen PC alkalmas a szerver szerepének betöltésére. A jelenlegi kialakításban egy panel PC van.

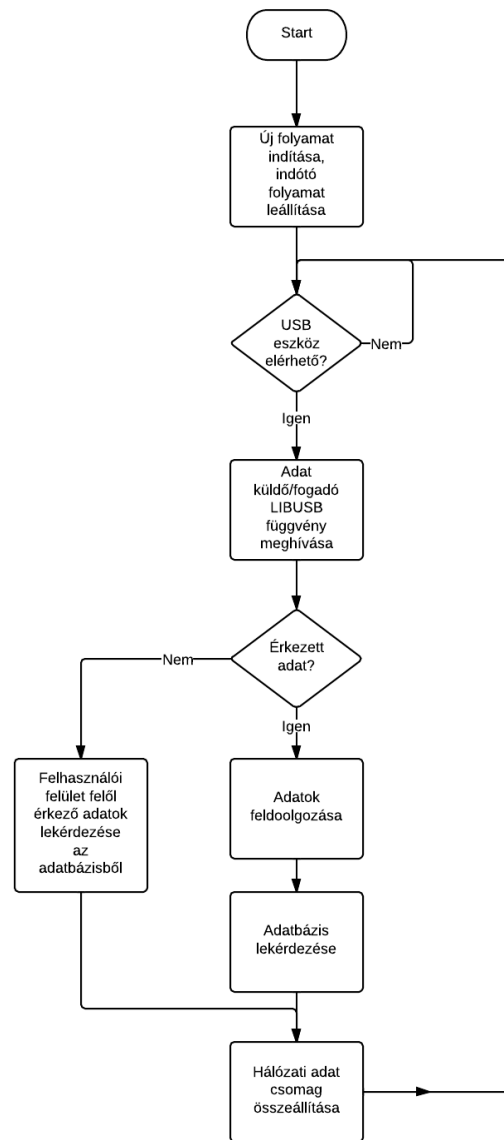
A hatékony és gyors fejlesztés érdekében a szerver Debian alapú LINUX operációs rendszerre lett fejlesztve. A hálózattal történő kapcsolattartást a monitor program látja el. Ez a program kezeli az USB HID eszközként beülő USB-átjárót és teremt kapcsolatot a MySQL adatbázissal.

A rendszer fejlesztésének utolsó lépéseként készítettem egy webes alapú grafikus megjelenítő felületet, amiben az adatbázis egyszerű kezelésén felül helyet kapott néhány extra funkció is.

9.4.1. Monitor program

A monitor program feladatai az USB HID eszköz kezelése, a hálózat felől érkező kérelmek adatbázisból történő kiszolgálása, válaszüzenetek küldése, valamint az adatbázis ciklikus olvasása a felhasználói felületről érkező kérelmek kiszolgálásához.

A monitor program a szerver indulásakor automatikusan elindul és fut a háttérben „daemon” kiszolgálóként. Az USB eszköz állapotáról az USB HID könyvtár segítségével, az operációs rendszertől lekért információk alapján értesül a program, valamint e könyvtár függvényével küld, illetve fogad adatokat és adja át a főprogramnak. Az USB eszköztől érkező adatok esetében a program megvizsgálja milyen paranccsal érkezett a csomag. Ezt követően a MySQL adatbázisból lekérdezi a beérkezett adatot és válaszüzenetet állít össze, majd küldi a meghatározott eszköznek.



26. ábra Monitorprogram folyamatábrája

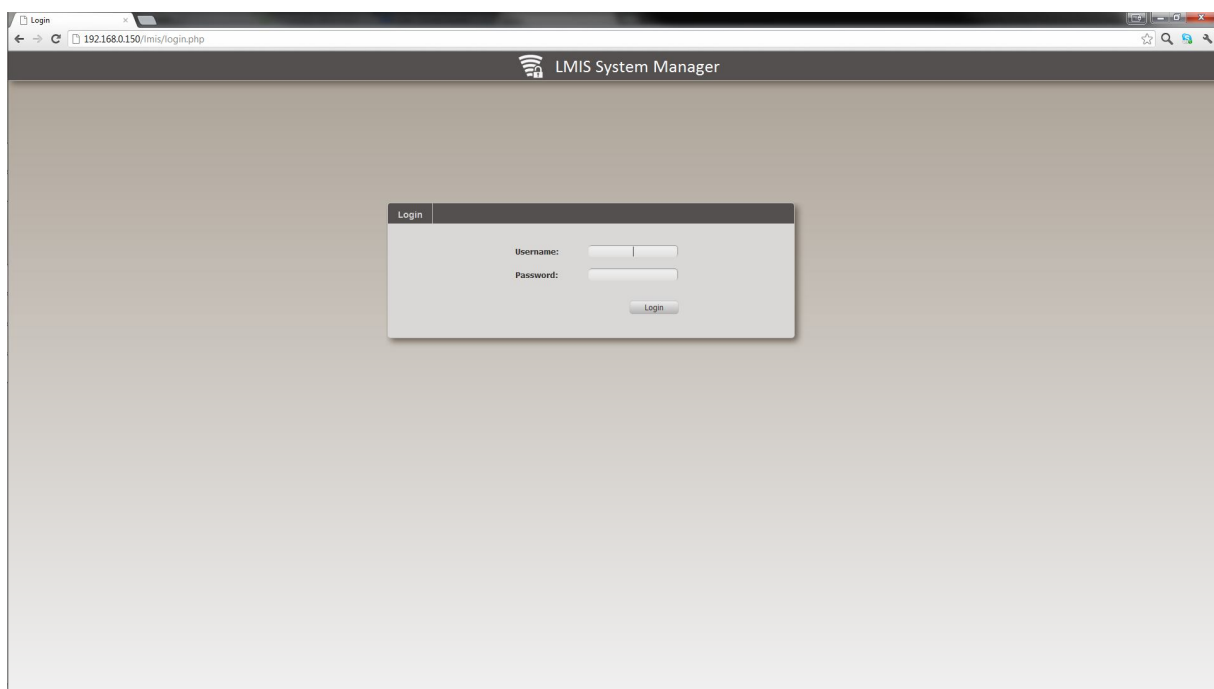
Az adatbázis lekérdezése szintén könyvtári (mysql,mysqlapi) függvények segítségével történik. Lekérdezéskor minden esetben egy új kapcsolatot kell létrehozni a MySQL szerverrel. A kapcsolat létrehozásához szükséges a szerver címe (azonos a szerver címével-localhost), felhasználónév és jelszó valamint a használni kívánt adatbázis neve (ezek ez a adatok a telepítéskor kerülnek definiálásra egy titkosított könyvtárba). Abban az esetben ha a kapcsolat sikeresen létrejött, a program elküldi a lekérdezést és a lekérdezés eredményét feldolgozza. A lekérdezés és feldolgozás minden parancs esetében különböző. Ezek mindegyikéhez külön-külön megírt saját függvények gondoskodnak.

9.4.2. Grafikus felhasználói felület

A rendszer kialakításának végeztével célszerűnek láttam egy grafikus felhasználói felület megalkotását. A felhasználói felületet az egyszerűbb használat miatt webes alapúra terveztem így a meglévő rendszer szerverén futhat, ez által a rendszer használóinak nem kell külön szoftvert telepíteni az egyes számítógépekre. A grafikus feleletet PHP (Hypertext Preprocessor), HTML (HyperText Markup Language), JavaScript és CSS (Cascading Style Sheets) segítségével, valamint AJAX (Asynchronous JavaScript and XML) használatával írtam meg. A dinamikus megjelenítés mellőzhetetlen eszköze a PHP. Ennek segítségével a szerver oldalon lefutó scriptek alakítják a megjelenített felületet, valamint végez műveleteket a szerveren (pl SQL lekérdezések). Az AJAX nem program nyelv, hanem egy eljárás. Segítségével a kliens oldalon lefutó JavaScript kód egy kérelmet küld a szerverhez ahol a PHP scripttől visszaküldött információkkal frissíthető a megjelenített felület.

A felhasználói felület kialakításakor szem előtt tartottam az egyszerűséget és könnyen képezhetőséget felhasználói oldalról. A grafikus felületen keresztül lényegében a rendszer által használt adatbázis kezelhető és a háttérben megbúvó esetleges bonyolultabb felépítést a felhasználó nem látja így egyszerű válik a kezelés. A grafikus felület igazodik a rendszer tulajdonságaihoz. A főbb menüpontok ezt próbálják meg követni az extra lehetőségekkel kiegészítve.

A rendszer biztonságos üzemeltetése miatt, a felületre csak az arra jogosultak léphetnek be, ezt egy login script biztosítja. A grafikus felület bármely oldalára navigálva, a szerveren lefut egy munkamenet ellenőrző script. Amennyiben érvénytelen a munkamenet automatikusan a login felületet tölti be. A belépéshez szükséges egy felhasználónév és jelszó.



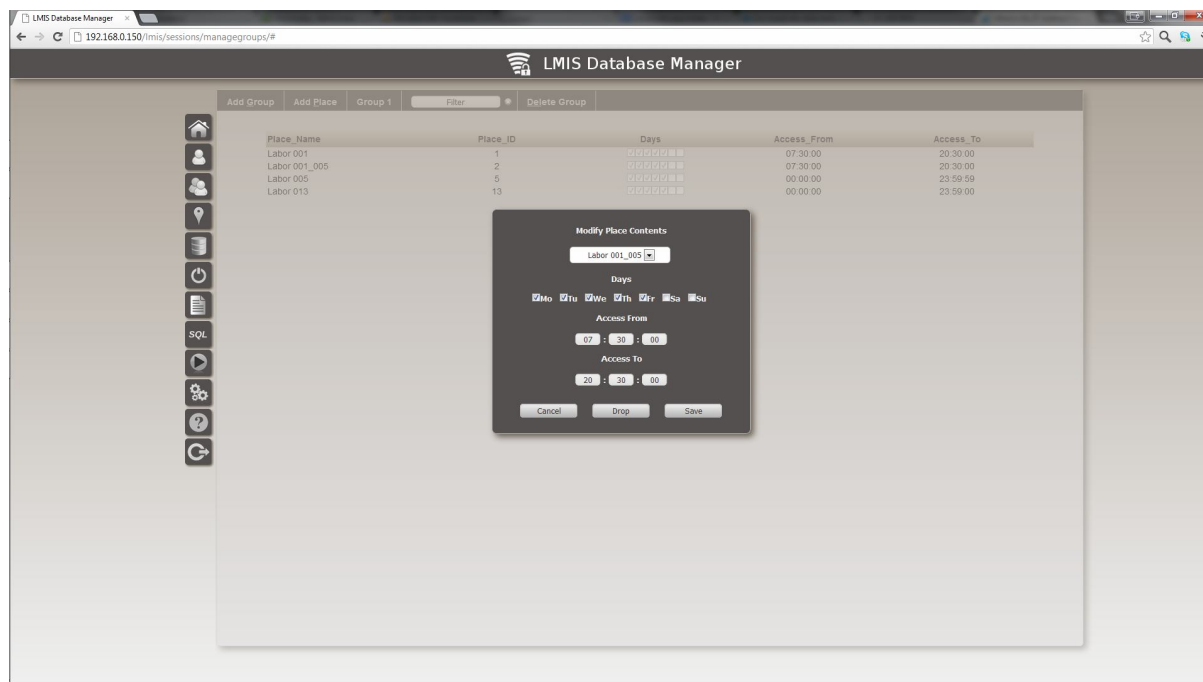
27. ábra Login felület

Annak érdekében, hogy ugyanaz a felület használható legyen adminisztrátor és felhasználó (pl. porta szolgálat) számára is a felület felhasználóihoz más jogosultsági szintek tartoznak. Ez azt jelenti, hogy alacsonyabb jogosultsági szinttel rendelkező felhasználó nem érhet el bizonyos menüpontokat. A továbbiakban ezt nem részletezve az összes funkció kerül leírásra. A belépéskor MySQL adatbázisból kérdezi le a megadott felhasználó nevet és jelszavát. A jelszó természetesen titkosítva kerül továbbításra, illetve az adatbázisban tárolásra. A megadott adatok ellenőrzése után, sikeres belépés esetében a főoldalt tölti be és elindít egy 15 perces munkamenetet, mely az idő letelte után automatikus megszüntet és oldal újra töltéskor ismét a login felületre navigál.

A rendszer telepítése során meg kell határozni a rendszer vezérlő egységeinek helyeit. Ez azt jelenti, hogy a hálózat egyes elemeinek hálózati címéhez a felhasználó által értelmezhető névvel kell ellátni. Ezt követően a felhasználói felületen az egyes helyek már ezzel a hozzárendelt, szimbolikus névvel fognak megjelenni. Természetesen későbbi módosításra lehetőség van.

A sikeres belépés után az adminisztrátor első feladata a beléptető rendszer használata előtt, hogy felhasználói csoportokat hozzon létre. A felhasználói csoportok használatának nagy előnye, hogy nem szükséges minden egyes felhasználónál megadni a jogosultságokat, hanem felhasználói csoportokban kerülnek meghatározásra, később csak ezekhez kell hozzárendelni a felhasználókat. A létrehozott csoporthoz hozzá kell adni az egyes átjárókat.

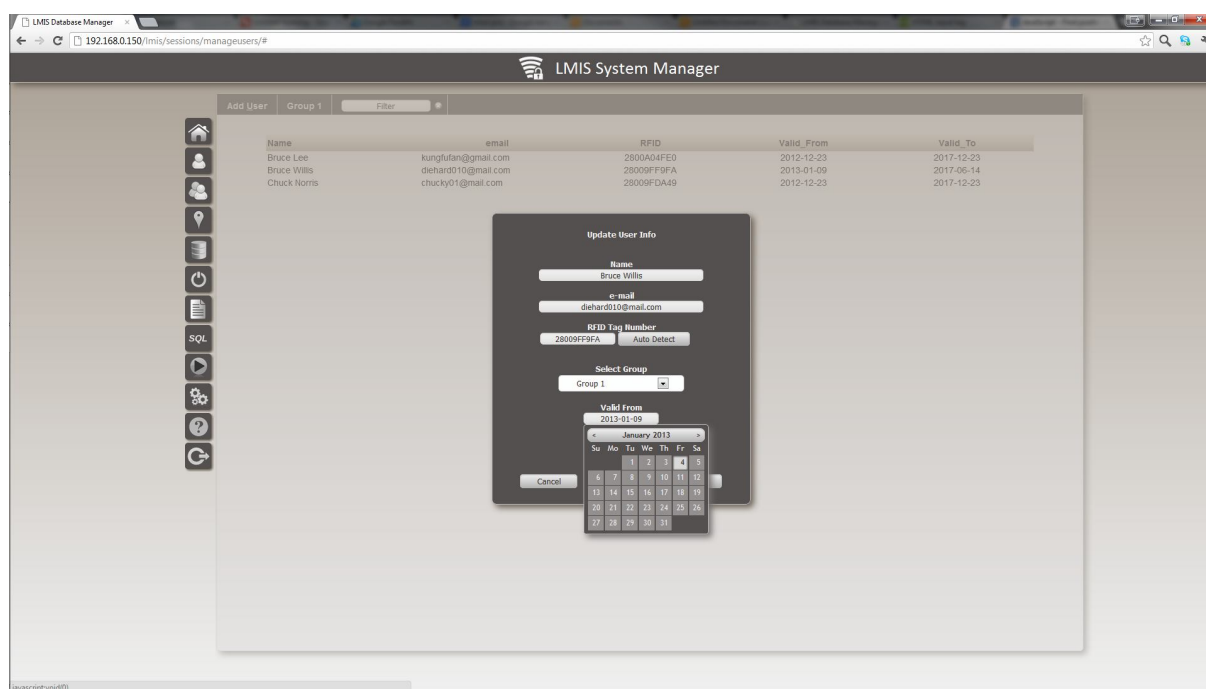
Az átjáró hozzáadása menüre kattintva a felugró ablakban csoport specifikusan kell meghatározni mely napokon mely idő intervallumban, kapnak jogosultságot a használatához. A csoporthoz hozzáadott átjárók, a hozzájuk tartozó adatokkal táblázatos formában jelenik meg.



28. ábra Csoport hozzáadása- adatok módosítása

A táblázatban megjelenő sorokra kattintva felugró ablakban módosíthatók az átjárók adatai. A könnyebb kezelhetőség érdekében lehetőség van a táblázat adatainak rendezésére, a táblázat oszlopainak fejlécére kattintva, növekvő illetve csökkenő sorrendben. Továbbá az átjárók egyszerűbb keresése a „Filter” feliratú ablakba kattintva, a begépelte szórészlet alapján dinamikusan szűri ki a nem egyező táblázat sorait.

A csoport vagy csoportok létrehozása után felhasználókat kell hozzáadni a rendszerhez. Az új felhasználó hozzáadása menüpontban az új felhasználó gombra kattintva vagy a Shift+U gomb kombinációval megjelenik az új felhasználó adatlapja. Ha már kiválasztottunk egy csoportot akkor automatikusan ahhoz rendeli hozzá de a csoportok legördülő menüben más csoportot is választhatunk.



29. ábra Felhasználó hozzáadása- adatok módosítása

Az adatlapon meg kell adni a felhasználó nevét, email címét(egyező nevek esetén egyedi azonosítóként használható) RFID azonosítójának számát (ezt manuálisan vagy az Auto Detect gombra kattintva a rendszer automatikusan beolvassa az asztali olvasóra helyezett azonosítót, ha van) valamint érvényesség intervallumát. A mentés után szintén egy táblázat jelenik meg a különböző csoportokban. A sorokra kattintva itt is lehetőség van módosításra, a felhasználó másik csoportba helyezhető illetve módosítható adatai. Ebben a menüpontban is lehetőség van a táblázat oszlopainak fejlécére kattintva a tetszőleges rendezéshez, illetve a „Filter” ablakba gépelve a felhasználók neve szerinti szűrésre.

A beléptető rendszer alapvető működéséhez mindössze ezekre az adminisztrációs feladatok elvégzésére van szükség.

A felhasználói felület további lehetőségeit tekintve beépítésre került a naplózott adatok megjelenítése, szerkesztése(törlés) illetve az adatok közötti keresés. A „Log” menüre kattintva megjelenik a „Live View” oldal, ahol táblázatos formában másodperces frissítéssel látható az átjárókon áthaladó felhasználók mozgása. Lehetőség van keresni a naplózott adatok között, keresési feltételek, szűrők megadásával.

Továbbá beépítésre került a rendszer használatával kapcsolatos információk megjelenítése diagrammok formájában,a naplózott adatokból nyert információk alapján.

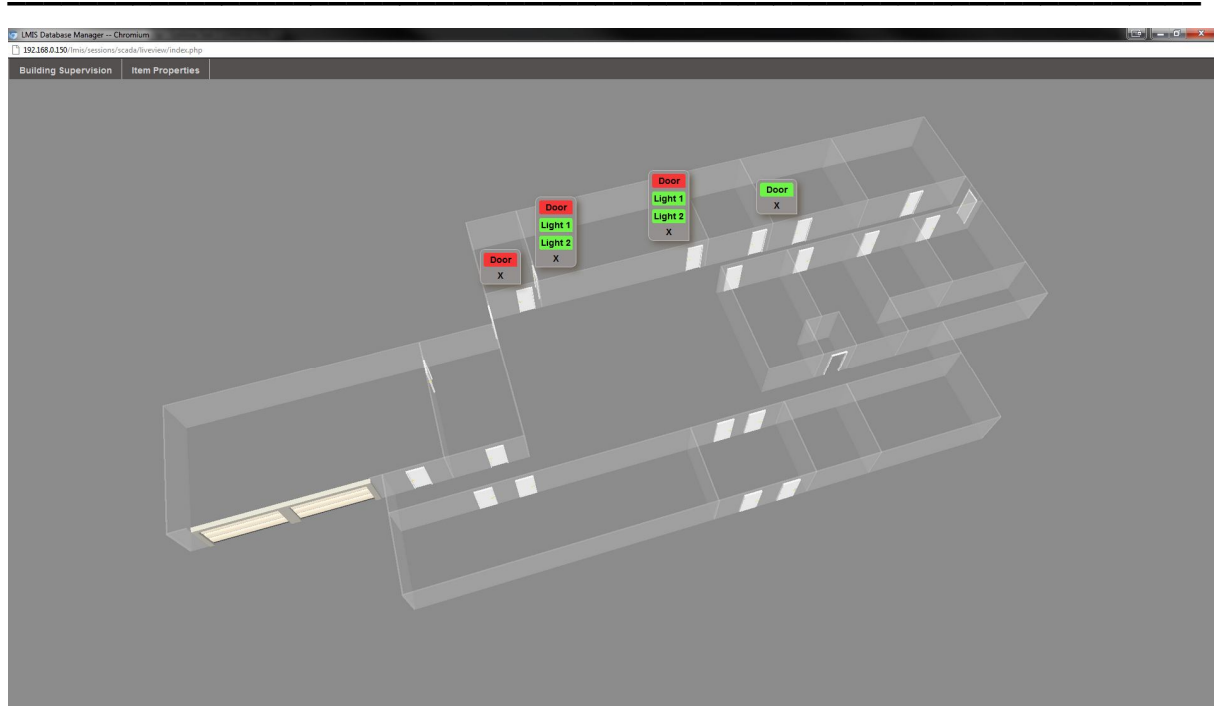


30. ábra Grafikonok

A grafikus felületben helyet kapott továbbá az épületautomatizálási feladatok meghatározásához szükséges felület, illetve ki/bemeneti műveletek felügyelete is. Itt megadhatók a rendszer automatikus műveletei, azaz az egyes hálózati elemek egymás közti műveletei (pl Hely02 bemenet01 invertál → Hely01 kimenet02 invertál). A rendszerben lehetőség van a szerver oldalról is beavatkozni. Itt azonnali vagy időpontra megadott művelet tárolható el. Az eltárolt műveleteket a rendszer automatikusan hajtja végre. Biztonsági szempontok miatt a beléptető rendszer vezérlő moduljainak az átjárót vezérlő kimenete az egyes modulokban le lettek tiltva ezen funkcióról.

A rendszergazdai illetve karbantartói eszköznek tekinthető SQL menüpontban megjelenő ablakban SQL lekérdezésekkel használható az adatbázis.

A felhasználó felület talán leghasznosabb kiegészítő funkciója a folyamat megjelenítő felület. Itt a rendszer telepítésének helyszínét, alaprajzát feltöltve lehetőség van elhelyezni az egyes átjárókhoz tartozó vezérlők helyét, és megadni a ki/bemenetek nevét vagy ahhoz kapcsolódó funkciókat. A kialakítást követően a megjelenítő menüpontban valós időben láthatóak a rendszerben használt eszközök állapotai. Ez hasznos lehet biztonsági szolgálat vagy porta tájékoztatására, valamint önálló épületautomatizálás is megjeleníthető.



31. ábra Épület felügyeleti megjelenítő felület

A folyamat megjelenítő felület előkészítésekor az egyes helyekhez tartozó ablakok az alaprajzon tetszőleges helyzetbe pozícionálhatók. Mentéskor a minden ablak tulajdonságai (név, ki/bemenetek, pozíció stb.) egy XML fájlba kerülnek eltárolásra. A valós idejű nézetben a mentett beállításoknak megfelelően töltődik be az oldal. A ki/bemenetek állapotát az adatbázisból kérdezi le, majd frissíti másodpercenként.

A felhasználói felülethez tartozik egy súgó mely felhasználói felület, illetve a rendszer hasznáival kapcsolatos információkat tartalmaz.

A felülethez tartozik még néhány további menüpont is a rendszer telepítéséhez és üzembe helyezésével kapcsolatban. A beállítások menüpont kizárólag rendszergazda jogosultsággal érhető el. Itt adhatóak hozzá felhasználók a felhasználói felülethez különböző jogosultságokkal. (adminisztrátor,). Szintén a beállítások menüpontban érhetőek el a rendszer telepítésekor és módosításakor szükséges hálózati beállítások és végezhetők el a szükséges eljárások.

A szintén csak rendszergazdai jogosultsággal elérhető menüpont az adatbázissal végezhető műveletek. A rendszer által használt adatbázis kialakítás (táblázatok neve, felépítése, kapcsolatok) egyszerű létrehozása az adatbázis nevének megadásával és a létrehozás gombra kattintva elvégezhető. Hasonlóan, könnyen létrehozható az adatbázis biztonsági mentése, valamint biztonsági mentés visszaállítható.

10. Beléptető rendszer működésének bemutatása

10.1 Titkosított kommunikáció

A vezeték nélküli hálózatok biztonsági szempontból igen sebezhetőek, mivel bárki hozzáférhet az adatokhoz, így a titkosítás meglehetősen fontos. Az IQRF protokoll sajnos nem tartalmazza a titkosítást így arról nekem kellett gondoskodni.

A számos titkosítási eljárás közül a 64 bites XTEA algoritmust választottam, mert egyszerűsége és gyorsasága mellett nehezen feltörhető. A titkosítás csak az adatok visszaolvasása ellen nyújt védelmet, viszont a rádiós rendszereknél ismert újraküldéses támadás ellen nem. Az újra küldéses támadás lényege, hogy az „elkapott” adat csomagot újraküldve a hálózat úgy érzékeli, mint ha az a hálózat valamely elemétől érkezne.

Ezt megakadályozva a titkosító algoritmus egy kvázi véletlenszerű szám és a csomagazonosító segítségével képzett maszkkal az XTEA kódolás előtt a csomag tartalmát maszkolja így az adott csomag újraküldésekor, a tartalom változása miatt a továbbiakban érvénytelen lesz és a hálózat ezeket eldobja.

	0.	08	0D	71	28	00	9F	DA	49
1.	BF	D1	B9	29	81	E1	1C	44	
2.	93	5D	61	42	79	07	E0	54	
3.	0F	03	35	43	BD	36	11	A1	
4.	DC	C1	98	F4	68	3D	BF	3A	
5.	54	1F	15	F2	D6	2C	09	83	
6.	B0	E2	F5	B5	98	D4	9D	94	
7.	48	C8	76	01	49	ED	A2	96	
8.	0C	04	95	85	FD	D8	02	3D	
9.	BE	6A	DF	8F	DE	6B	1A	CB	
10.	2F	B8	D7	4B	BD	36	11	A1	

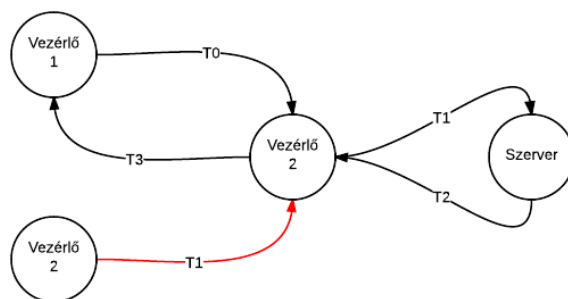
A titkosítás eredményességét a fent látható sorok példázzák. A 0. sorban látható az eredeti adat csomag hexadecimális alakja. A következő 10 sorban ugyan ez a csomag került titkosításra. Jól látható, hogy a titkosítani kívánt adat és a titkosított adat közt nagy az eltérés akár csak az egymást követő csomagok között.

10.2 Csomagok ütközése

Az IQRF hálózatban minden eszköz programja tartalmaz közös program részeket. Minden eszköz programjának legelején megvizsgálja, hogy rendelkezik-e hálózati azonosítóval, ha nem akkor várakozik a párosításra. Abban az esetben ha már párosítva van a hálózathoz elvégzik a modul specifikus inicializálásokat.

Az eszközökben szintén közös a titkosítási eljárás. A titkosítás az IQRF hálózaton belül van értelmezve. Ez azt jelenti, hogy az USB-átjáróhoz már a dekódolt adat jut el.

Az IQRF protokoll nem nyújt megoldást a csomagvesztés megakadályozására, így arról nekem kellett gondoskodni. Csomagvesztés akkor történhet mikor a hálózatban közel azonos időpontban kezdeményez kommunikációt kettő vagy több eszköz. Mivel routoláskor a modulok az időosztásos eljárás miatt várakoznak a kommunikáció végéig és ekkor más modultól is érkezik továbbítandó csomag, azok nem kerülnek továbbításra. Ez a probléma akkor léphet fel mikor a vezérlők kezdeményezik a kommunikációt. (Az olvasók közel helyezkednek el a vezérlőkhöz, így ott ez nem okoz problémát.)

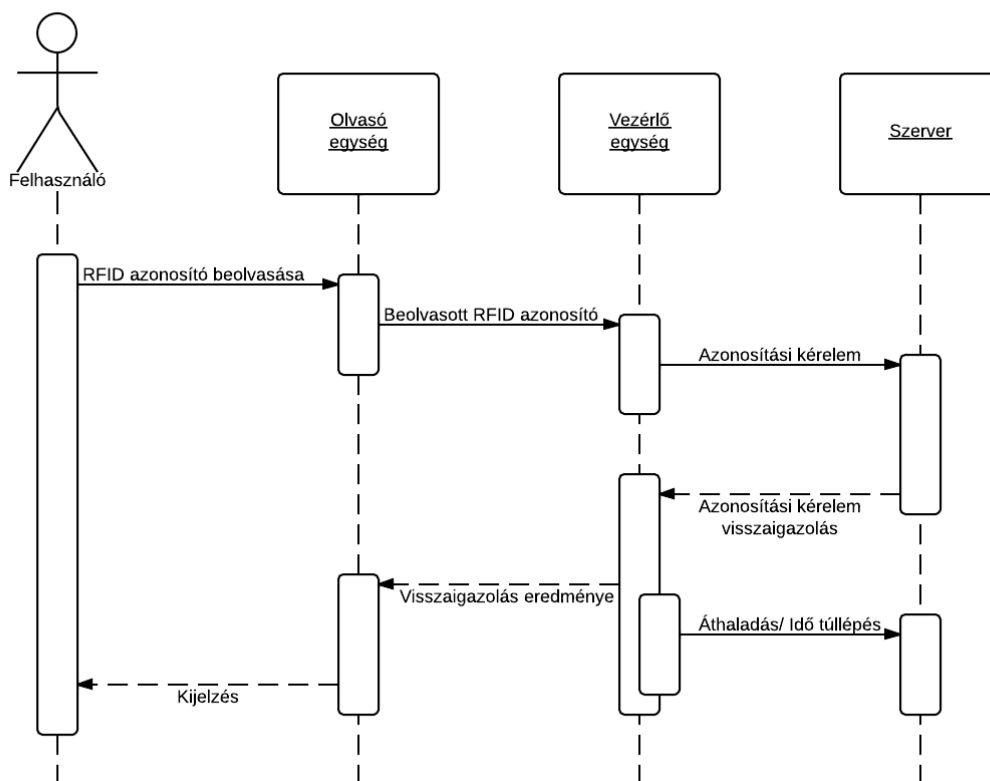


32. ábra Csomagok „ütközése”

A vezérlők által a szerver felé kezdeményezett kommunikáció, a beléptetés folyamatában minden esetben válaszüzenet követ. Azt a megoldást választottam, hogy a vezérlők küldéskor egy adott időréssel várakoznak a válaszüzenet érkezésére, és ha ebben az időrészben nem érkezik válasz, akkor az üzenetet újra küldi. Ezt az időrészt változtatásával az első küldés után még háromszor próbálkozik, az előzetek tesztek során ez elégségesnek bizonyult. Az újbóli ütközések elkerülése érdekében újraküldéskor a modulok gyártási számán alapuló kvázi véletlenszerű időrést használ.

10.2.1. Beléptetés folyamata

A beléptetés folyamata a felhasználó RFID azonosítójának beolvasásával kezdődik. Az azonosítót az olvasó egység elé tartva az olvasó modul beolvassa az azonosító sorszámot, és titkosítva küldi a vezérlő egységnek. Ekkor a vezérlő egy kérelem üzenetet küld a szerver felé. A szerver oldalon található USB-Gateway egység a szervernek átadja csomagot. A szerver SQL adatbázisból keresi ki a felhasználó jogosultságait az adott helynél majd válaszüzenet küldését kezdeményezi a kérést küldő vezérlőnek.

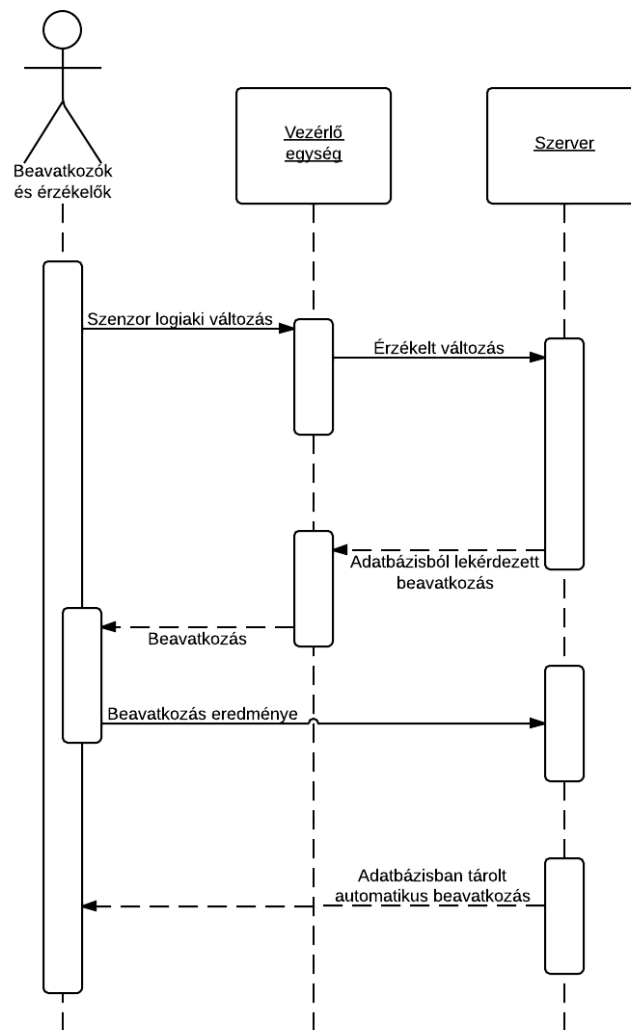


33. ábra Beléptetés folyamata

Sikeres beléptetés esetén a beléptetést végző elektro-mechanikus eszköz vezérlő kimenetére vezérlő jelet ad. Sikeres valamint sikertelen beléptetés esetén is az olvasó modulnak küldött üzenettel, az állapotjelző LED-en tájékoztatja a felhasználót jogosultság ellenőrzés eredményéről. Engedélyezett használat esetén az áthaladás érzékelő jelének megfelelően a vezérlő elveszi a vezérlő jelet, vagy ha nem halad át a felhasználó az átjárón idő túllépéssel veszi el.

10.2.2.Épületautomatizálás és épület felügyelet

Az épületautomatizálási funkció a már említett vezérlő egységek ki-és bemeneteit használva válik elérhetővé. A logikai ki-és bemenetek állapotát az adatbázisban meghatározott feltételeknek megfelelően a rendszer automatikusan végrehajtja és ezek állapotát, valamint a végrehajtás eredményét az adatbázisban frissíti.



34. ábra Automatikus beavatkozások folyamata

A beavatkozások kezdeményezése lehetnek egy azon, vagy más vezérlőktől származó állapot változások vagy a kezelő felületen meghatározott adatbázisban tárolt, időpontra vonatkozó akciók is. A felhasználói felületen keresztül lehetőség van a vezérlők ki-és bemeneteinek aktuális állapotának megjelenítésére is.

11. Tesztelés

A beléptető rendszer kiépítése és tesztelése 2013 elején kezdődött. A rendszer négy ajtóhoz lett telepítve, ez által még kis rendszerként üzemel. A tesztelés elsődleges szempontja a rendszer megbízható működésének vizsgálata. A működés vizsgálata a felhasználói felületen történő rendszer beállításokra, adatbázis feltöltésére, illetve a beléptetésekre és az épületautomatizálási funkcióra terjedt ki. A felhasználói felület használata az előzetes teszteknek megfelelően minden funkciója hibamentesen működött. Az egyetlen problémát az eltérő operációs rendszereken és böngészőkben való megjelenítés eltérése okozta. Az adatbázis feltöltése (beállítások, felhasználói adatok, automatikus beavatkozások) után a beléptetések vizsgálata következett. A beléptetések viszonylag nagy forgalom mellett is hibamentesen történtek. Az épületautomatizálási funkciók vizsgálatakor az automatikus és felhasználó felületen beállított tevékenységek is vizsgálva lettek. Az automatikus beavatkozáshoz kapcsolók illetve teremvilágítás lett kialakítva. Az adatbázisban tárolt beavatkozásokat a rendszer minden esetben végre hajtja.

A tesztelés jelenleg is folyamatban van, a tesztek eredményei még nem véglegesek. A rendszer véglegesítése a folyamatos teszt eredményeknek megfelelően kerül kialakításra.

12. Irodalomjegyzék

- [1] Filkorn József: Beléptető rendszerek c. előadás, 2009
- [2] Bunyitai Ákos: A beléptető rendszerek helye és szerepe a vagyonvédelemben, 2011
- [3] Petyus Dániel: RFID technológia, 2007
- [4] Ballagi Áron: Zigbee: vezeték nélküli komplex szenzorhálózatok gyorsan, olcsón, hatékonyan (Miskolci Egyetem, Automatizálási Tanszék)
- [5] Kuchta, R. : Smart Platform for Wireless Communication - Case Study
Networking, 2008. ICN 2008. Seventh International Conference, Brno Univ. of Technol., Brno, 13-18 April 2008
- [6] Sulc, V. : IQMESH Implementation in IQRF Wireless Communication Platform, Advances in Mesh Networks, 2009. MESH 2009. Second International Conference on, MICRORISC s.r.o., Jicin, Czech Republic, 18-23 June 2009
- [7] Yifeng Yang: Microchip MiWi™ PRO Wireless Networking Protocol
Microchip Technology Inc., 2011
- [8] www.iqrf.org
- [9] www.iqmesh.org
- [10] <http://uc-free.hu/?q=node/13>
- [11] <http://searchmobilecomputing.techtarget.com/definition/Wi-Fi>
- [12] <http://www.rfidjournal.com>