10.17625/NKE.2022.036

Doktori (PhD) értekezés

Vránics Dávid Ferenc

2022

NEMZETI KÖZSZOLGÁLATI EGYETEM
HADTUDOMÁNYI ÉS HONVÉDTISZTKÉPZŐ KAR
KATONAI MŰSZAKI DOKTORI ISKOLA

VRÁNICS DÁVID FERENC

A felhő alapú rendszerekből vezérelt pilóta nélküli légijármű-rendszerek biztonsági kérdései

Doktori (PhD) értekezés

Témavezető:

Dr. Palik Mátyás PhD

2022

TARTALOMJEGYZÉK

BEVEZETÉS

A témaválasztás indoklása, aktualitása

Napjainkban a modern telekommunikáció egyre növekvő teljesítményigényének kielégítésére a felhő alapú szolgáltatásokra nagy hangsúly helyeződik. Internetes tárhelyeken (felhőben) tároljuk a személyes üzeneteinket, adatainkat, fájljainkat, felhő alapú szolgáltatások segítségével keresünk, vagy éppen vásárolunk az interneten, és ezen keresztül tartjuk a kapcsolatot ismerőseinkkel is. Ma már egyes vállalatok a teljes üzletvitelüket felhőben végzik, ezért annak biztonsága alapvető szempont kell, hogy legyen.

A technológia fejlődésével és az eszközök fizikai méretének és előállítási költségének csökkenésével a távolról irányított, idővel teljesen autonóm pilóta nélküli légijármű-rendszerek bárki számára elérhetővé váltak, és elterjedten használják őket fénykép- és videófelvételek készítésére, csomagok házhoz juttatására, nem is beszélve a katonai/rendvédelmi felhasználásukról. A drónok rohamos elterjedésével hamar egyértelművé vált, hogy szükséges valamiféle szabályozás a használatukra. Erre, kifejezetten a bonyolultabb, veszélyesebb műveletek során – a jogi megoldások mellett – egy technológiai megoldást nyújthat, ha irányításukat és felügyeletüket központi szolgáltatásként nyújtják, ezzel biztosítható az ellenőrzésük, és a légiközlekedési balesetek elkerülése.

Az 1990-es évek óta egyre gyorsuló ütemben terjedt el mind a felhőszolgáltatások, mind a pilóta nélküli légijárművek használata. A 2010-es évekre a média hatására a köztudatban is elterjedt e két különálló fogalom, napjainkra pedig már sor került a közös alkalmazásukra is – pilóta nélküli légijárműveket irányító felhő alapú rendszerek formájában.

Elsőként a mezőgazdaság és térinformatika alkalmazási területén látott napvilágot néhány ilyen rendszer. Miután ezek a területek ígéretes eredményeket mutattak, további kutatás-fejlesztési és innovációs projektek indultak be. Napjainkban, Kínában a pilóta nélküli légijárművek állami felügyeletét is felhő alapú technológiával oldják meg [1] [2]. A kutatásaim szempontjából fontos és érdekes megemlíteni a Dronemap Planner alkalmazást, ami drónok felhő alapú távirányítását teszi lehetővé, és kutatásaimmal párhuzamosan, de attól függetlenül került implementálásra [3]. Ez a rendszer felhő alapon szolgál ki egy webes alkalmazást, amin keresztül drónokat távolról, egy felhasználó.

A tudományos probléma megfogalmazása

Tisztázatlan kérdés azonban ezeknek a rendszereknek a terhelhetősége, tesztelhetősége, és hogy az elterjedt protokollok közül melyik alkalmas arra, hogy biztosítsa a repülőeszközök megbízható távirányítását és nyomkövetését internet protokoll (IP[1]) alapú hálózatokon keresztül. Érdemes megvizsgálni ezek alkalmazásának életszerűségét költségvetési szempontból is. Hol van az a pont, amikortól jobban megéri felhő szolgáltatást bérelni fizikai számítógépek fenntartása helyett – avagy fordítva? A felhő rendszerek rugalmas erőforrás kiosztási képességei korábban nem látott gazdálkodási lehetőségeket adnak az üzemeltetés és felhasználás számára, melyek jelentős költségvetés- és megbízhatóságbeli előnyöket hordoznak magukban: az erőforrások automatikus skálázása és önjavító képessége pilóta nélküli légijármű-rendszerek esetén kivételesen hasznos tulajdonság lehet.

A felhő alapú számítástechnika képességei és a negyedik (több helyen már ötödik) generációs híradó-informatikai hálózatok nagy lefedettsége és átviteli sebessége lehetővé teszi akár a kiszolgáló oldali, valós idejű képelemzést, és ez alapján akár a repülési útvonal azonnali módosítását ütközési veszély fennállása esetén, vagy egyéb, a repülési feladat elvégzésének biztonságát veszélyeztető dinamikus kockázati tényező feldolgozását valós időben. Gondolhatunk példaként a veszélyes időjárási jelenségek, vagy az eseti kutatómentő repülések kikerülésére. A veszélyes helyzetek elkerülésén túl a már bajba került pilóta nélküli légijárművek adatainak elemzése rávilágíthat a rendszerek fizikai korlátjaira is.

Továbbá felmerül kérdésként, hogy egy ilyen rendszer felhasználása során az általa nyújtott információk (például a repülőeszközök helyzete) érdekesek lehetnek-e más légi- vagy földi közlekedési rendszer számára, ezért érdemes megvizsgálni, hogy azok milyen interfészen át kapcsolódhatnak egymáshoz biztonságosan. A kommunikációs csatornának és a kommunikáló feleknek biztosítania kell az adatok sértetlenségét, rendelkezésre állását és hitelességét, esetenként bizalmasságát is, miközben figyelembe veszik a rádiós frekvenciakiosztásra és sávszélességre, a választott spektrum megengedett telítettségre vonatkozó szabályozásokat.

Különbséget kell tenni felhasználást illetően a védelmi, kereskedelmi és hobbi célú pilóta nélküli légijármű-rendszerek (UAS[2]) képességei és az elvárt biztonsági szintek között, ennek megfelelően az őket kiszolgáló felhő alapú rendszerrel szemben támasztott követelmé-

[1] Internet Protocol
[2] Unmanned Aircraft System

nyeket is nagyon specifikusan kell kialakítani. Ehhez útmutatásként rendelkezésre állnak a különböző katonai, állami és polgári szervezetek specifikációi, melyek meghatározzák a szükséges peremfeltételeket jogi és technológiai szempontból egyaránt.

A rendszeren belül kezelt adatokat sorra véve arra a következtetésre juthatunk, hogy egyes adatok kritikusabbak, hiszen a légijármű irányításáért felelnek, vagy az európai irányelvek által meghatározott személyes adatokat tartalmaznak. Más adatok viszont közérdekűek, például a polgári légijármű pozíciója és azonosítója, vagy egyéb tulajdonságai melyek nyílt csatornán is szórhatók a fedélzeti ütközéselkerülés megvalósításának érdekében. Szükséges ezért az adatok és alrendszerek feladatköreinek osztályozása adatkezelés- és hozzáférés szempontjából. Így, mint az UAS földi alrendszere részének, a távpilótának azonosíthatóságát is biztosítani kell, hiszen a légijármű-rendszer kritikus eleméhez, az irányításhoz fér hozzá, akár távolról, az interneten keresztül. Ez nem csak a számonkérhetőség szempontjából, de a szándékos eltérítés elleni védekezés szempontjából is fontos.

Az utóbbi évek történései rávilágítottak arra, hogy az ellátási lánc biztonsága egy eddig alábecsült terület az informatikai rendszerek esetén – mind a hardveres, mind a szoftveres beszállítók szabotálhatják a rendszer biztonságát kiskapuk elhelyezésével a termékeikben, nem is beszélve a számtalan, napvilágot látott lehallgatási botrányról. Ezen valamelyest segíthet a nyílt forrású szoftverek és hardverek alkalmazása, így kutatásaim során törekedtem ilyen technológiai eszközkészlet kialakítására – ám önmagában ez sem küszöböli ki a problémát, hiszen egyes esetekben nem csak szoftverre és hardverre, hanem külső adatforrások megbízhatóságára is épít egy ilyen rendszer.

Repülési kísérletek során szerzett kézzel fogható eredményeken túl (pl. valóban repülő drón) szükség van olyan tesztesetek vizsgálatára is, amelyeket nem biztonságos, vagy nem életszerű terepen kivitelezni (pl. több száz drónnal végzett terheléses teszt, vagy hibás működés tesztelése). Ezek elvégzésére szükséges szimulált szoftveres környezet kialakítása, amin belül „büntetlenül," kár okozása nélkül vizsgálhatjuk etikusan a különböző szélsőséges eseteket, melyeket esetlegesen a jogi környezet sem engedélyezne valós körülmények között.

Kutatási célkitűzések

Célul tűztem ki, hogy

- A kutatás során **feltárom** és **bemutatom** a pilóta nélküli légijárművek (UAV[3]) és a felhő alapú rendszerek jelenlegi lehetőségeit;
- **Elemezem** az elérhető szabványokat és ajánlásokat, valamint jogszabályokat;
- Biztonsági szempontból **megvizsgálom** a pilóta nélküli légijárművek irányítására elterjedten használt protokollokat;
- **Feltárom** a két terület összekapcsolásának lehetőségeit;
- **Esettanulmányokat folytatok** és összeállítok egy felhő alapú UAS-t;
- Repülési és szimulációs **teszteket végzek**;
- **Átfogó javaslatokat teszek** a felhő alapú UAS-k tesztelésére és tervezésére vonatkozóan.

Kutatási hipotézisek megfogalmazása

- A felhő alapú rendszerekből irányított pilóta nélküli légijármű-rendszerek tesztelése eredményesen kivitelezhető két irányból: a járművek, illetve az irányítás tesztrendszerrel való helyettesítésével.
- A felhő alapú kiszolgálás elősegíti a drónok fizikai biztonsági szempontból megfelelő távirányítását és felügyeletét.
- A felhő alapú kiszolgálás elősegíti az UAS-k adminisztratív biztonsági szempontból megfelelő működtetetését, a folyamatok szervezését.
- A felhő alapú irányítás és felügyelet elősegíti a személyi biztonsági szempontból megfelelő működést, és a résztvevők egyértelmű azonosítását UAS-k esetén.
- A felhő alapú irányítás elősegíti az pilóta nélküli légijármű-rendszerek elektronikus biztonsági szempontból megfelelő működtetetését.

Kutatási módszerek

A kutatás során alkalmazásra kerülő módszerek, valamint a vizsgálati munka módszertani megközelítései a következők:

- Az elméleti tudásanyag megfelelő megalapozása a releváns tudományos oktatási anyagok és szakirodalom feldolgozásával.

[3] Unmanned Aerial Vehicle

- Gyakorlati kutatás és fejlesztés egy kísérleti rendszer és tesztkörnyezet kialakítása kapcsán.
- Informatikai laborkísérletek és szimulációk elvégzése az összeintegrált rendszeren.
- Saját primer kutatási eredmények, mérések értékelése.
- Kollaboráció hazai és külföldi szakértőkkel, oktatókkal, szakemberekkel.
- Egyetemi tudományos pályázaton történő részvétel.
- Esettanulmányok folytatása egyes nyílt rendszerek biztonsági hiányosságainak felmérésére.
- Különböző releváns technológiák közti párhuzamok felfedése és analízise, összehasonlító kritikai elemzése, a vizsgált problémára vonatkoztató következtetések levezetése.

Szakirodalmi áttekintés

Pilóta nélküli légijármű-rendszerekre vonatkozó hazai szakirodalom

A feltárást érdemes a legátfogóbb, legterjedelmesebb könyvvel kezdeni, ami a *Pilóta nélküli repülés profiknak és amatőröknek* címet viselő, Békési Bertold, Bottyán Zsolt, Dunai Pál, Halászné Tóth Alexandra, Makkay Imre, Palik Mátyás, Restás Ágoston és Wührl Tibor közreműködésével jött létre [4]. Ez a népszerű kiadvány több, mint 300 oldalon foglalja össze a területhez kapcsolódó alapismereteket.

A polgári és védelmi felhasználáshoz átfogó bevezetést nyújtó könyv után érdemes az áttekintést kifejezetten a katonai aspektusokkal foglalkozó kiadvány, a Repüléstudományi Közlemények cikkeivel folytatni.

Ványa László, *Hogyan védekezzünk a drónok ellen?* című közleménye [5] az amerikai UAV-k sikereinek összefoglalása után a 2011. június 17-én napvilágot látott, híressé vált iraki dokumentumot dolgozza fel, ami 22 ajánlást fogalmaz meg a drónok elleni sikeres védekezés érdekében. Ez a dokumentum az UAV-kkal műveletet végző oldalnak is hasznos információkat tartalmaz, hiszen így fel tud készülni, lehetőség szerint ki tudja kerülni a drónok elleni védekezésre irányuló törekvéseket.

A szerző másik közleménye *Kérdések és válaszok a szupertitkos RQ-170 iráni kézre kerüléséről* címmel [6] az eltérített amerikai UAV nagy sajtóvihart kavart esetét elemzi ki az akkoriban rendelkezésre álló információk alapján. Bár mint később kiderült, a drónt egy

komplex, a műholdas kommunikációt a földi irányítóközponttal való kommunikációt és a globális helymeghatározó rendszer (GPS[4]) működését zavaró elektronikai tevékenységgel térítették el. A közleményben felsorakoztatott, szakmailag megalapozott feltevések bepillantást nyújtanak ezeknek a rendszereknek a zavarási lehetőségeibe.

A lehetséges ellentevékenységen kívül részletesen bemutatja magát a légijármű-rendszert, és a zavarásra feltételezetten használt orosz gyártmányú szárazföldi állomás képességeit, paramétereit is.

Ványa László és Kovács László *Pilóta nélküli repülőgépek a terrorizmus elleni harcban* című publikációja [7] az UAV-k katonai és katasztrófavédelmi felhasználását tárgyalja. Az amerikai és izraeli gyártmányú eszközök jellemzése után érdekes példát hoz egy, terroristák által alkalmazott UAV esetére, ami napjainkban is releváns tapasztalatokkal bír, hiszen az utóbbi évek során többször előfordult, hogy konvencionális haderők ellen drónokra szerelt improvizált robbanóeszközöket vetettek be.

A cikk számomra legfontosabb része azonban ez után következik, hiszen a magyarországi UAV fejlesztéseket mutatja be. Említi a Szojka és a H-AEROBOT cégek fejlesztéseit, amelyeknek erős magyar vonatkozása is volt. A legfontosabb típusok a Szojka-III, ami kamerával, sugár vagy rádió (illetve rádiólokációs) felderítő és zavaró berendezéssel, nagy érzékenységű vizuális, vagy infravörös tartományú vizuális felderítő eszközökkel szerelhető fel; valamint a H-AEROBOT által kifejlesztett légijárművek közül legnagyobb hasznosteher-kapacitású Sas, illetve a valamivel kisebb Túzok, és a kisméretű Delta.

A Szendrőn rendszerbe állított tűzfelderítő pilóta nélküli légijármű-rendszerek bemutatásánál a szerzők külön kiemelik a kifejlesztésben részt vett (akkori) ZMNE hallgatók tevékenységét és az elért eredményeket. A közlemény felsorolja a 2006-os pilóta nélküli repülőgép beszerzési tender kritériumait, és bemutatja a győztes lengyel SOFAR mini UAV-t.

Papp István *Pilóta nélküli légijármű típusok jellemzése* című közleményében [8] a legelterjedtebb, legismertebb típusok összehasonlító vizsgálatáról olvashatunk.

Palik Mátyás *Need for Unmanned Aircraft System* című angol nyelvű közleményéből [9] három, a pilóta nélküli légijárművek katonai alkalmazásával kapcsolatos fontos jellemzőt emelnék ki; „dull, dirty, dangerous," azaz „fárasztó, piszkos, veszélyes" műveletekben alkalmazzák őket. A „fárasztó" jelentése, hogy akár több napos, a folyamatos koncentráció miatt fizikailag kimerítő lehet a művelet. Ezt a faktort Dunai Pál *Energiafelhasználás, a*

[4] Global Positioning System

keringési és légzőrendszer terhelési paramétereinek elemző vizsgálata UAV kezelőszemélyzet munkavégzése során című publikációjában [10] részleteiben mutatja be.

A „piszkos" jelentése, hogy fertőzött, mérgező, sugárfertőzött, az emberi szervezetre káros környezetben történhet a művelet.

A „veszélyes" jelentése, hogy a küldetés túl kockázatos lenne ahhoz, hogy akár a felderítési adatok hiányosságai okozta bizonytalanság miatt, akár az esetlegesen földre kényszerített és elfogott pilóta okozta politikai teher miatt hagyományos repülőgépekkel kivitelezhető legyen.

Ugyancsak Palik Mátyás *Pilóta nélküli légijármű rendszerek légi felderítésre történő alkalmazásának lehetőségei a légierő haderőnem repülőcsapatai katonai műveleteiben* című doktori disszertációjában [11] a katonai alkalmazás lehetőségeiről olvashatunk. Az értekezés elkülöníti a légi, földi és adatkapcsolati alrendszert.

A nemzetközi osztályozás és általánosan elvárt követelmények vázolása után bemutatja a minőségi képességeket; területlefedési képesség, mobilitás, túlélőképesség, kommunikációs képesség, megbízhatóság.

Fekete Csaba és Palik Mátyás *Introduction of the Hungarian Unmanned Aerial Vehicle operator's training course* [12] és *A hazai UAV kezelő személyzet képzésének tapasztalatai* [13] című publikációiból a hazai képzés módszertanáról tájékozódhatunk. Alapvetően két, különböző típusra történő képzési programról beszélhetünk. Az egyik a Meteor 3-MA típus, ami elsődlegesen a légvédelmi rakéta fegyvernem MISTRAL rendszereinek éleslövészetein szerepel célrepülőgépként. A másik a Skylark 1-LE típusú kis méretű, felderítő feladatokra alkalmazott repülő eszköz.

Palik Mátyás és Pongrácz Gábor *Communication issues of UAV integration into non segregated airspace* című publikációja [14] a pilóta nélküli légijárművekkel kapcsolatos kommunikációnak a légiközlekedés által korlátozás nélkül igénybe vehető (ellenőrzött, illetve nem ellenőrzött) légtérbe történő integrációjának lehetőségeit vizsgálja.

Vas Tímea és Palik Mátyás *UAV operation in aerodrome safety and ACS procedures* című publikációjában [15] az ellenőrzött légtérben történő UAV repülés eljárásbeli szabályozására tér ki. Javasolja, hogy az UAV irányító személyzet és a légiforgalmi irányítás közötti kapcsolatfelvételkor egyértelműen legyen tisztázva, hogy pilóta nélküli légijárműről van szó, majd a továbbiakban a pilóta által repült járművekhez hasonlóan történjen a kommunikáció.

A cikk az elektronikus biztonsági kérdésekre is kitér, a legfontosabb kockázati tényezőként az adatokba történő engedély nélküli és rosszindulatú beavatkozást, más földi állomás in-

terferenciáját és az UAV eszközzel való visszaélést nevezi meg. Fontosnak tartja a rendszer biztonsági kockázatelemzését és a kiberbiztonság megvalósítását. Szükségesnek ítéli a személyzet megfelelő felkészítését mind technikai, mind elméleti tudással.

Az eszköz részéről fontosnak ítéli meg, hogy képes legyen detektálni és megakadályozni az esetleges technikai problémák kialakulását és súlyosbodását. Végül kiemeli, hogy a legfontosabb a légiforgalmi irányítás és a távoli irányító személyzet közti kapcsolat kialakítása és fenntartása a repülés során.

Az említett két művet (az akkori) jogszabályi ismeretekkel jól kiegészíti a 2008-as *Pilóta nélküli repülés - légi közlekedés biztonság* című publikáció, [16] bár az elmúlt évek során sokat fejlődött a szabályozás jogi téren, az ebben felvetett problémák nagy része még mindig releváns lehet.

Bali Tamás *Ajánlások az UAV-k biztonságos légi és földi üzemeltetéséhez szükséges (repülési) szabályokra* című művében [17] 14 ajánlást fogalmaz meg az UAV-kkal kapcsolatos problémák feloldására, a jelenlegi is hosszas hatósági engedélyeztetési eljárástól az éjszakai repülés kérdéséig.

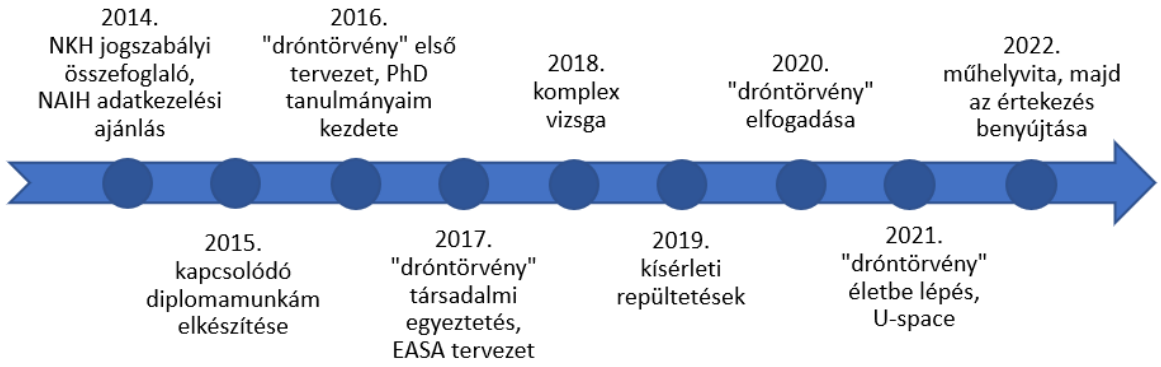
Ha az UAV-k fedélzeti rendszereinek technikai részleteire vagyunk kíváncsiak, érdemes áttekinteni Turóczi Antal *Négyrotoros pilóta nélküli helikopter fedélzeti automatikus repülésszabályozó berendezései* című doktori értekezését [18]. A négyrotoros pilóta nélküli helikopterek általános áttekintése után a fedélzeti elektronikával ismerkedhetünk meg, majd a repülésszabályzó rendszerek tervezésébe kaphatunk betekintést. Kutatásaim szempontjából ezek mind biztonsági szempontból támadható pontok.

A Hadobács Katalin és társszerzői által írt, *A pilóta nélküli légijárművek meteorológiai támogató rendszerének kialakítása és alkalmazhatóságának bemutatása esettanulmányokon keresztül* című mű [19] egy, a pilóta nélküli repülés támogatására kialakított időjárási adatrögzítő és előrejelző rendszert mutat be. A pontos időjárási adat kiszolgálás nagyban segíti az időjárás viszontagságaira különösen érzékeny, kis és közepes méretű pilóta nélküli légijárművek irányító személyzetét, hogy megfelelően felkészüljenek az esetleges kihívásokra. Ez a rendszer a pilóta nélküli légijármű-rendszerek fizikai biztonságának, biztonságosságának egy alapköve lehet, akár felhő alapú rendszerbe ágyazva.

Ehhez a publikációhoz szorosan kapcsolódik a *Repülésmeteorológiai klíma adatbázis kialakítása az UAV-k komplex meteorológiai támogató rendszeréhez* című mű [20]. Bottyán Zsolt és társzerzői publikációjában részletesen megtalálhatjuk a meteorológiai adatbázis és annak támogató rendszerének technikai leírását, a fejlesztés eddigi eredményeit és a további fejlesztési lehetőségeket.

A „dróntörvény” és az európai uniós jogszabályok

Magyarországon sokáig nem vonatkozott részletes szabályozás a 150 kg maximális felszálló tömeg alatti pilóta nélküli légijárművekre. A drónok gyors elterjedésével szükségessé vált kifejezetten az UAV-kra vonatkozó jogszabályok kidolgozása, az értekezéshez és a kapcsolódó témájú, korábbi diplomamunkámhoz köthető kutatási tevékenységem során közvetlenül tapasztalhattam az aktuális szabályozás alakulását, ennek idővonala az 1. ábrán követhető.



1. ábra: Kutatásaim mérföldkövei és a jogszabályok alakulása.
(Szerkesztette a szerző.)

A jogszabályokról 2014-ben a Nemzeti Közlekedési Hatóság (Légügyi Hivatala, mint repülési szabályozásért hatályos szerv) weboldalán találhattunk egy összefoglaló dokumentumot [21]. Eszerint a következő jogszabályok voltak a figyelembe veendők:

- 1995. évi XCVII. törvény a légiközlekedésről;
- 4/1998. (I. 16.) Korm. rendelet a magyar légtér igénybevételéről;
- 14/2000. (XI. 14.) KöViM rendelet a Magyar Köztársaság légterében és repülőterein történő repülések végrehajtásának szabályairól;
- 26/2007. (III. 1.) GKM-HM-KvVM együttes rendelet a magyar légtér légiközlekedés céljára történő kijelöléséről;
- 399/2012. (XII. 20.) Korm. rendelet a légi távérzékelés engedélyezésének és a távérzékelési adatok használatának rendjéről.

Ugyancsak 2014-ben született egy ajánlás *A Nemzeti Adatvédelmi és Információszabadság Hatóság ajánlása a drónokkal megvalósított adatkezelésekről* címmel [22], ami az említett hatóság (röviden NAIH) weboldalán érhető el, de ez főleg csak a személyiségi jogi kérdéseket tárgyalta, a repülési szabályokat nem érintette. Javaslatokat tett állami, kereskedelmi és magáncélú felhasználóknak a személyes adatok, kifejezetten az UAV-kkal készített felvételek kezelésére, az esetleges félreértések és jogi következmények elkerülése végett.

Bár ez az ajánlás nem technikai részleteket tárgyal, jól mutatja, hogy akkoriban az UAV-k jogi szabályozását még mindig sok hiányosság vette körül.

A hiányosságok lefedésére, 2016 végére kidolgozásra került a várva várt, a köznyelvben csak „dróntörvényként" emlegetett jogszabály-módosítási tervezet első változata [23]. Ez 2017. elején nem csak közigazgatási, hanem társadalmi egyeztetésen is átesett, a véleményezés eredményeinek és javaslatainak feldolgozása és az esetleges módosítások után 2017. július 1-re volt várható a hatályba léptetése.

A tervezet kitért a pilóta nélküli légijárművek légiközlekedési tevékenységére kiterjedő kötelező felelősségbiztosítás kereteire, amellyel egy időben különböző kategóriákba is sorolta a repülő eszközöket maximális felszálló tömeg alapján. Kiegészítette a leszállóhely és repülőtér meghatározását egy új kategóriával, ami pilóta nélküli légijárművek fel- és leszállási tevékenységét hivatott kiszolgálni.

A Nemzeti Fejlesztési Minisztérium (NFM) a kapcsolódó rendeletben pontosan tisztázta a kapcsolódó fogalmakat, illetve a szabályozást a 0,25 és 150 kg közötti pilóta nélküli légijárművekre korlátozta. Részletezte az általános működtetés szabályait, illetve az említett maximális felszálló tömeg alapján meghatározott kategóriák specifikumait. Részletezte a légtér biztosításának folyamatát, a repülési tevékenységben közvetve, illetve közvetlenül résztvevő személyek feladatait, majd a nyilvántartás folyamatát. Kitért a légijármű engedélyezésére, és a vezetéséhez, illetve az oktatáshoz szükséges képesítések és engedélyek kérdésére.

A disszertációban lentebb ismertetett 2019. évi repültetéseim során ezen tervezetet vettem figyelembe és annak megfelelően jártam el.

A hosszas konzultáció után elkészült tervezet érvénybe léptetése azonban még mindig váratott magára. Az Európai Repülésbiztonsági Ügynökség (EASA[5]) az uniós szabályozás kialakításával foglalatoskodott, 2017. júliusában prezentálták a tervezetet, ami 2017. szeptember 15-ig volt véleményezhető. Az EASA hivatalos szakvéleménye 2018. februárjában került benyújtásra az Európai Bizottság számára, ami alapján a hivatalos döntés 2018. végére volt várható, míg a bevezetés 2019-re [24] [25].

Az esetleges ellentmondások és koncepcionális változások elkerülése végett ezért a hazai szabályzás továbbra sem került addig bevezetésre, csupán ajánlás maradt.

A hazai 1995. évi XCVII. légiközlekedésről szóló törvény köznyelvben csak „dróntörvényként" emlegetett, végső módosítási javaslata végül 2020. november 10-én került be-

[5] European Union Aviation Safety Agency

nyújtásra, majd elfogadása után 2021. február 10-től lépett érvénybe. Ez az európai szabályozásnak megfelelő, de annál helyenként szigorúbb megkötéseket is tartalmaz a különböző kategóriákra vonatkozóan: például 250 grammról 120 grammra korlátozza a játék kategóriába eső drónok maximális felszálló tömegét.

Az U-space elnevezésű, európai pilóta nélküli légiforgalmi menedzsment szabályozási kereteit a Bizottság (EU) 2021/664 végrehajtási rendelete [26] írja le, mely 2021. április 22-én került publikálásra. Az értekezés szempontjából a rendelet IV. fejezete a legrelevánsabb, melyben az elvárt repüléstámogató szolgáltatásokat és a feléjük támasztott követelményeket definiálja. Az ebben megnevezett szolgáltatások a következők:

- hálózatazonosító szolgáltatás;
- földrajzi helymeghatározási szolgáltatás;
- UAS-repülésengedélyezési szolgáltatás;
- forgalmi információs szolgáltatás;
- meteorológiai szolgáltatás;
- megfelelőség-ellenőrzési szolgáltatás.

Pilóta nélkül légijármű-rendszereket érintő külföldi szakirodalom

Az európai szabályozások közül érdemes kiemelni a Spitzbergák esetét. A norvég Környezetért Felelős Hivatal (Miljødirektoratet) tervezete kiterjesztené a Spitzbergák Környezetvédelmi Törvényt, mely módosítással betiltaná a drónok használatát a Spitzbergák területének nagy részén, hogy ezzel korlátozza az emberi behatást a védett területen. Kiemelten: *„Távolról irányított pilóta nélküli járművek (drónok stb.) tiltása. Tilos pilóta nélküli járművek (drónok) és más távirányított járművek használata a levegőben, szárazföldön és víz alatt. A drónok továbbra is használhatók kutatási és megfigyelési céllal, de ez bejelentéshez és a Spitzbergák Kormányzójának engedélyéhez kötött a védett területeken…*" [27].

A tervezett szigorítások gyakorlatilag megtiltják vagy engedélyhez és bejelentéshez kötik a drónhasználatot a Spitzbergák szárazföldi területeinek 67%-án, illetve a partmenti területek 88%-án, melynek várható bürokratikus terhe jelentős aggodalmat váltott ki a kutató társadalomban, hiszen napjainkban a legtöbb kutató kampány fontos részét képezik a fent említett drónok és egyéb eszközök.

Az Amerikai Védelmi Minisztérium (US DoD[6]) közzétette tervezetét [28] a katonai célú UAV-kkal kapcsolatos igényeire és céljaira. Többek között az Ázsiában tapasztaltakra

[6] United States Department of Defense

építve tervezik az UAV-k összhaderőnemi felhasználásának további fejlesztését, mind a széles körben alkalmazható képességekre, mind a költséghatékonyságra hivatkozva.

Joseph A. Marty *Vulnerability Analysis of the MAVLink Protocol for Command and Control of Unmanned Aircraft* című diplomamunkájában [29] az egyik legelterjedtebben használt UAV kommunikációs protokoll sebezhetőségét vizsgálta. Sikeresen mutat be lehetséges támadásokat, és az eredményeket értékeli biztonsági következmények, energiafelvételi következmények és hálózati késleltetés függvényében.

A *Strategic Concept of Employment for Unmanned Aircraft Systems in NATO* című kiadvány [30] egyik legfontosabb eleme, hogy leírja a pilóta nélküli légijárművek osztályozását tömeg és képességek alapján. Ezen túlmenően foglalkozik a kategóriák bevetési lehetőségeivel, a képességeik tükrében. A vezetés-irányítás, küldetés tervezés és vészhelyzeti tervezés leírása után foglalkozik a pilóta által vezetett rendszerekkel való integráció, interoperabilitás kérdésével is.

Az interneten át végzett, UAV-kat érintő műveletek kockázatelemzésének és biztonsági elemzésének módszertanát vizsgálta Azza Allouch, Anis Koubâa, Mohamed Khalgui és Tarek Abbes [31]. A veszélyforrások azonosítására, kockázatok kvalitatív elemzésére és kezelésére vonatkozó ajánlások után a drónokkal végzett csomagszállítást érintő javaslatokat is tesznek, főként a *Gépek biztonsága. Vezérlőrendszerek biztonsággal összefüggő részei. A tervezés általános alapelvei (ISO 13849),* Nemzetközi Szabványügyi Szervezet (ISO[7]) által kiadott szabvány [32] és a *Gépek biztonsága. A kialakítás általános elvei. Kockázatfelmérés és kockázatcsökkentés (ISO 12100)* [33] szabványokra alapozva. Egy másik megközelítésként bemutatják a Bayes-hálók valószínűségi modellként történő alkalmazásának lehetőségét a biztonság kvantitatív elemzéséhez.

Felhő alapú rendszerek területe

A felhő alapú rendszerekhez kapcsolódó publikációk közül elsőként Tóth András *A hálózat nyújtotta képesség megvalósításának lehetőségei a Magyar Honvédség kommunikációs rendszerében* című doktori értekezését [34] vizsgálom.

A hálózat nyújtotta elméleti is gyakorlati képesség alapjaival kezd, a vezetés-irányítás (C2[8]), a konzultáció, vezetés-irányítás (C3[9]), a vezetés, irányítás, kommunikáció, számító-

[7] International Organization for Standardization
[8] Command and Control
[9] Consultation, Command and Control

gép, hírszerzés, megfigyelés és felderítés (C4ISR[10]) fogalmainak tisztázásával. Később a felhő informatika típusait mutatja be, a nyilvános, magán, hibrid és közösségi felhő rendszereket. Kutatásom szempontjából fontos elkülöníteni ezeket, hiszen védelmi alkalmazás terén aligha jöhet szóba jelenleg publikus felhő alkalmazása biztonsági okokból, ezt a szerző is implicit megállapítja.

A következő fontos kategorizálás, a szolgáltatásként kínált infrastruktúra (IaaS[11]), a szolgáltatásként kínált platform (PaaS[12]) és a szolgáltatásként kínált szoftver (SaaS[13]). Ezek a lehetőségek azt határozzák meg, hogy mekkora felelősség hárul a felhő rendszer felhasználójára, karbantartási, kiszolgálási szempontból. Ez úgy is értelmezhető, hogy a felhasználó mennyire hajlandó kiengedni kezéből az irányítást.

Ezután megállapítja, hogy az Észak-atlanti Szerződés Szervezete (NATO[14]) kommunikációs rendszere teljes mértékben digitalizált, a jelen kihívásainak tökéletesen megfelel. Az integráció érdekében a Magyar Honvédség rendszereinek digitalizálására is törekedni kell.

Magyar Honvédség Műveleti Vezetési Rendszerének elemzése eredményeként a szerző arra a megállapításra jut, hogy annak minden körülmények között biztosítania kell a parancsnoki döntéshozatal feltételeit, az irányítási és vezetési rendszer működését béke időszakban, a béke időszaki vezetési objektum veszélyeztetettsége esetén, valamint békétől eltérő állapotok során egyaránt. Ezt a fontos szempontot terveztem megvizsgálni felhő alapú rendszer alkalmazásának esetén.

Megállapítja, hogy a Magyar Honvédségben zászlóalj szint alatt digitális rádióhálók kerülnek alkalmazásra, míg felette és hadműveleti, hadászati szinten az elsődleges kapcsolatok Ethernet vagy műholdas hálózatok kiépítésével valósulnak meg. Ez a felépítés párhuzamot von a jelen értekezés későbbi fejezeteiben leírtakkal tervezés szempontjából.

Racskó Péter *A felhő alapú számítástechnika biztonsági kérdései a közigazgatásban* című egyetemi jegyzete [35] oktatási céllal jött létre, különlegessége, hogy összefoglalja az Európai Unió és egyéb külföldi országok a számítási felhő közszférában történő alkalmazására vonatkozó álláspontját és törekvéseit. Kutatásom szempontjából kiemelendő a *Biztonság és megfelelőség* fejezet, illetve *A számítási felhő általános kockázatai* fejezet. Ezeken kívül tárgyalja a felhőben történő tárolás kockázatait és a kockázatok, felelősség kérdését. Kitér

[10] Command, Control, Communications, Computers, Intelligence, Surveillance and Reconnaissance
[11] Infrastructure as a Service
[12] Platform as a Service
[13] Software as a Service
[14] North Atlantic Treaty Organisation

a titkosításra, és a titkosított adatok tárolására, illetve a kulcsmenedzsmentre, illetve az adatátvitel titkosítására is.

Fontos információkat ad a kockázatelemzési elvekről, illetve a felhő szolgáltató átvilágításáról.

Napjainkra számtalan más típusú felhő szolgáltatás is napvilágot látott az IaaS, PaaS és SaaS szintjein túl, szinte minden felhasználói, alkalmazói igény kielégítésére találhatunk egy megfelelő szolgáltatástípust [36]. Ezek közül kiemelném a szolgáltatásként kínált drón (Drone as a Service) kategóriát, [37] mely különösen fontos kifejezés a kutatásaim szempontjából. Azonban a korábbi diplomamunkámban megálmodott, és a doktori kutatásaim során megvalósított rendszer előrevetíti, hogy egy ilyen rendszer képes lehet nem csak UAV-k, hanem egyéb (szárazföldi, vízi, légi vagy akár a világűrben működő) járművek távoli irányítására és felügyeletére, illetve útvonalak tervezésén túl egyéb akciók (például kamera felvétel indítása, gimbal mozgatása, leszálló talpak kiengedése, markoló/kar nyitása, hordozott teher leválasztása, fékező vagy ejtőernyő nyitása, rögzítőfék oldása stb.) programozására is a MAVLink protokoll lehetőségeinek köszönhetően. Ennek a fogalombéli hiányosságnak feloldására elneveztem egy új, bővebb kategóriát „Mission as a Service-nek," (MaaS) vagyis szolgáltatásként kínált küldetésnek, melyet a következőképp definiálom:

„Olyan összetett, nagy biztonságú, felhő alapú szolgáltatástípus, amely lehetővé teszi komplex műveletek- és küldetések tervezését és azok végrehajtásának távfelügyeletét, naplózását és a kapcsolódó információelosztást autonóm működésű, vagy ember által távirányított felszíni, felszín alatti, légi vagy a világűrben működő járművek számára."

1. definíció: Mission as a Service, azaz szolgáltatásként kínált küldetés.
(Megfogalmazta a szerző.)

A Mission as a Service kifejezést először 2019-ben alkalmaztam [S5] a prototípus rendszer bemutatása során egy magyar nyelvű publikációmban. Független forrásokban később több helyen találkoztam a kifejezéssel, mindegyik esetben (Space) Mission as a Service-ként, világűrbéli, műholdas szolgáltatásokat takart, melynek keretein belül a műholdak fedélzeti kapacitásához, műszereihez, adataihoz bérelhet hozzáférést a felhasználó [38] [39]. Ezért, ha a szövegkontextus szükségessé teszi a fogalombéli megkülönböztetést, javaslom az Unmanned Mission as a Service (UMaaS) pontosítást, kiemelve a pilóta vagy irányító személyzet nélküli működtetést, szemben a Space Mission as a Service kifejezéssel.

A felhő alapú rendszereket hozzáférhetőség alapján a következő csoportokba sorolhatjuk, az USA Védelmi Minisztériumának stratégiája szerint: [36]

- Publikus felhő, amikor az ügyfelek erőforrás kapacitást (hálózat, számítási kapacitás, tároló) bérelnek egy szolgáltatótól.
- Privát felhő, amikor egy szervezet saját maga által kialakított és fenntartott felhő rendszert üzemeltet, bérelt, vagy saját maga által üzemeltetett erőforrásokon.
- A közösségi felhőt a következőképpen definiálja. Egy hasonló igényekkel rendelkező szervezeteket vagy privát ügyfeleket, közösséget kiszolgáló rendszer átmenet a publikus és a privát felhő közt.
- Hibrid felhő alatt a felsorolt felhő csoportok vegyítése értendő.

Kockázati szinteket is meghatároz, ami a kutatásomban kifejezetten hasznos szempontot ad. Az adatokat alacsony, közepes és magas kockázati szintekre osztja.

Szintén az USA Védelmi Minisztériuma kiadott egy útmutatót a felhő alapú számítási rendszerek biztonsági követelményei címmel [40]. A dokumentum hátterének rövid felvezetése után leírja a bizalmasság, sértetlenség és rendelkezésre állás alap hármasát, illetve meghatározza az adatok védelmi szintjeit 1-től (nyilvános közzétételre jóváhagyott nyílt információ) 6-ig (minősített adatok „titkos" szintig).

Kitér a felhő alapú szolgáltatások biztonsági kockázatelemzésére, megkülönböztetve a kereskedelmi forgalomban elérhető, nyilvános felhőszolgáltatások és a DoD által kiszolgált, privát felhő szolgáltatások sajátosságait, illetve ezek esetén a felelősségi körökre kérdésére is. A következő fő fejezetben részletesen kifejti a biztonsági követelményeket, mind a fizikai, adminisztratív, személyi és elektronikus dimenzióban. Az utolsó fő fejezetben a számítógépes hálózati védelem és a biztonsági események esetén követendő cselekvési terv kérdéseivel foglalkozik.

Az USA Haditengerészeti Minisztériumának honlapján megtalálhatunk egy segéddokumentumot, [41] ami a fenti dokumentum alapján készült, és a védendő adatok említett hat védelmi szintbe történő bekategorizálását segíti.

Szabványok terén megjelent az ISO és a Nemzetközi Elektrotechnikai Bizottság (IEC[15]) 27000-res szabványcsaládon belül az ISO/IEC 27017-es, [42] ami az ISO/IEC 27002-tes, *Gyakorlati útmutató az információbiztonsági kontrollokhoz/intézkedésekhez* [43] szabvány kifejezetten felhő alapú rendszerekre történő kiterjesztése.

Az Európai Távközlési Szabványügyi Intézet (ETSI[16]) kiadott egy útmutatót, [44] ami a hálózati elemek virtualizálásának biztonsági megfontolásaival foglalkozik.

[15] International Electrotechnical Commission
[16] European Telecommunications Standards Institute

Bevezet négy fontos fogalmat, ami a fel- és leskálázódás, illetve a kifelé és befelé skálázódás – ezeket vertikális és horizontális skálázódásnak nevezzük más szóval. A vertikális lényege, hogy szükség esetén az adott virtuális elem kapacitását növeljük, a horizontális pedig a több elem közti erőforrás elosztást javítjuk.

Kifejezetten a biztonsági aspektusokra vonatkozóan az amerikai Nemzeti Szabványügyi és Technológiai Intézet (NIST[17]) is kiadott egy közleményt, [45] ami a publikus felhő alapú rendszerek esetén nyújt iránymutatást. Ez a korábban hivatkozott külföldi útmutatókkal és szabványokkal állítható párhuzamba tartalmilag.

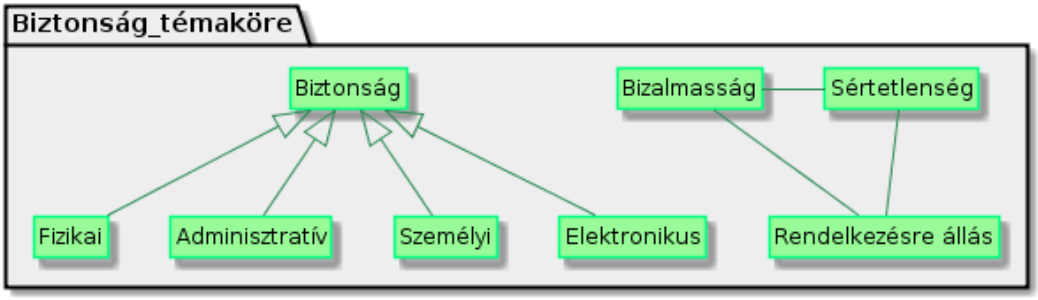
Következtetések

A sorra megjelenő, a témával foglalkozó szabványok és ajánlások, konferencia kiadványok, könyvek és folyóiratcikkek jól mutatják, mennyire a tudományos élet fókuszában van a két terület jelenleg is.

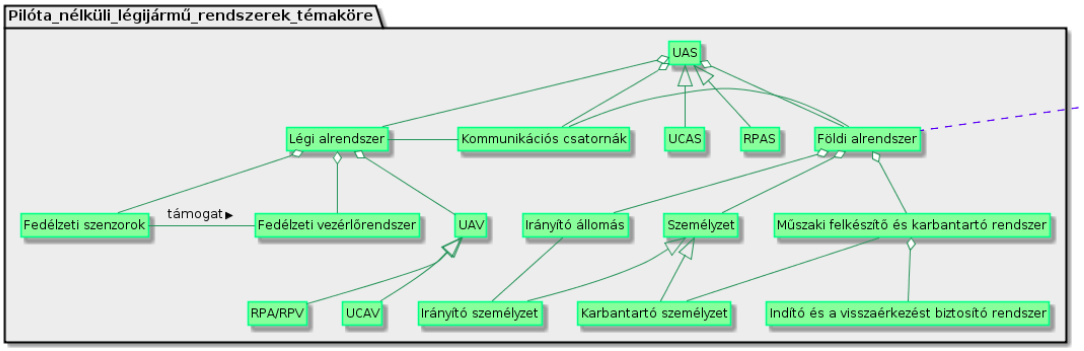
A feldolgozott anyagokban nagyon sok tartalombeli átfedés van, viszont még maradtak kevésbé vizsgált részterületek, amiket további kutatással lehet orvosolni. Korábban nem született olyan tanulmány, ami a két terület fizikai, adminisztratív (avagy dokumentációs [46]), személyi és elektronikus biztonságát együttesen, rendszerezetten vizsgálná. Ez a megállapítás egyfelől megerősített témaválasztásom aktualitását tekintve, másrészt keretet adott a téma megközelítésbéli felbontására, és segítette a kutatási hipotézisek megfogalmazását is. Az értekezés egyes fejezeteiben továbbá kapcsolódási pontokat találtam a U-space szabályozás IV. fejezete által meghatározott, különböző szolgáltatásokkal szemben támasztott követelményekhez is [26].

Az irodalmi kutatás eredményeként összeállítottam a következő fogalomtérképeket a biztonság (2. ábra), az UAS-k (3. ábra) és a felhő rendszerek (4. ábra) területével kapcsolatban előforduló gyakori fogalmakból [S2]. Az UAS-k és a felhő terület egy lehetséges kapcsolódási pontját a két ábrát virtuálisan összekötő kék szaggatott vonallal jelöltem. A fogalomtérképeket Egységesített Modellező Nyelv (UML[18]) osztály diagram formájában készítettem el.

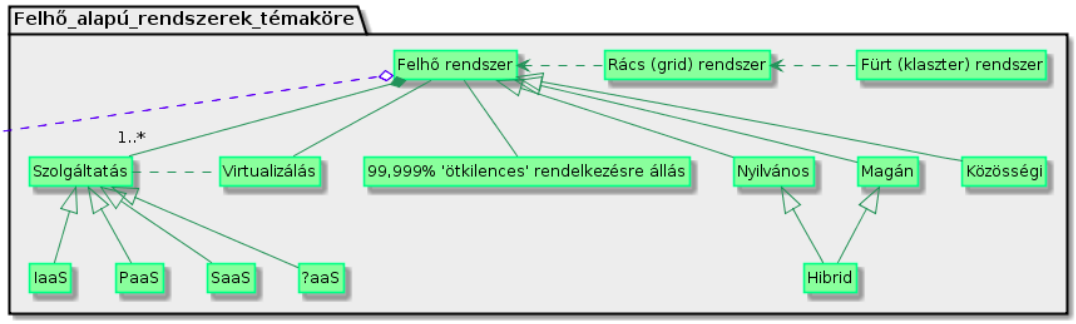
[17] National Institute of Standards and Technology
[18] Unified Modeling Language



2. ábra: A biztonság témaköre.
(Készítette a szerző. Forrás: [46])



3. ábra: A pilóta nélküli légijármű rendszerek témaköre.
(Készítette a szerző. Forrás: [11])



4. ábra: A felhő alapú rendszerek témaköre.
(Készítette a szerző. Forrás: [34])

Láthatjuk, hogy a hazai és nemzetközi irodalom széles repertoárja áll rendelkezésre – a hagyományos papír alapú média mellett – különböző publikációs adatbázisokban és hivatalos szervezetek honlapján elektronikus formában is. A jogszabályok elérhetők és szabadon kereshetők az Európai Unió és a Magyar Közlöny honlapján, a szabványok pedig a szabványosító szervezetek honlapjain (általában díjazás ellenében) érhetők el.

Az értekezés felépítése

Az értekezés **1. fejezetében** bemutatom a pilóta nélküli légijármű-rendszerek különböző aspektusait, történetét, képességeit, felhasználási lehetőségeit. Hasonló szempontok alapján

bemutatom a felhő alapú számítástechnika területét és biztonsági, illetve személyes adatokat érintő kérdéseit.

A **2. fejezetben** részletes technikai leírást adok egy felhő alapú UAS gyakori követelményeiről, illetve az elterjedt irányítási és azonosítási protokollokról, majd a rendszer felbontása alapján párhuzamot vonok az IoT rendszerek felépítésével.

A **3. fejezetben** bemutatom a kialakított tesztkörnyezeteket: a repülési tesztekhez használt repülőeszközt, légteret és (az akkori előírásoknak megfelelő) jogi hátteret, illetve a kifejlesztett szimulátor szoftver felépítését, a tesztesetek kijelölésének megfontolásait.

A **4. fejezetben** a végrehajtott repülési teszteseteket mutatom be, melyek rámutattak a rendszer egyes hiányosságaira és lehetőségeire.

A kapcsolódó laboratóriumi tesztesetek során 100 drónt szimulálok szoftveresen, miközben demonstrálom a felhő rendszer skálázódási és túlélőképességét, túlterhelt helyzetben vagy hálózati katasztrófa esetén.

Bemutatom a felhő és fizikai rendszerek egy teljesítmény- és költségbeli összehasonlítását időjárás előrejelző modell futtatása esetén.

Összehasonlítom a különböző szélmérési lehetőségeket UAV-k esetén, illetve bemutatok a veszélyes időjárási jelenségek autonóm elkerülésére egy technikai megoldást.

Az **5. fejezetben** felvezettem az UAS-specifikus publikus kulcsú infrastruktúra lehetőségeit, egy lehetséges európai szintű eljárásrend, illetve szervezeti felépítés felvázolásával.

Összegzem a felhőben kezelt UAS-specifikus adatok dimenzióit.

A **6. fejezetben** személyi biztonság témakörében technikai megoldásokat mutatok be a távpilóták és drónok ad-hoc elektronikus összerendelésére, a felszállások távoli engedélyezésére, illetve a hatósági beavatkozás lehetőségeire.

Bemutatom az UAV-k és távpilóták, illetve műveletek távoli azonosítására használható OpenDroneID üzenetek tartalmát, melyek megfelelnek az Európai Uniós előírások elektronikus azonosításra vonatkozó követelményeinek.

A **7. fejezetben** az elektronikus biztonság kérdését érintve megvizsgálom az Open Glider Network rendszerét, és megmutatom egy esettanulmányon keresztül, miért fontos nyílt rendszerek esetén is az információbiztonság szem előtt tartása.

Bemutatom az OpenDroneID rendszer működését és felépítését is, annak korlátait és lehetőségeit.

Matematikai számításokkal levezetve bemutatom a MAVLink 2.0 aláírás mezőjének egy lehetséges valószínűségszámítás alapú támadását.

Végül a robotpilóta irányába a földi irányító állomás szimulálásával végzett laboratóriumi teszteseteket mutatok be.

KÖSZÖNETNYILVÁNÍTÁS

Hálával tartozom témavezetőmnek a szakmai támogatásért, iránymutatásért, aki az adminisztráció útvesztőiben is mindig a fejem felett tartotta a lámpást.
Az Ericsson Magyarország Kft. két részlegének, ahol eddig megfordultam a cégnél töltött 10 évem alatt: a hajdani Test Competence Center „Titánjainak" és a Cloud Execution Environment „FelHőseinek".
A Nemzeti Közszolgálati Egyetem GINOP-2.3.2-15-2016-00007 azonosító számú *„A légiközlekedés-biztonsághoz kapcsolódó interdiszciplináris tudományos potenciál növelése és integrálása a nemzetközi kutatás-fejlesztési hálózatba a Nemzeti Közszolgálati Egyetemen (VOLARE)"* projektjén dolgozó kollégáimnak, akikkel „felhőalapról" és „felhő alapról" egyaránt lehet elmélyülő szakmai vitát folytatni.
Munkatársaimnak a MouldTech Systems Kft-nél, akik mernek nagyot álmodni.
Külön köszönetet érdemel családom a megértő és kitartó, szüntelen támogatásért.

Kutatásom eredményeit ajánlom nagyapám, Bődi Ferenc ny. ezredes; és volt főnököm, BSc témavezetőm, Lelik Elemér emlékének.

1 A KUTATÁS TECHNIKAI ESZKÖZRENDSZERE

1.1 Pilóta nélküli légijármű-rendszerek bemutatása [S1]

1.1.1 Kapcsolódó fogalmak tisztázása

A sajtóban gyakran találkozhatunk a következő kifejezésekkel: drón, UAV, UAS, RPAS, RPV, robotrepülőgép stb. A legtöbbször ezek alatt egy fogalmat értenek, egyes estekben ezeket a fogalmakat egymással tévesen összekeverik. Gyakorlatilag olyan repülő eszközt és a hozzá kapcsolódó kommunikációs, navigációs, valamint irányító rendszert értenek alattuk, aminek irányításához nincs szükség a légijármű fedélzetén fizikailag jelenlévő pilótára.

A felsoroltak közül legtöbbször a „drón" szóval találkozhatunk, ez az angol nyelvből átvett, eredetileg „drone" szó magyarított átirata, aminek jelentése a méhészetből átvett „dolgozó", „here". Az átlagember a „drón" szó hallatára azonnal repülő eszközre asszociál, ellenben drónnak nevezhetjük azokat az eszközöket is, amelyek felszínen, felszín alatt vagy akár a világűrben végeznek távirányított, vagy -felügyelt tevékenységet.

Az UAV és UAS rövidítések a személyzet nélküli légijármű, illetve légijármű-rendszer angol megfelelőiből származnak, főleg tudományos és védelmi területen találkozhatunk velük – mind forgószárnyas, mind merevszárnyas légijárművekkel kapcsolatban. A MAV[19] kis méretű légijárművet jelent, apró méretükből adódóan ezt a megnevezést is leginkább pilóta nélküli eszközökre alkalmazzák. Fontos és aktuális kifejezés a téma szempontjából még az UTM[20] – pilóta nélküli légijármű-rendszerek forgalmi menedzsmentjét biztosító megoldások együttese, mely magába foglalja az UAS-en kívül többek között a repülés többi résztvevőjét, a hatóságokat, repülésmeteorológiai rendszereket, és a légforgalmi tájékoztatás rendszerét. Az RPV[21], mint távolról irányított jármű és RPAS[22], azaz távolról irányított légijármű rendszer megnevezéseket eleinte leginkább a távirányításra átalakított, eredetileg pilóták által vezetett hagyományos repülőgép(rendszer)ekre használták, ma már ezt is elterjedten említik hivatalos körökben az UAV és UAS szinonimáiként, elsősorban a civil drón alkalmazásokkal kapcsolatban.

A „robotrepülőgép" szót a média gyakran helytelenül használja akár a polgári felhasználású, hobby célú UAV-k leírására is. Robotrepülőgép alatt a sajtóban gyakran az angol „cru-

[19] Micro Air Vehicle
[20] Unmanned Aircraft Systems Traffic Management
[21] Remotely Piloted Vehicle
[22] Remotely Piloted Aircraft System

ise missile" kifejezésből tükörfordított „cirkáló rakéta" kifejezéssel illetett haditechnikai eszközöket értjük. Ezen megnevezés esetén a „rakéta" szó használata sem helytálló, mert több típusuk gázturbinát használ a meghajtásra, nem rakéta hajtóművet. Ezek általában közepes vagy nagy hatótávolságú, távirányított és/vagy autonóm repülésre képes fegyverek, melyek célja – a legtöbb UAV-tól eltérően – a célpontok becsapódással történő megsemmisítése. Esetükben a helyes kifejezés a manőverező robotrepülőgép.

Technikai megvalósításuk tekintetében megkülönböztethetünk forgószárnyas drónoknál kvadrokoptert (négyhajtóműves), hexakoptert (hathajtóműves), oktokoptert (nyolchajtóműves) illetve egyéb multikoptereket is – vagy akár további különleges rendszereket, például koaxkoptert (koaxiális hajtóművel rendelkező drón), helikvadot (rotor fordulatszám helyett kollektív állásszögállítással irányítható négyhajtóműves drón). Ez a fajta nevezéktan nem mutatja meg, hogy a szóban forgó eszköz pontosan milyen képességekkel rendelkezik, vagy, hogy esetlegesen ez csak egy platform, ami tovább bővíthető, csupán a vázszerkezet és a rotorok elrendezését adja vissza.

Kutatásom során azt tapasztaltam, a polgári életben beszerezhető kis méretű repülő eszközöket a köznyelv „drónokként" azonosítja, a katonai műveletekben vagy tudományos kutatásokban résztvevő, általában nagyméretű eszközöket pedig a szakma „UAV" megnevezéssel illeti. Az RPAS vagy RPV kifejezés pedig szinte kizárólag a hivatalos, civilszövegkörnyezetben használatos. Viszonylag új fogalom a „nagy magasságú, nagy hatótávolságú" (HALE[23]) és „nagy magasságú pszeudoműhold" (HAPS[24]) UAS, melyeket az általában napelemmel felszerelt, egy felszállással akár hónapokat is a levegőben tölteni képes UAS-kra értik. Az értekezésben a felsoroltak közül leginkább a drón, UAV, illetve UAS kifejezéseket alkalmazom.

1.1.2 Műszaki fejlődés, polgári felhasználás

A kezdetleges távirányítású modell repülőgépekhez hasonlóan az egyik legelterjedtebb irányítási módszer a négy csatornás, 2,4 GHz-es tartományban működő távirányító. A polgári életben leginkább elterjedt eszközöknél, ahol ezt a megoldást részesítik előnyben és rendelkeznek média (videó és hang) átvitellel is, utóbbit külön csatornán oldják meg, esetleg teljesen elkülönített irányító és megjelenítő rendszerrel, ahogy az 5. ábrán is megfigyelhető.

[23] High Altitude Long Endurance
[24] High-Altitude Pseudo-Satellite

Széles körben alkalmazott megoldás, hogy egy eszköz, amennyiben alkalmas videó rögzítésére, a felvételt nem csak továbbítja a felhasználónak, hanem helyben is rögzíti (univerzális soros busz (USB[25]) tárolóra, biztonságos digitális (SD[26]) kártyára), így, ha akadozik vagy nem megfelelő minőségű a lesugárzott videókép, később hozzáférhető a folyamatos, sokszor jobb minőségű, rögzítettfelvétel.

Ipari felhasználású UAS-knál az esetleges hasznos teher (például külön vezérelhető képrögzítő rendszer) esetén szükség lehet a pilóta mellett egy külön operátorra is, aki a fedélzeti hasznos terheket kezeli.

A wifi-irányított eszközöknél elvben nincs korlátozva az adatfolyamok száma. Ilyenkor a legtöbb esetben maga a repülő eszköz viselkedik egy wifi hozzáférési ponthoz hasonlóan, a szórt hálózathoz a távirányító eszközök a megszokott módon csatlakozhatnak, és az irányításhoz szükséges jel, a videó és a telemetria adatok külön-külön csatornán (átviteli vezérlő protokoll/internetprotokoll (TCP/IP[27]) modellnek megfelelő portokon) kerülnek átvitelre az irányítóállomás és a repülő eszköz között.

Az újabb távközlési technológiák elterjedésével az irányítási és telemetrikus csatornák egyre hatékonyabbá és megbízhatóbbá válnak, lehetőség nyílik a légijárművek folyamatos nyomkövetésére vagy összekapcsolására repülés közben.

5. ábra: DJI gyártmányú oktokopter a hozzá tartozó távirányítóval.
(A képeket készítette a szerző.)

[25] Universal Serial Bus
[26] Secure Digital
[27] Transmission Control Protocol/Internet Protocol

A wifivel felszerelt UAS-k egy fejlettebb változatának tekinthetjük a 4. generációs (4G[28])/5. generációs (5G[29]) vagy egyéb IoT (LoRaWAN, NB-IoT) kommunikációra képes repülő eszközöket. Ez némileg magasabb költséggel járó és viszonylag új megoldás, így az alsó- és középkategóriás, polgári életben is megvásárolható eszközökben ritkán találkozni ilyesmivel. A Nemzeti Média- és Hírközlési Hatóság (NMHH) Spektrumgazdálkodási Osztályának közleményében tájékozódhatunk további lehetséges frekvenciák és technológiák használatról és azok esetleges engedélyezési kérdéseiről [47].

Az autonóm repülésre képes, GPS-szel felszerelt, vagy tehetetlenségi navigációs rendszerrel rendelkező UAV-k célja a földrajzi A-ból B-be történő (akár felügyelet nélküli) eljutás.

1.1.3 Hatótávolság fejlődése

Az előzőekben leírt irányítási modelleknek megfelelően különböző csoportokba sorolhatjuk az UAV-kat hatótávolság alapján is.

Első csoportnak tekinthetjük a hatásosan csak látótávolságig reptethető eszközöket.

Következő csoportnak tekinthetjük az olyan UAS-kat, ahol van élő képátvitel, és a korábban leírtakhoz hasonlóan elkülönített rádió távirányítással működnek. Ezek hatótávolsága több kilométer is lehet.

Külön csoportként itt is felvethetjük a wifivel ellátott UAS-kat, ahol minden átvitel wifi alapon történik. Ennek hátránya a rövid, körülbelül 150 méteres hatótáv, ami függ az időjárási és terepviszonyoktól is. Ennek kibővítése a már említett mobil hálózati adatkapcsolat kiépítésére képes változat, ahol a hatótávolságot a mobil térerő és az ezt befolyásoló tényezők szabják meg.

Bár az ötödik (és a kidolgozás alatt álló hatodik) generációs és IoT hálózatok (lásd később) hasonló felhasználások kiszolgálását célozzák – okos gépjárművek, okos háztartási készülékek, okos városok –, a főként földfelszíni alkalmazás és az irányított antennák miatt nagyjából 1500 láb AGL (földfelszín feletti magasság) fölött a megfelelő lefedettség meglehetősen ritka.

Utolsó csoportként emeljük ki a GPS-szel és/vagy inerciálisan navigációra alkalmas pilóta nélküli repülő eszközöket, ahol elég a földrajzi, vagy relatív koordinátákat az eszközbe táplálni, és az beavatkozás nélkül képes eljutni a drón a megadott céljához. Itt a hatótávolságot gyakorlatban főleg az üzemanyagtartály vagy akkumulátor kapacitása, a navigációs műholdak aktuális láthatósága és a jogi szabályozás korlátozhatja. Kísérletek folynak ha-

[28] 4th Generation
[29] 5th Generation

sonló önirányítású pilóta nélküli repülőgépek napelemmel történő üzemeltetésére, amik időjárástól függően akár hónapokig is szolgálatot teljesíthetnek. Ezeket nevezi a szakma HAPS vagy HALE UAV-knak melyek felhasználása lehet például „földközeli műhold" analógiájára mobil átjátszó állomás katasztrófa sújtotta területeken, hegyek-erdők közti, nehezen lefedhető helyeken egy ideiglenes művelet támogatására; vagy rendvédelmi, határrendészeti felhasználásban egy terület hosszú ideig tartó megfigyelése, ellenőrzése.

1.1.4 Képességek fejlődése

Rendvédelmi felhasználásban néhány országban megjelentek a paintball lövedékekkel felszerelt tömegoszlatásra alkalmas UAV-k [48]. Indiában paprika spray-vel felszerelt eszközökkel kísérleteznek a rendvédelmi szervezetek fejlesztői [49].

Mára szinte bármely elektronikai üzletben megvásárolhatók a képrögzítésre is alkalmas drónok. A hobbi felhasználás mellett külön cégek alapultak esküvők filmezésére, terepfelmérésre, térképezésre, hő- és infrakamerás felvételek készítésére, nehezen megközelíthető helyek felderítésére, épületek, műemlékek felmérésére, földek permetezésére.

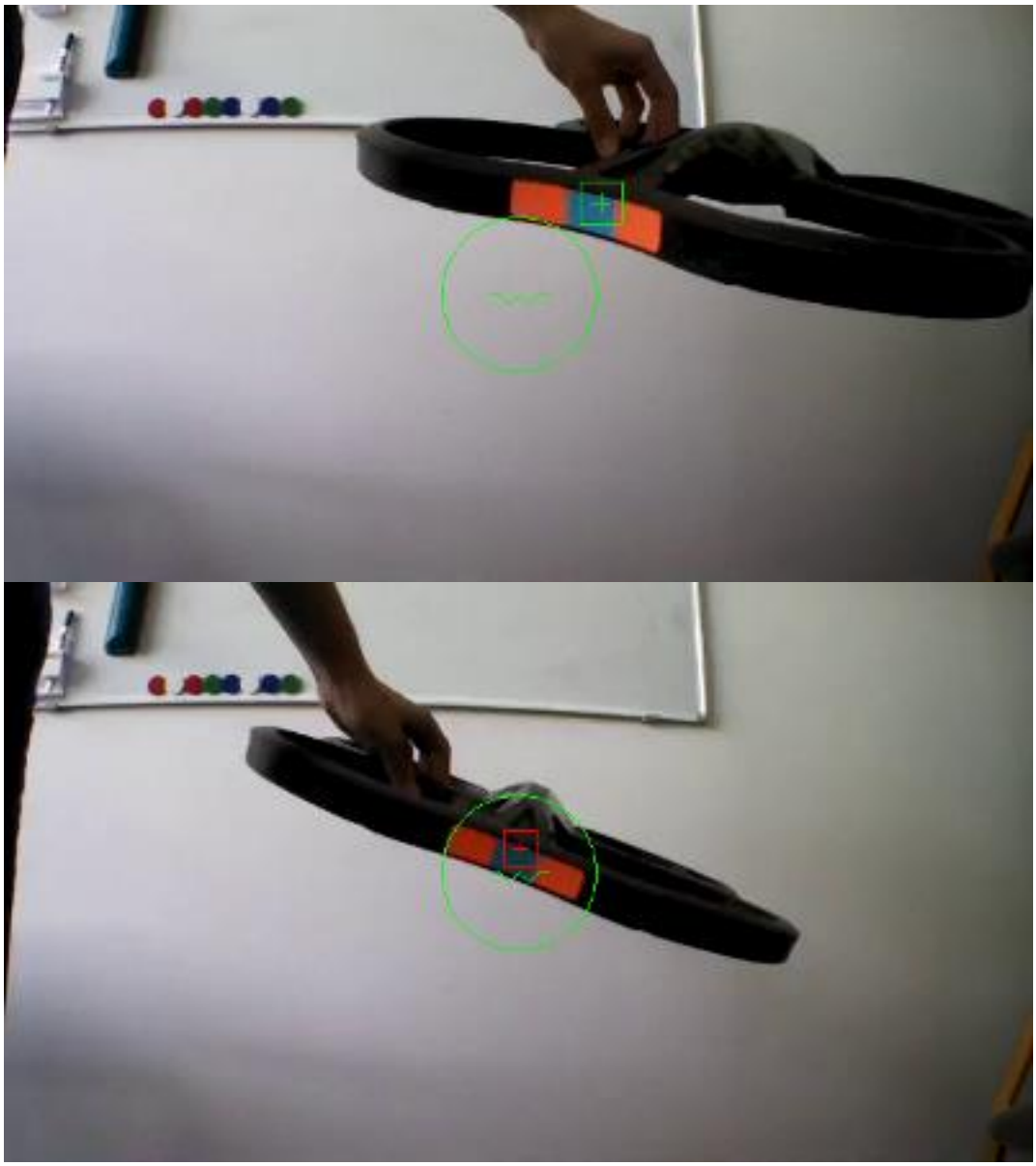
Külön kiemelhetjük az Amazon cég anno nagy botrányt kavart bejelentését, miszerint csomagok kézbesítését megcélzó szolgáltatást indít, ahol a megrendelt csomagokat pilóta nélküli repülőgépek juttatják az megrendelő címére. 2019-től kezdődően a Federal Aviation Administration (FAA) sorra jóváhagyta a Wing Aviation, és az UPS Flight Forward vállalatok petícióit drónflotta üzemeltetésére csomagszállítás céljával az Egyesült Államok területén, 2020-ban végül az Amazon Prime Air szolgáltatása is megkapta a működési engedélyt [50].

A polgári drón rendszerek sokat fejlődtek 2010-es évek eleji robbanásszerű piaci térnyerésük óta. Az akkumulátor kapacitásuk és hatótávolságuk megtöbbszöröződött, a felszerelhető hasznos teher pedig tovább csökkent méretben és tovább fejlődött képességek terén. Az áruházak polcain a kezdeti egyszerűbb kézi irányítású drónok helyét átvették a stabilizált, „okos", félig vagy teljesen autonóm repülésre képes megfelelőik, melyek nagy felbontású kamerával szerelve érkeznek. Az ipari UAV-k pedig felszerelhetők professzionális, lézeres 3D szkennerrel, multispektrális kamerával vagy akár gázösszetételt elemző szenzorral.

Az autonóm feladatok, küldetések számának növekedésével és az egyre telítődő légtérrel az útvonaltervezés és ütközéselkerülés erősen számításigényes feladata a fedélzeti alrendszerektől inkább a földi alrendszerek felé tolódik a pilóta nélküli repülés ökoszisztémájában. A telekommunikációs rendszerek fejlődésének analógiájára várható, hogy egyes számítások az UAS-k esetében is a peremhálózat (edge) felé tolódnak [51] a hálózati késlelte-

tés minimalizálása érdekében, például kamerakép alapján történő dinamikus ütközéselkerülés megvalósítása, ahol az (egy rendszerben lévő) veszélyeztetett légijárművek közös földi állomáshoz kapcsolódnak. A 6. ábrán látható a fedélzeti képfeldolgozás és a lesugárzott kameraképen történő utólagos megjelenítés egy példája a korábbi diplomamunkámból [52]. A technológia akkori képességei kimerültek abban, hogy az algoritmus a 720p felbontású kameraképen pár méter távolságból képes volt felismerni egy, a céltárgyra ragasztott élénk színű matricát.

Napjainkra elérhetők kis méretű, akár több párhuzamos neurális hálót futtató számítógépek (például az NVIDIA Jetson Nano [53]), melyek képesek nagy felbontású képek intelligens feldolgozására, tetszőleges minták valós idejű felismerésére. Ilyen kiegészítő komponens nyilván elhelyezhető egy UAV-n is, viszont ez tovább csökkenti a hordozható hasznos teher számára rendelkezésre álló akkumulátor- és emelőkapacitást, illetve külső komponens nem minden esetben csatlakoztatható régebbi, elavult, vagy zárt rendszerű drónokhoz, így nagyobb számítási kapacitást igénylő feladatok esetén gazdaságosabb ezt a funkcionalitást a földi alrendszerbe kiszervezni, a kameraképet utólag elemezni. Nyílt rendszerű és megfelelő fedélzeti számítási kapacitással rendelkező drónok esetén lehetséges az elemzést a robotpilóta szoftverében is megvalósítani, ahogy ez a lenti ábrákon is látható.



6. ábra: Fedélzeti kamerakép feldolgozása valós időben.
(A képernyőképeket készítette a szerző.)

1.1.5 Alkalmazási területek

A kis méretű UAS-k alkalmazásával lehetőség nyílik nagyméretű mezőgazdasági területek megfigyelésére, felmérésére vagy permetezésére is. A drónokra szerelt nagy felbontású kamerákkal különböző látható és nem látható spektrumokban felvett képekkel hatékonyan megállapítható az egyes területeken telepített növényzet fejlődése és betegsége egyaránt. Pár éve nekem is volt szerencsém támogatni egy sikeres közösségi finanszírozású projektet, mely során 20 millió fát ültettetett el – többek között magokat hexakopterekről kijuttatva – egy fiatal vállalkozó [54].

Afrikában sikerrel alkalmaznak UAV-kat vadorzás megelőzésére és felderítésére, állatok nyomon követésére, állatcsoportok egyedeinek számlálására [55].

A planetáris határréteg magasabb szintjeinek meteorológiai szondázását hagyományosan ballonokkal végzik. Ennek a módszernek hátrányai többek között, hogy egy-egy felereszt és hosszasabb procedúrát vesz igénybe a héliummal történő töltés miatt, illetve a szabadon engedett ballont pedig később be kell gyűjteni, és a visszaszerzésére nincs teljes garancia, így a szenzorrendszereket is gyakran egyszerhasználatosra tervezik. Utóbbi problémák feloldására részmegoldást nyújthat a kötöttballonos módszer, mely folyamán a mérések végeztével a ballon visszacsörlőzhető a kiindulási pontra. Ezen megoldás alkalmazásának hátránya viszont, hogy komolyabb szélben nem engedhető fel a ballon az erős elsodródás miatt.

Az ebből adódó hátrányok és hiányosságok kiküszöbölésére adta magát az újfajta megközelítés: UAV-k alkalmazása a szenzorok célba juttatására és visszatérítésére. A technológia ezen alkalmazása mára több, mint 10 éves múltra tekint vissza [56]. Mára az UAV-k ellenállóképessége olyan szintre fejlődött, hogy extrém időjárási körülmények közt is megállják a helyüket a meteorológiai kampányok során, például -20°C körüli hőmérsékleten [57], vagy trópusi ciklonok belsejében is [58] sikeres bevetéseket hajtottak végre velük a kutatók.

Magyarországon, Egyetemünk vonatkozásban is komoly múltra tekint vissza ezen alkalmazási terület kutatása, melyhez kapcsolódóan kiemelném a TÁMOP-4.2.1.B-11/2/KMR-2011-0001 „Kritikus infrastruktúra védelmi kutatások” című pályázatot [59], majd a GINOP-2.3.2-15-2016-00007 azonosító számú „A légiközlekedés-biztonsághoz kapcsolódó interdiszciplináris tudományos kutatási potenciál növelése és integrálása a nemzetközi kutatás-fejlesztési hálózatba a Nemzeti Közszolgálati Egyetemen (VOLARE)” című pályázatot, melyek sikerrel zárultak a szolnoki campus kutatóinak részvételével [60]. Ez utóbbi projekt UAS_ENVIRON kiemelt kutatási területén magam is részt vettem 2016. október 3. - 2021. március 31. között, doktori kutatásaimmal párhuzamosan.

A katasztrófavédelemben elterjedten alkalmaznak pilóta nélküli repülőgépeket a kutató-mentő akciók támogatására, kár utólagos felmérésére, eltűnt, vagy sebesült személyek felkutatására, esetleg gyógyszerek, mentőeszközök helyszínre juttatására.

2014-ben a német posta indított történelmi elsőként gyógyszerek kézbesítésére szakosodott, nyílt tenger fölött közlekedő drónszolgáltatást, az Északi-tengeren található Juist szigetet ellátására [61]. Majd később, 2016-ban két bajor-alpoki közösség kiszolgálására csomagszállító drónokat is üzembe állított. Legutóbb, 2018-ban Tanzániában egy nehezen megközelíthető viktória-tavi szigetre indított UAV missziót a DHL, hogy meggyorsítsa a betegségek diagnosztizálására szolgáló vérvizsgálatok elvégzését. Hat hónap alatt több,

mint 180 fel és leszállást, 2200 kilométert és 2000 repült percet teljesített a hűtött tárolórekesszel ellátott drón [62].

Korábban a Facebook közösségi portált akkor üzemeltető vállalat pilóta nélküli repülőgépek földközeli műhold-szerű alkalmazásával kísérletezett, internet lefedettség biztosítására elmaradott országokban, vagy nehezen megközelíthető helyeken [63]. Végül az Aquila projektet négy év után törölték, az Airbus-szal társulva kutatják a további lehetőségeket [64].

Alkalmazásuk kiterjedhet tűzfelderítés, tűzoltás körére is, [65] magyar vonatkozásban Szendrő városát érdemes megemlítenünk, itt állítottak szolgálatba a katasztrófavédelemnél kisméretű, felderítő UAV-t a világon elsőként [7]. A PNR No1 és PNR No2 pilóta nélküli repülőgépek bevetésre kerültek például tűzfelderítési feladatok során és az árvízi védekezés segítésére is.

A világ fegyveres erői már évtizedek óta alkalmaznak pilóta nélküli légijárműveket különböző harci tevékenységekre, illetve katonai műveletek támogatására. A jelenlegi katonai fejlesztések területén egyre inkább az autonomitás és kötelékben történő feladatellátás hatékonyságának fokozására törekszenek a fejlesztők. Repülőgépek légi utántöltését különböző műszerek segítségével eddig hagyományosan humán személyzet hajtotta végre. Az Egyesült Államok haditengerészete sikeresen tesztelte mind pilóta nélküli légijárművek autonóm légi utántöltését, illetve hagyományos repülőgépek UAV-ról történő légi utántöltését is [66] [67]. 2014 óta az orosz-ukrán konfliktus és háború során, az ukrán oldalon sikerrel alkalmaznak piacon kapható és saját építésű drónokat is. Az Aerorozvidka nevű egység korábban polgári önkéntesekből alakult, majd integrálódott a fegyveres erők alá. Tevékenységi körük kiterjed a pilóta nélküli légijármű-rendszerek, helyzetismeret és kiberbiztonság területére [68].

Embertömeg követésére, megfigyelésére hatékonyan alkalmazhatók különböző – látható és infra spektrumban üzemelő kamerával felszerelt forgószárnyas pilóta nélküli légijárművek. Hazánkban a határvédelmi feladatok támogatására kerültek alkalmazásra az említett kategóriába tartozó eszközök, lásd 7. ábra.

7. ábra: A katasztrófavédelem munkatársa irányít egy drónt a magyar-szerb határon felállított ideiglenes határzárnál Mórahalom térségében 2016. február 22-én.
(Forrás: [69])

Nem nehéz belátni, a korszerű, nagy felbontású, kis tömegű kamerák megjelenésének és elterjedésének köszönhetően akár arcfelismerő algoritmussal kiegészítve segíthetik a rendvédelmi szervek munkáját hasonló eszközök.

A sikeres alkalmazásból kiindulva adja magát a tömegoszlatás támogatásának lehetősége is.

Nagy visszhangot vert, amikor a sajtó beszámolt a Desert Wolf „Skunk Riot Control Copter" paprika, illetve marker festék töltetű paintball lövedékeket célba juttató multikopteréről (lásd 8. ábra), mely stroboszkóppal, lézeres célzóberendezéssel és hangszórókkal felszerelve képes beavatkozni zavargások esetén.

8. ábra: Skunk Riot Control Copter.
(Forrás: [48])

Ennek továbbfejlesztett változata, a „Mozzy Wildlife Darting Copter” nagyvadak befogásához szükséges altató lövedékek kijuttatására alkalmas. Éjszakai repülés támogatására FLIR Quark éjjellátó kamerával is fel van szerelve.

Felmerül az ötlet, hogy miért ne kerülhetne sor a későbbiekben forgószárnyas UAV-k alkalmazásra más formátumú nem halálos harcanyagok kijuttatása esetén?

A legegyszerűbb eset, ha tegyük fel, a légijármű a „szokásos”, gránát formában kijuttatható anyaggal lebeg a tömeg fölé, majd távirányítással élesíti és leejti a gránátot. A rotorok keltette, viszonylag jól irányított, „jet-szerű” vertikális légáram, mozgó légtömeg is jó szolgálatot tehet egyéb tömegoszlató anyag szórt kijuttatásánál: A kijuttatandó tömegoszlató anyagok közül a gáz vagy folyadék halmazállapotú, illetve szemcsés, kristályos jellegű, aeroszol anyagok jöhetnek számításba.

Tömegoszlatásra főként könnyfakasztó, garat- illetve torok nyálkahártya ingerlő hatású – tehát a szemet, az alsó és a felső légutakat támadó – harcanyagokat alkalmaznak.

„A könnyfakasztó anyagok az idegvégződéseken, a szaruhártyán, a nyálkahártyákon és a bőrön fejtik ki hatásukat. Igen sok szerves halogénszármazék rendelkezik ingerlő tulajdonságokkal, ismertebb képviselőik az adamzit, a Clark, a klóracetofenon (KAF), valamint a leghatásosabbnak ítélt „CS" fedőnevű anyag.” [70].

Az UAS-k bevetésével a válságkörzetek területén is sikeresen lehet légi megfigyelő tevékenységet végezni. Segítségükkel a tevékenység során a nemzetközi segélyszervezetek

munkatársai és a béketámogató erők távolról figyelhetik meg az eseményeket, ezzel minimálisra csökkentve a személyi sérülés lehetőségét a körzetben.

1.1.6 Szélsőséges felhasználások

Egyes esetekben a drónokat, szélsőséges személyek vagy csoportok felhasználhatják radikális célok elérésére is. 2014. októberében a szerb-albán labdarugó mérkőzésen néhány perccel a szünet előtt ismeretlen elkövetők egy távirányítós repülőgépre kötött albán zászlóval provokálták a Partizan-stadion szerb résztvevőit. A szerb nézők és a szerb játékosok egyaránt éles kritikájuknak adtak hangot az eseményre.

2015-ben a japán miniszterelnöki rezidencia tetején egy homokkal teli csomaggal szállt le egy drón, aminek a háttérsugárzása kimutatható volt – bár az emberre veszélyes mértéket nem érte el. A drón egy kis kamerát és egy műanyag üvegcsét vitt, amely radioaktív homokot tartalmazott a fukusimai körzetből, ahol még mindig magasak a sugárzási szintek. Sajtóinformációk szerint a berepülés a kormány nukleáris energiaügyi politikája elleni tiltakozás volt.

A számtalan légtérsértési és biztonsági incidens hatására a DJI cég megvalósította az általa forgalmazott drónok esetén a drón repülés elől elzárt légterek (NDZ[30]) kezelését GEO Zones néven, [71] ami lehetőséget ad az egyes földrajzi helyeken történő repülés korlátozására, például ütközéselkerülés vagy tiltott légtér elkerülése céljával. A kezdeményezés térkép és adatbázis formájában szolgáltatja a korlátozott vagy tiltott légterek adatait a felhasználók és UAV-k számára.

Amíg lehet saját drónt építeni nyomkövetés nélkül, addig ez a módszer nem véd meg felkészült, egyedi támadásoktól. 2018-ban Szíriában például a 9. ábrán láthatóhoz hasonló házi készítésű UAV-kkal hajtottak végre terrortámadást orosz katonai bázis ellen, mely során a bombákkal felszerelt 13 UAV közül hetet légvédelmi rakétával semlegesítettek, hat fölött pedig sikerrel átvették az irányítást, melyekből hármat épségben földre is kényszerítettek [72].

[30] No Drone Zone

9. ábra: A szíriai támadásban részt vevő egyik UAV.
(Forrás: [73])

Az ilyen támadások kivédésére különböző rendszereket fejlesztettek ki, melyek képesek elektronikai zavarás, fizikai eltérítés vagy megsemmisítés útján megakadályozni, hogy a támadó elérhesse a célpontot.

1.2 Felhő alapú számítástechnika bemutatása

1.2.1 Története

A számítógépek és számítógépes hálózatok fejlesztésével, fejlődésével a 20. század közepére elérhetővé vált, hogy több számítógépből lehetőség legyen egy nagyobb, szuperszámítógépet alkotni.

Az elosztott számítási rendszerek története egészen az 1960-as évekig nyúlik vissza, amikor először felmerült a fürt (klaszter) számítási rendszerek ötlete. Ez azt foglalta magába, hogy több, hasonló felépítésű, egymáshoz fizikailag viszonylag közel, például egy teremben található számítógépet egyenként ugyanannak az egyszerű feladatnak a megoldására programozták fel, és erre optimalizált algoritmusokkal egyes számításokat nagyságrendekkel gyorsabban, párhuzamosítva lehetett végrehajtani, melynek köszönhetően egyes lineáris futásidejű számítások logaritmikus nagyságrendre gyorsíthatók [74]. Az új felmerülő probléma itt a matematikai elmélethez képest gyakorlatban a kommunikációs költség, amit a párhuzamosan futó szálak szinkronizálása okoz.

Az 1990-es évek elején jelent meg a rácsszámítás, mint kifejezés, ami az elektromos rácshálózat analógiájára született. Ebben az esetben több, különböző hardverrel rendelkező, egymástól fizikailag távol elhelyezkedő gép kapcsolható össze, ezzel összeadva a számítási kapacitásukat. Ilyenkor az ütemezést, szinkronizálást egy keretrendszerrel oldják meg, aminek a dolgozó folyamatai a különböző fizikai gépeken futnak, és hozzáférést biztosítanak a gép erőforrásaihoz a központi ütemező gépnek, gépeknek. Ezeknek a gépeknek az összekapcsolása általában interneten keresztül valósul meg, és erőforrás igényes, általában tudományos számításokhoz veszik igénybe. A klaszter rendszerekhez képest itt a különböző szálak nem feltétlenül ugyanazt a feladatot látják el, így kibővítve a lehetséges alkalmazások körét bonyolultabb feladatokra.

Az évtized végén merült fel az ötlet a rács technológia továbbfejlesztésére, ahol bármilyen gép, bármilyen feladatot elláthat, dedikált erőforrással, és a gépek közti magas szintű hálózati redundanciával. Ezt gyakorlatban különböző virtualizációs technológiákkal oldják meg. Ez a felhő alapú rendszerek alapgondolata: bárki, aki felhő alapú szolgáltatást vesz igénybe, nem kell, hogy azzal foglalkozzon, hol vannak a bizonyos gépek fizikailag, vagy honnan van kiszolgálva az általa igénybe vett szolgáltatás, csak szolgáltatási szinttől függően virtuális erőforrást, vagy szolgáltatást bérel. A felhő alapú rendszerek legnagyobb előnye a magas szintű rendelkezésreállás és a logikailag korlátlanul bővíthető számítási vagy tárolási kapacitás, melynek leginkább a hardveres dimenzió szab határt. Röviden összefoglalva, felhő alapú rendszereken akár több fizikai számítógépre virtualizált számítási teljesítményt vagy szolgáltatást értünk.

Különleges felhasználói igények kielégítésére a felhő egyes számítási elemeit a maghálózatból a felhasználás helyéhez közel, a felhő „peremére” kitolva csökkenthetjük a hálózati késleltetést, ez a megközelítés az úgynevezett „edge computing”.

1.2.2 Általános felépítés

A legtöbb felhő alapú rendszer rendelkezik egy vagy több központi vezérlővel (controller), és az általuk vezérelt számítási egységekkel (compute). A számítási egységeken futnak a különböző feladatokat ellátó virtuális gépek, melyek állapotát a vezérlő folyamatai felügyelik.

Fizikai felépítésében érdekesség, hogy a felhő rendszereket általában adatközpontokba szervezik, hogy az adott zóna gépei közt minél kisebb hálózati késés legyen. Ezekben az adatközpontokban egyes esetekben akár teljesen zárt konténerekben találhatók a gépcsoportok, [75] fizikailag nem lehet hozzájuk férni, minden rendszer (folyadékhűtés, hálózat,

tápellátás) kívülről kapcsolódik a konténerhez. A konténerekben több száz gép is lehet, és mivel a konténer nem felnyitható, ha ezeknek bizonyos százaléka elhasználódik, a teljes konténert cserélik, nincs lehetőség a gépek egyenkénti szerelésére.

1.2.3 Képességek

A DoD stratégiája szerint [36] szoftver szolgáltatás (SaaS) esetén az ügyfelek alkalmazásokat használnak, amiket egy felhő alapú rendszer szolgáltat. Az alkalmazásokat kliens eszközökkel lehet használni, például web böngészőből vagy egyéb távoli elérési szolgáltatással. Az ügyfél nem rendelkezik az alkalmazást kiszolgáló felhő infrastruktúra fölött, amibe a hálózatot, szervereket, operációs rendszereket, tárolót értjük.

Platform szolgáltatás (PaaS) esetén az ügyfelek saját fejlesztésű alkalmazásokat telepíthetnek, konfigurálhatják a futtató környezetet, de a kiszolgáló hálózatot, szervereket, operációs rendszereket, tárolót nem menedzselik.

Infrastruktúra szolgáltatás (IaaS) esetén Az ügyfelek tetszőleges szoftvert futtathatnak a felhő rendszeren, felügyelhetik a hálózatot, szervereket, operációs rendszereket, tárolót és egyéb erőforrásokat. Nem menedzselhetik a kiszolgáló infrastruktúrát, de az operációs rendszert, tárolót és az alkalmazásokat igen. Esetlegesen néhány hálózati elemet, például tűzfalat kezelhetnek a rendszeren.

Adat szolgáltatás (DaaS[31]) esetén az ügyfelek adatokhoz férhetnek hozzá, földrajzi helytől függetlenül. A szolgáltatást az adatokhoz való hozzáférés jelenti, az ügyfélnek nincs szüksége az infrastruktúra felügyeletére vagy alkalmazásokra. Az OpenStack architektúrában az adatbázis képességet a „Trove” komponens segíti.

Tárhely szolgáltatás (STaaS[32]) az ügyfelek tárterületet bérelnek a szolgáltatótól, földrajzi helytől függetlenül hatékonyan kívánják elérni azt. A felhő alapú rendszerekre jellemző nagyfokú skálázhatóság miatt a kiszolgálható tárterületnek logikailag csak az infrastruktúra kapacitása szab határt.

1.2.4 Hozzáférési szintek

A felhő alapú rendszereket hozzáférhetőség alapján a következő csoportokba sorolhatjuk [36].

Publikus felhő esetén az ügyfelek erőforrás kapacitást (hálózat, számítási kapacitás, tároló) bérelnek egy szolgáltatótól. Ebben az esetben a szolgáltató nyújt minden szükséges eszközt, az ügyfeleket nem terheli létesítési, karbantartási feladat a rendszerrel kapcsolatban.

[31] Data as a Service
[32] STorage as a Service

A szolgáltató több ügyfelet is kiszolgál, akik ugyanabból a felhő rendszerből kapják az erőforrásokat. A legfontosabb biztonsági feladatot emiatt a publikus felhő rendszerekben a felhasználók környezetének megfelelő szintű elkülönítése jelenti amellett, hogy ez a jogos hozzáférést ne korlátozza.

Privát felhő esetén egy szervezet saját maga által kialakított és fenntartott felhő rendszert üzemeltet, bérelt, vagy maga által üzemeltetett erőforrásokon. Ennek a beruházási, fenntartási költsége jellemzően magasabb, mint a publikus felhőé, ellenben teljes kontrollt ad a hozzáférés fölött. Privát és publikus felhő közti választás esetén költség szempontjából érdemes szem előtt tartani a rendszer kihasználtságát (napi üzemóráinak számát) a szervezeten belül. Privát felhőt rendszerint olyan szervezetek alkalmaznak, akik belső, érzékenynek ítélt adatokat kezelnek; vagy célfeladatot látnak el a rendszerrel, például egyetemi vagy tudományos kutatási célokat, esetleg cégen belüli munkafolyamatokat szolgálnak ki, vagy támogatnak.

Közösségi felhő esetén egy hasonló igényekkel rendelkező szervezeteket vagy privát ügyfeleket, közösséget kiszolgáló rendszer átmenet a publikus és a privát felhő közt. Közösséget alkothatnak a hasonló céllal rendelkező szervezetek, akik például együttműködésben vesznek részt egy cégek közti kollaboráció során; vagy olyan ügyfelek, akik közös biztonsági követelményekkel rendelkeznek, esetleg egy szabvány vagy munkamódszer szerint kívánnak működni, esetleg együttműködni.

Hibrid felhő esetén a felsorolt felhő csoportok vegyíthetők szükség esetén. Bár a felhő rendszerek egyenként elkülönítve különböző hozzáférhetőséggel rendelkezhetnek, lehetséges az összekapcsolásuk például terheléselosztás vagy közösen használt alkalmazás kiszolgálása céljából.

1.2.5 Kockázati szintek csoportosítása

Az alacsony, közepes, magas kockázati szintű adatok elkülönítése, illetve kezelése külön biztonsági megfontolásokat igényel [36].

Egy szervezet, ha úgy ítéli meg, alacsony kockázati szintű adatait tárolhatja publikus felhőben, költséghatékonysági megfontolásokból, például a cég ismertető honlapját közzéteheti ilyen rendszer használatával a világhálón. Védelmi felhasználásban ez például jelentheti azt, hogy a napi feladatok ellátásában, amiknek kiesése nem veszélyezteti a műveleti biztonságot, különös megfontolás után, a bizalmasság, sértetlenség és rendelkezésre állás figyelembevételével engedélyezhető egy nyilvános felhő rendszer használata. Gondolhatunk példaként a Magyar Honvédség facebook oldalára.

Közepes kockázati szintű adatok felhőben történő kezelésénél jóval szigorúbbak a követelmények. Az ügyfelek megkövetelik az adatok felügyelhetőségét, biztosítékot, tartalék megoldásokat várnak el szolgáltatás kiesés vagy adatvesztés esetére. Ezen a szinten már csak komoly megfontolás után használhatóak publikus felhő rendszerek, de szigorúbb követelmények mentén. Polgári felhasználásban például gondolhatunk itt adatok biztonsági mentésére egy felhő alapú tárhelyen. A védelmi szférában példaként informatikai támogató rendszerek működtetésére, mint archiváló tárolásra, vagy adminisztratív alkalmazások kiszolgálására használható, amennyiben ezek kiesése vagy az adatok kompromittálódása nem veszélyezteti a műveleti biztonságot.

Magas kockázati szintű adatokat nem, vagy nagyon ritkán szokás publikus felhőben tárolni. Ennek oka a bizalmatlanság a külső szolgáltató felé, ezért ilyen minőségű adatokat főleg privát kialakítású felhőben szokás kezelni. Ezeknek az adatoknak a lehetséges kiszivárgása jellemzően veszélyezteti az üzletvitel, védelmi felhasználásban a műveletek biztonságát, ezért napjainkban ritkán bízhatók publikus felhő alapú rendszerekre.

1.2.6 Adatnyilvántartás

Az adatok nyilvántartása, címzése egy felhő rendszerben jellemzően teljesen elektronikusan, technológiai megoldásokkal történik. Az adatok fizikai, földrajzi elhelyezése annyiban érdekes kérdés, hogy a valamilyen szempontból összetartozó adatokat (például gyakran egyszerre igényelt, lekérdezett adatokat) érdemes fizikailag közel tárolni, közel szervezni egymáshoz, hogy az elérésük sebessége a lehető legoptimálisabb legyen. Ha viszont arra optimalizálunk, hogy (például védelmi célú alkalmazás során) az egyes rendszerelemek megsemmisülése, elérhetetlenné válása esetén se szakadjon meg a szolgáltatás, érdemes georedundánsan, egymástól fizikailag távol elhelyezni a rendszer egyes elemeit.

Az adatok elosztására jogi szempontból is érdemes figyelmet fordítani, hiszen nemzetközi rendszereknél megkötések vonatkozhatnak arra, hogy az egyes országok nemzetbiztonsági szempontból érzékeny adatait mely más országok területén szabad tárolni, illetve hálózatán átküldeni.

A felhő alapú rendszerekben az adatokat alapvetően objektum vagy blokk alapon tárolhatjuk.

Objektum alapon skálázható, elosztott tárolást valósíthatunk meg, az adatok több szerverre szétosztva tárolódnak az adatközpontban. Ha nagyobb tároló kapacitásra van szükség, egyszerűen újabb szervert helyezhetünk a tárolóba, és így skálázható a rendszer. Egy ilyen

alapú tárolást sok, ám olcsó szerveren érdemes megvalósítani. A kutatásaim során használt OpenStack architektúrában ezt a képességet a „Swift” komponens valósítja meg [75].
Blokk alapon perzisztens tárolókat kapcsolhatunk a szerverekhez. Ez a hagyományos lemezmeghajtók vagy képfájlok mintájára képzelhető el. Ezeket sebesség és teljesítményoptimalizálásra használhatjuk, például adatbázisok kiszolgálásakor. Ennek előnye az úgynevezett „snapshot[33]” kezelés, ami leegyszerűsítve a blokkok állapotának elmentését jelenti, ezzel biztosítva az adatok biztonsági mentését. A snapshotokból az adatok helyreállíthatóak szükség esetén, vagy felhasználhatók új blokk eszközök létrehozásakor. Az OpenStack architektúrában ezt a képességet a „Cinder” komponens valósítja meg [75].
Az erőforrások felügyeletét és a skálázást jellemzően egy telemetriaszolgáltatás automatikusan végzi, ezzel segítve a rendelkezésre állás védelmét. Az OpenStack architektúrában ezt a képességet a „Ceilometer” komponens valósítja meg [75].

1.2.7 Incidensek

A felhő alapú rendszerekkel kapcsolatban legtöbbet adatlopásokról vagy terheléses támadásokról hallhatunk, mint biztonsági események.
Az Európai Unió Hálózati és Információbiztonságért felelős Ügynöksége (ENISA[34]) kidolgozott egy keretrendszert a felhő alapú rendszerek incidens riportolására [77]. Ez útmutatást ad, hogyan kommunikáljuk, összegezzük az egy-egy támadásból nyert tapasztalatokat, és készítsünk új útmutatásokat a tanultak alapján.
Egy felhő szolgáltatás-kiesésekkel foglalkozó honlapon elérhető és nyomon követhető több biztonsági incidens [78]. Itt a rövid leírások közt láthatjuk, hogy sok kiesés oka főleg a szolgáltatás-megtagadást okozó terheléses támadások (például HBO, Telstra elleni 2014-ben), és a karbantartás közben felmerült hibák (például Twitter, 2014).
Az incidensek kinyomozására, visszakövetésére és ennek speciális kihívásaira a felhőkön belül külön iparág van alakulóban [79].

1.2.8 Alkalmazásuk

Mint már említettem, a felhő alapú rendszerek nagy előnye a szolgáltatások magas szintű elérhetősége, rendelkezésre állása és megbízhatósága.
A rendelkezésre állásra jellemző mérőszám a működés és kiesés időbeli aránya. Jellemzően egy felhő alapú rendszertől elvárt megbízhatóság az úgynevezett „ötkilences”, vagyis

[33] pillanatkép
[34] The European Union Agency for Cybersecurity

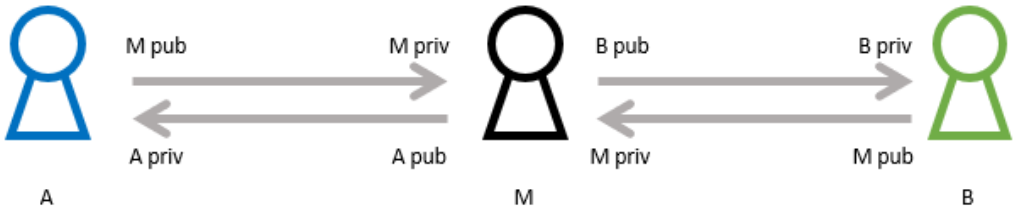
99,999%-ban elérhetőnek kell lennie a nyújtott szolgáltatásoknak. Ez gyakorlatilag azt fedi, hogy a szolgáltatásoknak évente körülbelül összesen 5 percnyi kiesése megengedett.
Ez a nagyfokú megbízhatóság az élet sok területén kívánatos, leggyakrabban a telekommunikáció vagy adatszolgáltatás területeken alkalmazzák jelenleg. Magyarország e-egészségügy portálja, az Elektronikus Egészségügyi Szolgáltatási Tér (EESZT) is felhő alapon működő szolgáltatás.
A legismertebb szolgáltatások internetes tárhelyet, közösségi média oldalakat, videómegosztó oldalakat, kereső oldalakat szolgálnak ki. A koncepció lényegét talán ott lehet megfogni, hogy ezen oldalak felhasználóinak nem érdeke tudni, hogy a szolgáltatás hátterében mekkora vagy mennyi szerver számítógép van, a fontos csak az, hogy éjjel-nappal elérhető legyen a szolgáltatás, és folyamatos legyen a felhasználói élmény (például ne akadozzon a megtekintett videó).

1.3 A nyilvános kulcsú infrastruktúra alapjai

A következő fejezet a nyilvános kulcsú infrastruktúra (másnéven publikus kulcsú infrastruktúra (PKI[35])) alapelveit, összetevőit és szereplőit mutatja be [S6].
A koncepció alapja az aszimmetrikus kulcsú titkosítás, egy matematikai eljárás, ami egy privát és publikus kulcsból álló kulcspárt foglal magába.
A kulcspár nyilvános fele szabadon közzétehető, a privát kulcsot viszont minden kommunikációs fél titkosan kezeli, nem osztja meg mással. A kulcspár különleges matematikai tulajdonságokon alapuló megkonstruálásának köszönhetően biztosítja azt, hogy az egyik kulcssal titkosított adatot csak a másik kulccsal lehessen visszafejteni – és fordítva. Ebből adódik az eljárás aszimmetrikus mivolta, szemben azokkal a hagyományos titkosító eljárásokkal, ahol ugyanazon kulccsal, jelszóval, jelmondattal történik a rejtjelzés és a visszafejtés is.
Amikor egy *A* és *B* fél kommunikál, A képes az üzenetét *B* nyilvános kulcsával eltitkosítani, és csak *B* képes a saját privát kulcsával visszafejteni azt. Amikor *A* aláír egy üzenetet a saját privát kulcsával, *B* képes *A* publikus kulcsának felhasználásával ellenőrizni, hogy tényleg *A* készítette az üzenetet és nem történt rajta módosítás az átvitel során.
A fenti eljárás csak akkor működik, ha a felek tudják biztosítani a nyilvános kulcsok teljesen biztonságos cseréjét, máskülönben egy harmadik *M* fél közbeékelődéses támadást vihet véghez (lásd 10. ábra), melynek során lehallgathatja, módosíthatja, meghamisíthatja az *A*

[35] Public Key Infrastructure

és *B* közötti üzenetváltásokat, miközben a szembenálló felek úgy érzékelik, a másik féllel kommunikálnak.



10. ábra: Közbeékelődéses támadás aszimmetrikusan titkosított csatorna esetén. (Az ábrát szerkesztette a szerző.)

A felek és publikus kulcsuk hitelességének biztosítására született meg a nyilvános kulcsú infrastruktúra koncepciója.

Egy mindennapi felhasználási esetben *A* lehet egy weboldalt böngésző felhasználó, aki biztonságokan kíván csatlakozni a weboldalhoz. *B* pedig lehet a weboldalt kiszolgáló webszerver. Ahhoz, hogy *A* biztosan tudja, *B*-vel kommunikál, *A*-nak megfelelő szintű bizalmat kell tudnia felépíteni a rendszer és az infrastruktúra kihasználásával. Ehhez *B* első körben legenerálja saját kulcspárját, melyből a privát kulcsot biztonságos helyen elektronikusan eltárolja, a publikus kulcsot pedig kiegészíti egyéb csatolt adatokkal, amik *B*-t azonosítják. Ez utóbbit nevezzük tanúsítvány aláírási kérelemnek (CSR[36]). Ezt aztán továbbítja egy tanúsító hatóság (CA[37]) vagy egy elkülönített nyilvántartó hatóság (RA[38]) felé, aki ellenőrzi *B* identitiását, ezesetben a *B* webes tartományát üzemeltető cég legitim mivoltát, illetve, hogy a CSR-t valóban ez a szervezet állította ki. Természetes személyek esetén a személyazonosság kerül helyben ellenőrzésre, például e-mail címhez tartozó tanúsítvány kiállításakor.

Ezután a CA aláírja *B* tanúsítványát a saját privát kulcsával. Ha *A* megbízhatónak ítéli ezt a CA-t, *A* ellenőrizni tudja, hogy a kapott tanúsítvány valóban *B*-hez tartozik, majd megkezdheti a biztonságos kommunikációs csatorna használatát.

Ám honnan tudhatja *A*, hogy megbízhat a CA-ban? A CA-kból álló láncolat végén található gyökér CA tanúsítványa különleges: önmaga által kerül aláírásra egy speciális ceremónia során (a hozzá tartozó privát kulcs biztonságos letárolásával együtt), melyet általában fegyveres őrök, tanúk és kamerák előtt, magas biztonsági szintű épületekben hajtanak végre, hogy biztosítsák az eljárás maximális megbízhatóságát. Ezt a műveletet érthető módon nagyon költséges lenne minden CA esetén megfelelően végrehajtani, részben ezért a CA-

[36] Certificate Signing Request
[37] Certificate Authority
[38] Registration Authority

kat egymást tanúsító láncolatba szokás rendezni. Ha nem lenne ez a láncolat, a gyökér CA-ra maradna az összes tanúsító eljárás terhe, így az internet számtalan weboldalát egyetlen szervezet kellene, hogy közvetlen tanúsítsa, gondoljunk csak bele, mennyi sorbaállással, várakozással járna ez az ügyfelek szempontjából, nem is beszélve arról, hogy a világon mindenki, aki e-mailes tanúsítványt szeretne, egy központi irodába kellene, hogy befáradjon… Egy esetleges privát kulcs kiszivárgás esetén annál több félnél szükséges újra generálni és tanúsíttatni a kulcspárt, minél közelebb van a gyökér CA-hoz a kompromittált CA az irányított fában, ezért érdemes szélességében is teríteni a tanúsítási fát.

A gyökér CA-k a fenti eljárásnak köszönhetően általában elismertek a nagyobb szoftvervendorok körében, így azok a szoftverükhöz (pl. webböngésző, operációs rendszer) csatolva telepítik az ügyfeleknél a gyökér CA tanúsítványokat. Így esetünkben *A* böngészője már tartalmazza a gyökér CA tanúsítványát, mellyel ellenőrizheti *B* tanúsítványát, ha azt közvetlen a gyökér CA írta alá. Amennyiben (és gyakorlatban ez az elterjedtebb) *B* tanúsítványát a fában mélyebben található CA írta alá, *A* legegyszerűbben végigjárhatja a láncot ettől a CA-tól egészen a gyökér CA-ig, miközben mindegyik CA tanúsítványát ellenőrzi, és végül, ha a gyökér CA megtalálható *A* böngészőjének „gyári" tanúsítvány gyűjteményében, tudhatja, hogy valóban *B*-t igazolja a lánc elején felmutatott tanúsítvány.

Ezen a ponton még mindig előfordulhatnak esetek, amikor *A* nem bízhat meg *B*-ben teljes mértékben. *B* tanúsítványa lejárhat vagy visszavonásra kerülhet. Ha *B* privát kulcsa kompromittálódik, kiszivárog, *B* kezdeményezheti a CA-jánál a tanúsítvány visszavonását a visszaélések megelőzése végett, majd kérvényezhet egy újabb tanúsítványt a korábban vázolt eljárást követve. Ezesetben a *B* kompromittált privát kulcsához tartozó tanúsítvány hozzáadódik a visszavont tanúsítványok listájához (CRL[39]), ami *A* számára is hozzáférhető. A CRL szabadon letölthető és végigböngészhető, ám mivel a lista mára számtalan tanúsítványból áll, kevésbé költséges, ha *A* inkább az online tanúsítvány státusz protokollt (OCSP[40]) használva kérdezi le kifejezetten *B* tanúsítványának állapotát.

Arra az esetre, ha *B* nem észlelné, hogy privát kulcsa kiszivárgott, a tanúsítvány lejárati ideje biztosítja, hogy a privát kulccsal történő visszaélés időben lekorlátolt legyen. Az érvényesség szokásos időtartama általában egy-két év, melynek kezdő és végdátuma az elektronikus tanúsítvány megfelelő mezőiben van feltűntetve, így ez akár helyben is ellenőrizhető.

[39] Certificate Revocation List
[40] Online Certificate Status Protocol

A PKI-vel összefüggő eljárások szigorú követelményeknek kell, megfeleljenek, melyeket az IETF [80] specifikációi és a nyilvános kulcsú kriptográfiai szabványok (PKCS[41]) foglalnak magukba.

1.4 Következtetések

A drónok elterjedésével és képességeinek fejlődésével új horizontok nyíltak meg a hobbirepülés szerelmesei és az ipari szereplők előtt. Sajnos a rosszakarók találékonysága ezt a területet sem hagyta érintetlenül, hamar előfordultak az első terrorcselekmények és katonai létesítmények elleni támadások saját építésű, vagy piacon elérhető polgári UAV-kkal is. Ez jól mutatja annak szükségességét, hogy a rendszerek távfelügyelete, nyomonkövethetősége és a távpilóták számonkérhetősége biztosított legyen.

A felhő rendszerek megjelenése generációs ugrást tett lehetővé a távközlési hálózatok területén, ám felhasználásuk nem csak ezen a területen terjedt el: szinte mindannyian használunk felhő alapú rendszereket adatink tárolására, az internetes keresés meggyorsítására vagy videónézésre, zenehallgatásra. Napjainkban már kormányzati szinten is találkozhatunk felhő szolgáltatásokkal, és az utóbbi évek biztonsági incidensei rávilágítottak, hogy ezek biztonsága különleges megfontolást igényel, mind a személyes adatok védelme, mind a kritikus infrastruktúravédelem szempontjából.

Kutatásaimmal párhuzamosan attól független felhő alapú UAV-kat kezelő rendszerek is megjelentek a drónok állami távfelügyeletének vagy távirányításának céljával [1] [2] [3]. Mindegyik rendszer esetén megfigyelhetjük a földi és légi alrendszer elkülönülését, illetve a több drón központi kezeléséből adódó felügyeleti és ütközéselkerülési lehetőségeket. A technológiai tendenciákat figyelembe véve elmondható, hogy a Mission as a Service szolgáltatások koncepciója jövőbemutató, ám a jelen technológiai lehetőségei mellett már elérhető megoldás, mely esetén fontos a biztonság fizikai, adminisztratív, személyi és elektronikus dimenzióinak szem előtt tartása.

[41] Public Key Cryptography Standards

2 A KÍSÉRLETI FELHŐ ALAPÚ UAS FELÉPÍTÉSE

2.1 Követelmények

2.1.1 Tervezési megfontolások

A kitűzött cél egy felhőből irányított pilóta nélküli légijármű rendszer megvalósítása volt, nyílt technológiák lehető legnagyobb arányban történő felhasználásával [S3]. Kutatásaim kezdetekor az informatikai felhő fogalma főként tárhelyszolgáltatóként élt a köztudatban, a civil drónok pedig leginkább kézi távirányítóval vagy wifin keresztül, mobilalkalmazással voltak irányíthatók. Az általam elkészített megvalósítás esetén ezért a manuálisan reptetett vagy autonóm működésű, komolyabb, kereskedelmi és állami célú UAS-k reprezentálása a volt cél.

Ennek másik oka, hogy a játék, hobbi és verseny UAV-k szórakoztatást célzó „feladatköre" miatt az egyszerű rádiós összeköttetést (egyelőre) nem életszerű felhő alapú irányítással kiváltani. A hobbi UAV-k repülési adatainak (eseti légterének, vagy útvonaltervének) felhőbe integrálása általában kézzel, a repülés végrehajtását megelőzően történhet meg, például a MyDroneSpace appon keresztül, ahogy azt a jogszabály [81] is előírja, illetve a légijárműre felszerelt külső nyomkövető egység biztosíthatja a digitális láthatóságot.

A kommunikációs protokoll kiválasztásánál is a fenti felhasználási eseteket tartottam szem előtt.

A felhő rendszer tulajdonságai közül a legkülönlegesebbnek mondhatókra koncentráltam, melyek a hagyományos kiszolgálókhoz képest várhatóan kivételes megbízhatóságot nyújthatnak egy Mission as a Service szolgáltatás esetén, az infrastruktúra dinamikus és rugalmas alakításával.

2.1.2 Általános funkciók

A repültetések során a térképes felhasználói felület a következő alapvető képességekkel kell, hogy rendelkezzen:

- Az UAV-k helyzetének megjelenítése.
- Egy vagy több UAV kijelölése.
- Útvonalterv vagy úticél grafikus tervezése, UAV-kra való feltöltése vagy törlése.
- Rotorok távoli élesítése és biztosítása.
- UAV-k autonóm fel- és leszállítása.
- Váltás kézi irányítás vagy autonóm működés között.

2.1.3 Vízszintes skálázás

A felhő rendszerek egyik újdonsága (a rács és fürt számítási rendszerekhez viszonyítva) a nagyfokú rugalmasság. Ezt a skálázhatóság, skálázódási tulajdonság biztosítja.

A vízszintes skálázás jelentése több párhuzamos virtuális gép dinamikus indítása (vagy leállítása) a felmerülő szükségletek alapján – szemben a függőleges skálázás elvével, amikor egy meglévő virtuális gép erőforrásait növeljük (vagy csökkentjük) az igényeknek megfelelően.

A feladat megvalósítása során a vízszintes skálázás alkalmazására és tesztelésére fókuszáltam. Ennek oka, hogy a legtöbb mai felhő architektúra élő rendszeren, megszakítás nélkül csak korlátozottan képes extra erőforrásokat a futó virtuális gépekhez rendelni. OpenStack esetén például élő virtuális gépek migrációjával oldható meg ez a fajta feladat, amikor a rendszer létrehoz egy nagyobb kapacitású virtuális számítógépet (VM[42]), majd a futó szolgáltatást az új gépre migrálja, és a régit leállítja. Ez gyakorlatban sokszor a szolgáltatás pár másodperces megszakadásával jár, ami esetünkben megengedhetetlen.

2.1.4 Antiaffinitás

Néhány felhasználás esetén kívánatos, hogy a virtuális gépeket egymáshoz fizikailag minél közelebb indítsuk, lehetőleg egy számítógépen, hogy ezzel például köztük a hálózati késleltetést csökkentsük. A virtuális gépek elhelyezésének ilyen megközelítését, miszerint automatikusan „szorosan” egymás mellett kerülnek indításra, a felhő affinitási tulajdonságának nevezzük.

Esetünkben inkább ennek pont az ellentéte a cél: hogy földrajzilag minél jobban terítve legyenek az erőforrások, ha lehet, minél távolabb kerüljenek egymástól a VM-ek, akár külön adatközpontokba is. Ez lenne az antiaffinitás tulajdonsága. Ezzel biztosíthatjuk, hogy mikor az egyik szerverteremben áramszünet van, vagy akár (például katonai felhasználás esetén) fizikailag megsemmisül a telephely, esetleg megszakad vele a kapcsolat, a többi adatközpont vagy számítógép át tudja venni a szerepét, a szolgáltatás felhasználók által észlelhető megszakadása nélkül. Ez adja a rendszer robusztusságát, vagyis a felhő túlélőképességét.

2.1.5 Tartós munkamenetek

A terheléselosztó komponens végzi például az UAV-k által küldött üzenetek VM-ek közti elosztását. A hálózati kapcsolatok kezelésének megkönnyítése szempontjából érdemes az

[42] Virtual Machine

egyes UAV-kat mindig ugyanahhoz a virtuális géphez „sorsolni”. Komoly erőforrásokat spórolhatunk meg a hálózati kapcsolat újbóli felépítésének vagy lebontásának kihagyásával, és a meglévő kapcsolat újbóli felhasználásával az egyes üzenetek fogadása esetén, hiszen a viszonylag kis méretű MAVLink 1.0 üzenetek hossza összemérhető ezen üzenetek hosszával.

2.1.6 Elterjedt irányítási és UAV azonosítási protokollok

Az egyes drónok rendeltetésétől függően több megközelítés létezik protokollok szempontjából. A hagyományos 2,4 GHz távirányítóval irányított játékdrónok és modellrepülőgépek impulzusszélesség-modulációt alkalmaznak (PWM[43]). A nagy sebességgel repülő, videojelet is lesugárzó, belsőnézetes (FPV[44]) versenydrónok fedélzeti rendszerei különböző, gyártó-specifikus protokollokat támogathatnak, [82] mint például:

- FrSky D8;
- FrSky D16;
- FlySky AFHDS;
- TBS Crossfire;
- Spektrum DSMX (újabb);
- Spektrum DSM2 (régebbi);
- Futaba FASST.

Okosjárművek esetén gyakran alkalmazzák a vezérlőközeli hálózat (CAN[45]) protokollját, mely decentralizált kommunikációt tesz lehetővé különböző komponensek, például a központi számítógép és a motorvezérlők közt [83]. Egyes dróngyártók támogatják az ilyen rendszerekbe történő integrációt.

Napjainkban az autonóm működésre képes, gyakran saját építésű drónok esetén azonban elmondható, hogy a MAVLink protokoll különböző verzióinak használata a legelterjedtebb [84]. Ez a bináris protokoll eredetileg kisméretű UAV-k rádiós kapcsolaton történő irányítására lett optimalizálva. Napjainkra kiegészítésre került szárazföldi és víz alatti járművek, illetve egyes hasznos terhek (például csörlő, hidraulikus permetező, gimbal, szervók stb.) irányítására szolgáló funkciókkal is.

[43] Pulse Width Modulation
[44] First Person View
[45] Controller Area Network

A MAVLink egyes hiányosságainak kezelésére, a hálózati kommunikáció egységesítésére és az azonosító üzenetek formátumának szabványossá alakítására később megjelent az OpenDroneID koncepciója.

2.1.6.1 MAVLink 1.0

A MAVLink 1.0 üzenetek bájtszintű felépítését az 1. melléklet mutatja.

A rendszerazonosító (`sysid`) tartománya láthatóan elég szűkös, a kitüntetett nullás azonosító szórt üzeneteknek van fenntartva, a tartomány vége pedig általában a földi állomások azonosítására szolgál. Így egy kapcsolaton maximum 254 légijárművel tartható fenn kommunikáció, ez elég erős limitáció a regisztrált pilóta nélküli járművek számára vonatkozóan. A komponens azonosító (`compid`) az egy UAV-n helyet kapó alrendszerek, például MAVLink-képes robotpilóta, kamera, gimbal vagy GPS azonosítására szolgál.

Az Amerikai Légierő berkein belül született egy dolgozat, ami a MAVLink 1.0 biztonsági hiányosságaira alapozva mutat be támadási módszereket [29].

A szerző a helyi és távoli hozzáférésre, közbeékelődéses támadásokra (lehallgatás, eltérítés) fókuszál, illetve szolgáltatás megtagadás jellegű támadások lehetőségeire.

Egy másik, belga kutatócsapat fuzzing technikával keresett és talált hibákat a protokoll megvalósításában [85]. A cikk kiadásáig nem végeztek mélyebb behatolástesztelést a talált hibák mentén.

2.1.6.2 MAVLink 2.0

A MAVLink 2.0 üzenetek bájtszintű felépítését a 2. melléklet mutatja.

Kutatásom szempontjából talán a legfontosabb különbség az új (opcionális) aláírás mező az üzenet végén, melyet részleteiben a lenti táblázat ír le.

Mező	**Leírás**
Kapcsolat azonosító (8 bit)	A kapcsolat azonosítója melyen a csomag közlekedik.
Időbélyeg (48 bit)	Időbélyeg 10 mikroszekundum osztással 2015 január 1 óta. Szigorúan monoton növekvő, üzenetenként egy kapcsolatra értelmezve. Ennek következménye, hogy az időbélyeg minimum 100 000 csomag/másodperc csomagküldési intenzitás esetén a valós idő elé (a jövőbe) torlódik. (A gyakorlatban általában jóval alacsonyabb az intenzitás.)
Aláírás (48 bit)	48 bitnyi SHA256 aláírás, a teljes csomagra, az időbélyegre és egy titkos kulcsra számítva.

1. táblázat: A MAVLink 2.0 csomagok aláírás sorának felépítése.

(A táblázatot fordította és szerkesztette a szerző. Forrás: [86])

Az aláírás tartalmaz egy szimmetrikus előre kiosztott titkos kulcsot (PSK[46]), aminek a kulcscseréje titkosítatlanul történik. Ennek megfelelően a kulcscserét mindenképp megbízható kapcsolaton át kell végrehajtani a földi alrendszer és a robotpilóta egység között. Ezt a hivatalos ajánlás szerint USB kapcsolaton a legegyszerűbb kivitelezni [87].

Az aláírás mező bevezetésével a J. Marty által leírt támadások egy része kivédhető lett. Az irányítás eltérítése például a szekvencia szám, időbélyeg és titkos kulcs megfelelő fabrikálása nélkül nem kivitelezhető. A SHA256 napjainkban széles körben elfogadott és alkalmazott algoritmus, például a NIST ajánlása szerint is megbízhatónak számít [88]. Az algoritmus erősségén ebben az esetben ront, hogy a MAVLink 2.0 csomagok aláírásakor az eredetileg előállított 256 bites aláírásnak csak az első 48 bitjét tartja meg a protokoll, ezzel gyengítve az eredeti hasítófüggvény magas ütközésellenálló tulajdonságát, részleteket lásd a 7.3 fejezetben.

Egy másik, amerikai kutatókból álló csapat ugyancsak vizsgálta a MAVLink 1.0 és 2.0 sebezhetőségeit [89]. A 2.0 verzió esetén a biztonságosabb kulcscserét, illetve az újrajátszásos támadások elleni védelmet emeli ki, mint fejlesztendő pont, illetve egy titkosított kapcsolat kialakítását.

2.1.6.3 OpenDroneID

Az OpenDroneID projekt célja egy olcsó, de megbízható jeladó képesség megvalósítása drónok számára, hogy azok a vevő egységek hatókörén belül azonosíthatók legyenek [90]. Az aktuális specifikáció hagyományos Bluetooth szórt csomagokon és a Bluetooth 5 (nagy hatótávolságú) kiterjesztésein alapul, emellett wifi alapú megvalósítás is elérhető Neighbor-aware Network protokollal.

A megoldás segíti a polgári repülés pilótás és pilóta nélküli résztvevőit, a rendvédelmet, a kritikus infrastruktúra védelmet és a légi forgalmi irányítás munkáját a megfelelő szintű helyzetismeret elérésében.

A kiküldött csomagok statikus és dinamikus üzenetek csoportjába sorolhatók. A statikus adatok ritkábban kerülnek kiküldésre a dinamikus adatokhoz képest. Az üzenetek „kapcsolat nélküli” üzenetek, nem igényelnek visszajelzést, jóváhagyást a fogadó oldaltól.

Míg a wifi és hagyományos Bluetooth hatótávolsága nagyjából 150 m-re korlátozódik a terepviszonyoktól és a rádiós interferenciától függően, a Bluetooth 5 hatótávolsága akár 240 m is lehet. Az OpenDroneID szórt Bluetooth-ra vonatkozó specifikációjának célja, hogy a szórt üzeneteket egyszerű vevőállomásokkal (például régebbi okostelefonokkal) is

[46] Pre-Shared Key

lehetőség legyen fogadni, a nagy nyereségű antennával felszerelt dedikált földi állomások és modern okostelefonok mellett – melyek képesek kihasználni a legújabb szabványok által nyújtott nagyobb hatótávolság előnyeit.
A projekt nyilvános specifikációval és példakódokkal támogatja a közösséget a specifikáció gyors megvalósításában.
A MAVLink protokoll legújabb verziójában már elérhető az OpenDroneID egy kezdeti megvalósítása, amely – ha elkészül –, remélhetőleg segít feloldani a MAVLink jelenlegi technológiai korlátait a légijárművek és távpilóták azonosítása terén.

2.2 A rendszer technikai megvalósítása

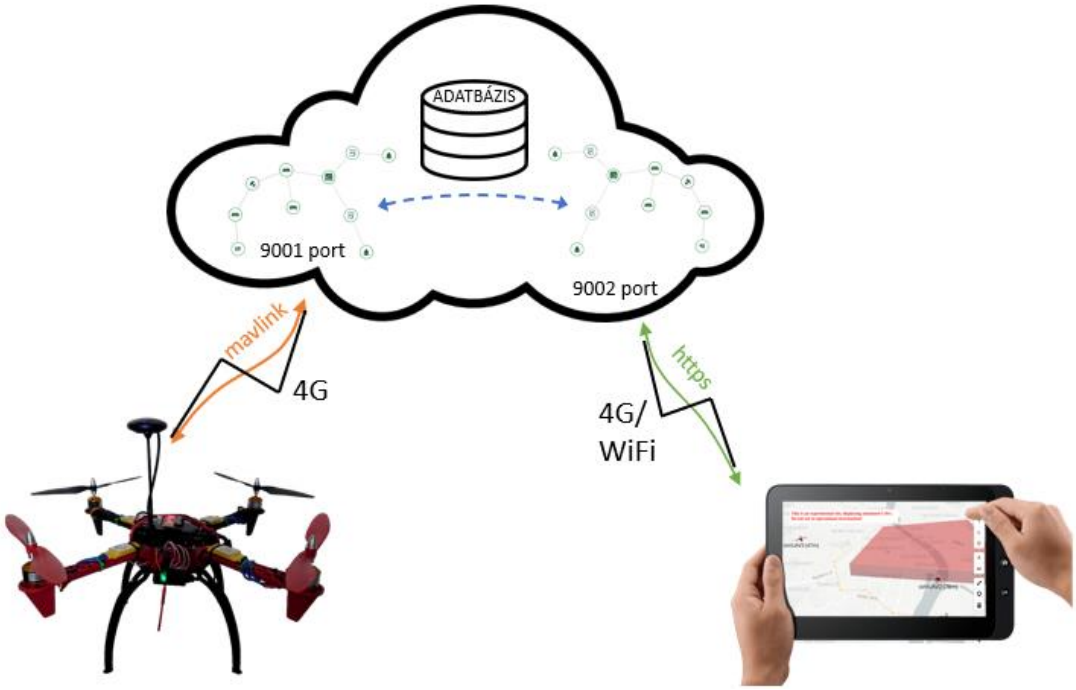
2.2.1 Áttekintés

A rendszer felépítését tekintve elkülönül a repülés tényleges kivitelezéséért felelős légi alrendszer, illetve az ezt felügyelő és parancsokkal irányító földi alrendszer. A földi alrendszeren belül elkülönül a központi adatbázist, illetve a drón és távpilóta interfészeket működtető felhő rendszer és a felhasználó böngészőjében futó térképes megjelenítő felület. Általánosságban elmondható, hogy az egyes feladatkörök jól körülhatárolhatók a rendszeren belül, azok meghatározott interfészeken kapcsolódnak egymáshoz.
A prototípus rendszer magját egy OpenStack alapú felhő rendszer adja [S5]. Az UAV-k irányába átvitelvezérlési protokoll (TCP[47]) alapú MAVLink 1.0 szerver szolgálja ki a kapcsolatot, illetve menti adatbázisba a kapott adatokat, miközben az UAV felé küldött parancsokat is továbbítja.
A kiszolgált honlap célja egy szemmel könnyen áttekinthető, térképes megjelenítés, ami egyéb repüléstervezést segítő rétegekkel is kiegészíthető (például NDZ-k, időjárási előrejelzés, épületek), integrált küldetéstervezési funkcióval, akár több UAV együttes kijelölésével. Mindezt okostelefonon vagy számítógépen, platform független módon.
A tényleges megjelenítendő adatokat a korábban említett adatbázisból nyeri a honlap, a felületen küldetéstervezési lehetőség mellett egyedi vezérlő elemek is helyet kaptak, az egyes akciók (például fel- és leszállás) végrehajtására.
A levegő-föld adatátvitel digitális (csomagkapcsolt) kapcsolattal valósul meg, bár a repülő eszköz a hagyományos, 2,4 GHz frekvenciájú távirányító egységgel is fel van szerelve, amellyel vészhelyzet esetén átvehető, felül írható az irányítás. Az teszteszköz forgószár-

[47] Transmission Control Protocol

nyas, kvadrokopter felépítésű, bár a robotpilóta egységen futó firmware frissítésével, merevszárnyas eszközzel is kompatibilissé tehető a rendszer.

A koncepcióhoz a 11. ábra ad áttekintést.



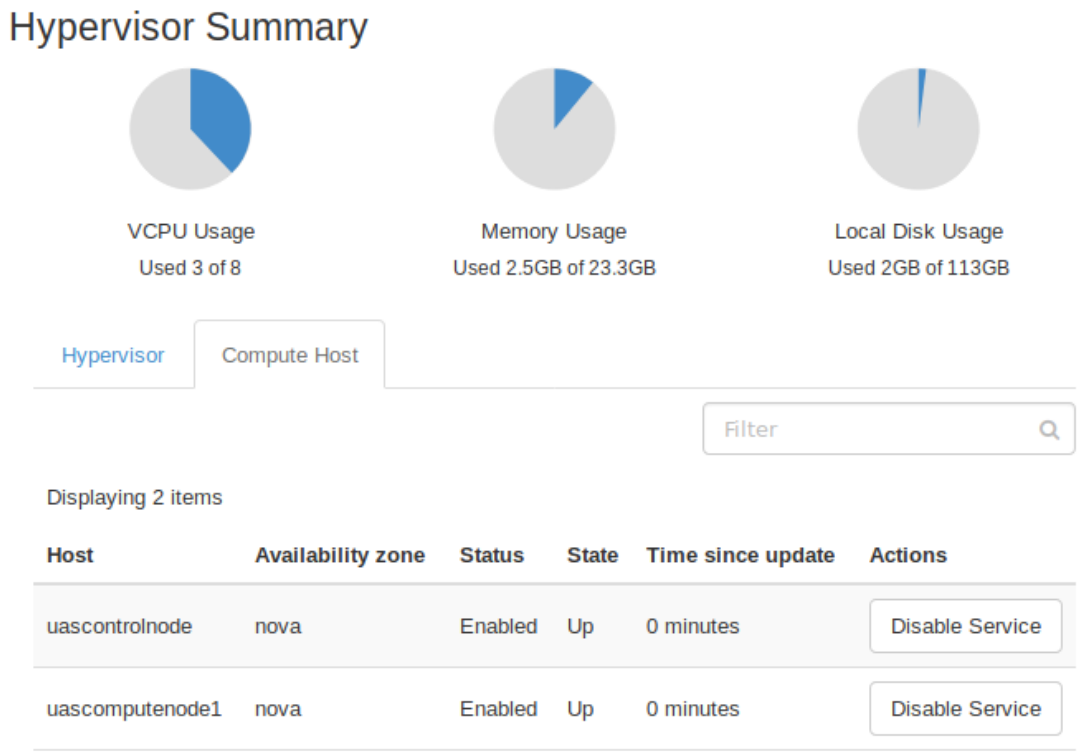
11. ábra: A komplett rendszer sematikus ábrája.
(Készítette a szerző.)

Az irodalmi áttekintésben olvasható indoklásnak megfelelően és a felhő rendszerek nevezéktanához történő illeszkedés céljával a rendszert és a kapcsolódó szolgáltatást az újonnan definiált Mission as a Service kategóriába sorolom.

2.2.2 Földi alrendszer

2.2.2.1 Privát felhő

Felhő infrastruktúrát kialakíthatunk akár otthon a számítógépünkön, számítógépeinken is, hiszen a virtualizációs technológiának köszönhetően a hardver platform maga kevéssé lényeges, nem szükséges hozzá drága célhardver megléte. Jelen megvalósításban két különböző típusú notebook számítógépre lett kiterjesztve a felhő. Így, ahogy a 12. ábra is mutatja, összességében 8 virtuális processzor szál és nagyjából 24 GB memória áll rendelkezésre. Igény szerint bármikor több további számítógép csatlakoztatható a hálózathoz, illetve a rendszerhez.



12. ábra: Több számítógép – egy irányító és egy tisztán számítási feladatú elem a rendszerben. Összesen 3/8 virtuális processzort, 2,5/23,3 GB memóriát és 2/113 GB tárhelyet vesz igénybe az aktuálisan futó rendszer.
(A képernyőképet készítette a szerző)

2.2.2.2 Openstack infrastruktúra

Az OpenStack az egyik legelterjedtebb nyílt forrású felhő megoldás, ami különböző fantázianevekkel illetett „projektekből” épül fel [75]. Ezek közül a következőket alkalmaztam a fejlesztés és telepítés során:

- erőforrás szervezés („Heat”);
- webportál („Horizon”);
- számítási erőforrások („Nova”);
- blokkos tároló („Cinder”);
- objektum tároló („Swift”);
- hálózat („Neutron”);
- képfájlok („Glance”);
- azonosítás („Keystone”);
- monitorozás („Ceilometer”);
- munkamenet („Mistral”);
- metrika, statisztika („Gnocchi”);
- riasztás („Aodh”);

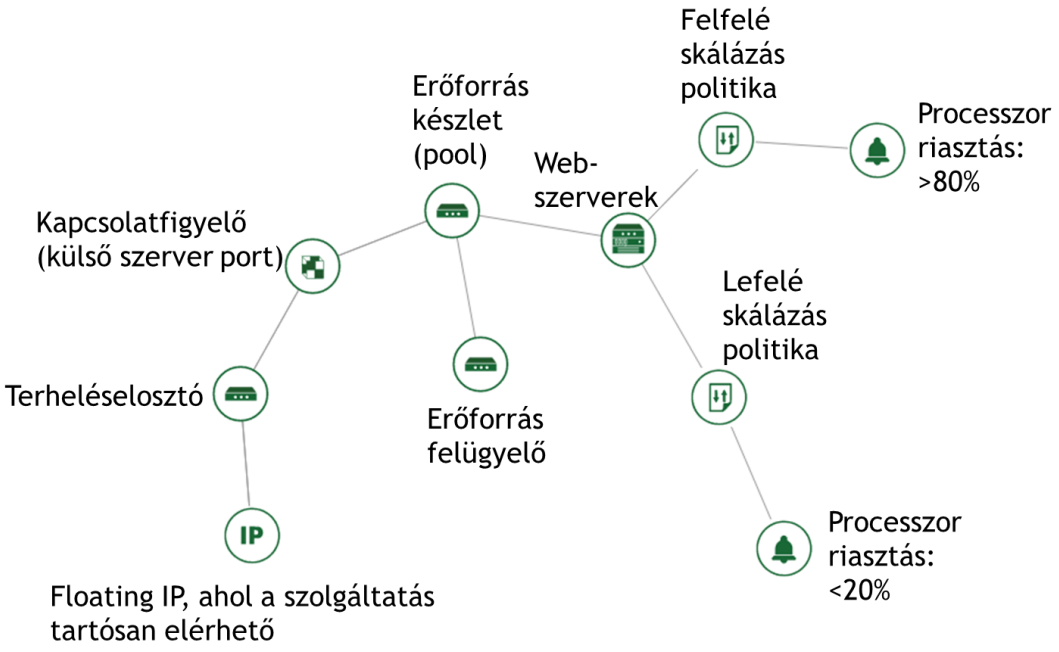
- terheléselosztás („Octavia”);
- eseménysor („Zaqar”).

A felhő rendszerek egyik legkívánatosabb tulajdonsága a magas fokú rendelkezésre állás, vagy HA[48]. Ehhez szorosan kapcsolódó fogalom az LB[49] vagyis terheléselosztás. A szolgáltatás külső hozzáférési pontjait valamilyen HA proxy megoldás mögé szokás rejteni, ami alapjaiban egy robusztus átjárót jelent a külvilág felé. A proxy mögött több párhuzamosan dolgozó folyamat között osztjuk el a számítási feladatokat, amik képesek hatékonyan osztozni a közösen használt erőforrásokon. Ez a felhőben futó szolgáltatások tervezésénél az egyik legfontosabb szempont. Ezzel a módszerrel a rendelkezésre állást olyan magas szinten garantálni lehet, hogy általában a felhő kiszolgálók „ötkilences”, vagyis 99,999% rendelkezésre állást vállalnak a szerződésekben. Ez évente mindössze 5 perc megengedhető szolgáltatás-kiesést jelent.

Jelen rendszer egyik oldalon a térképes felületet és a hozzá tartozó „REST” koncepciónak megfelelő alkalmazásprogramozási felületet (API[50]) szolgálja ki, a másik oldalon pedig egy `pymavlink`[51] könyvtáron alapuló szervert.

A párhuzamos futásra optimalizált dolgozó szálakat tetszés szerint indíthatjuk, vagy leállíthatjuk a leterheltség függvényében. Ezt nevezzük horizontális skálázásnak. Jelen megvalósítást az OpenStack Heat erőforrás szervező projektjét használva állítottam össze. Egy előre elkészített sablonnal konfigurálhatjuk az erőforrásainkat. A drónok irányába MAVLink kapcsolatot adó interfészt kiszolgáló, automatikusan skálázódó erőforrások logikai kapcsolata a 13. ábrán figyelhető meg. (A 20 és 80%-os limitek részleteit lásd a 4.2.2 fejezetben.)

[48] High Availability
[49] Load Balancing
[50] Application Programming Interface
[51] Python MAVLink



13. ábra: Önskálázó OpenStack konfiguráció.
(Az ábrát szerkesztette a szerző.)

Az első komolyabb kihívással a processzor metrikák elérése során találkoztam: a legfrissebb Ceilometer verziókban már nem támogatott a `cpu_util` metrika (és egyéb aggregált metrikák sem), ami processzor használatot adná vissza százalékos formában. Kizárólag a processzoridő érhető el szigorúan monoton növekvő formában. Ezt a metrikát nem sikerült a Gnocchi komponenssel reprodukálni, így jobb híján egy korábbi Ceilometer verzióra álltam vissza.

Hasonlóan kívánatos tulajdonság lehet a párhuzamosan dolgozó virtuális gépek önjavítása, vagyis hiba esetén érzékeljék az incidenst és indítsák újra a szolgáltatásukat „tiszta lappal”. Erre is sikerült egy konfigurációt összeállítani. Viszont amikor ötvözni próbáltam az önjavítást az önskálázással, versenyhelyzet alakult ki skálázás esetén: lefelé skálázáskor, amikor a fölöslegesen dolgozó virtuális gép törlődik, a törlés hatására a gép újra indítja magát, hiszen az önjavításnak ez lenne az egyik célja. Ennek következtében a skálázó újfent próbálkozik a virtuális gép felszabadításával, amire az újra megjavítja magát. Ezt a problémát kereskedelmi felhő megoldásokban inkább kiegészítő komponensekkel oldják meg [91]. A kísérleti rendszer esetén végül az egyszerű skálázást hagytam meg, hiba esetén a többi gép terhelése megnő, és a következő kiértékelési időpontban (jelenleg 5 percenként) indul egy újabb példány. Sajnos a hibás virtuális gép kézzel történő eltávolításig beragadt állapotban marad.

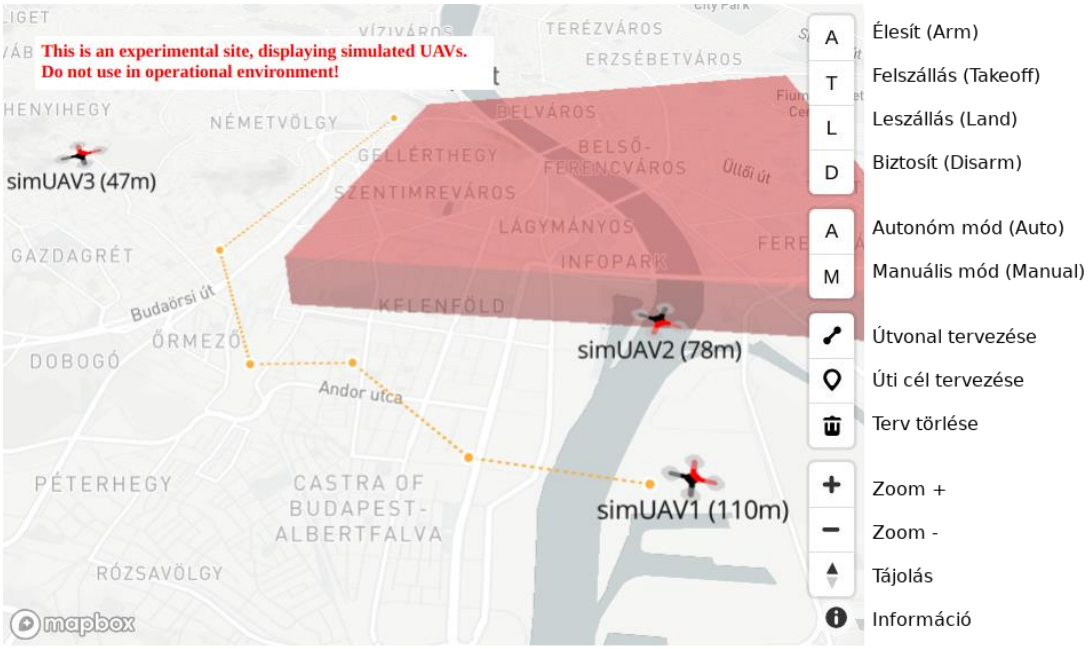
2.2.2.3 *Devstack telepítő*

Az OpenStack-es infrastruktúra telepítéséhez DevStack-et alkalmaztam. Ennek sajnos limitációja, hogy a fizikai gépek újraindítása esetén a Neutron hálózatkezelő szolgáltatás nem képes újra helyesen elindulni. A két notebookot energiagazdálkodási okokból nem tartottam 24/7 bekapcsolva, így a tesztelési időszakokban egy szkripttel mindig újra telepítettem az egész OpenStack környezetet, ez nagyjából gépenként 20 percet vesz igénybe.

A MAVLink protokoll használatát segítendő, C/C++ és Python nyelven is elérhető nyílt forrású könyvtár a GitHubon. A `pymavlink` Python könyvtár esetén limitáció, hogy csak egy szerver és kliens képes egy kapcsolaton kommunikálni, egy időben (a két végpont a földi állomás és a légijármű). A `pymavlink` forráskódjából kiindulva sikeresen újraírtam a hálózati socket kezelés kódrészletet, hiszen korábbi formájában nem volt „felhőbarát” a működése, a könyvtár így készenállt a több csatlakozó drón kezelésére. A valós élethelyzetek későbbi szimulálásához létfontosságú volt, hogy a kiszolgáló egy hálózati portján több légijármű is tudjon kommunikálni.

2.2.2.4 *Mapbox térkép*

A felhasználói oldalon a térképes megjelenítést MapBox keretrendszerrel valósítottam meg, ahogy a 14. ábrán is látható. A megjelenés alap esetben felülnézetes 2D, jobb egérgombbal 3 dimenzióban is forgatható.



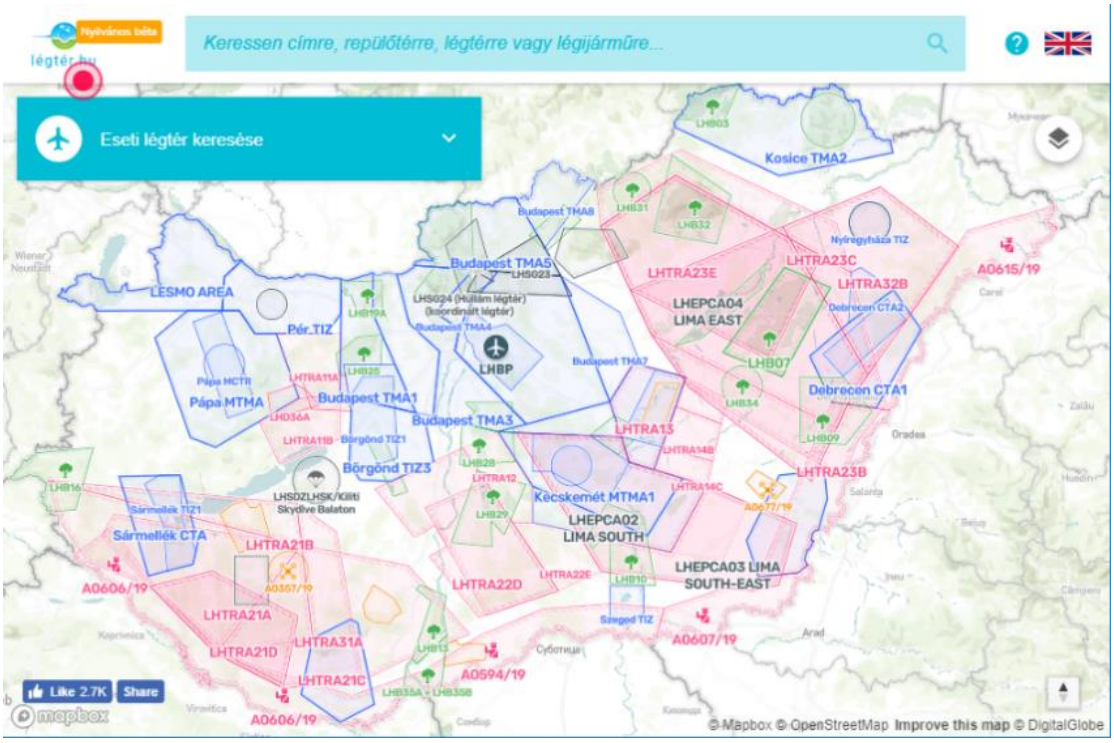
14. ábra: A térképes felhasználói felület, tervezett útvonallal és minta NDZ-vel.
(A képernyőképet készítette a szerző.)

A felhasználónak lehetősége van az UAV-k számára küldetések (útvonalak, úti célok) megtervezésére/törlésére, a repülő eszközök élesítésére/biztosítására, fel/leszállítására, illetve autonóm vagy kézi irányítású módba kapcsolására.

A vörös színű test egy NDZ-t hivatott reprezentálni, gyakorlati funkciója nincs, csak a megjelenítést teszteltem vele. Továbbá lehetőség van a nézetet nagyítani és kicsinyíteni, illetve észak irányba tájolni a korábban elforgatott térképet. Nagyobb mértékű zoom esetén, ahogy a 15. ábra is mutatja, az épületek is kiemelkednek a felszínből, segítve a tereptárgyak, akadályok térbeli áttekintését.

15. ábra: Épületek 3D nézetben.
(A képernyőképet készítette a szerző.)

Ezen térképes keretrendszer kiválasztásának egyik oka, hogy a Légtér.hu térképes megjelenítője is MapBoxon alapul (lásd 16. ábra), esetleges keretrendszerbeli hibák feltárása esetén közvetlen hozzá tudok járulni ennek a rendszernek a jobbá és biztonságosabbá tételéhez is.



16. ábra: A Légtér.hu térképes felülete.
(A képernyőképet készítette a szerző.)

Érdemes megjegyezni, hogy a MapBox legtöbb függvényhívása földrajzi hosszúság-szélesség párokkal dolgozik, amíg a MAVLink protokoll szélesség-hosszúság párokkal, fordított sorrendben. Ezek véletlen felcserélése esetén az UAV útvonala Magyarország helyett leginkább Szaúd-Arábiába fog vezetni.

Az UAV-k utolsó ismert pozíciójának térképes megjelenítése segíthet az eltűnt vagy lezuhant eszközök felkutatásában is.

2.2.3 Légi alrendszer

A 17. ábrán látható repülő eszköz alapját egy DJI F450 „Flame Wheel” jellegű keret adja. A kiegészítő lábak lehetővé teszik különböző kiegészítő hasznos terhek (szenzorok, nyomkövető jeladók, kamera stb.) felszerelését a keret alá. A keret belsejében kap helyet az Ardupilot APM[52] 2.6 típusú robotpilóta egység, és a 2,4 GHz másodlagos távirányító modul, illetve a nagy kapacitású lítium akkumulátor. A keret tetején került elhelyezésre egy akkumulátor feszültség figyelő modul, illetve az elsődleges adatkapcsolatért felelős okostelefon. Az okostelefon USB OTG kábellel kapcsolódik az APM-hez, amin keresztül MAVLink protokoll segítségével tudja utasítani a robotpilótát, illetve adatfolyamokhoz fér hozzá a GPS, gyorsulásmérő, iránytű, giroszkóp és egyéb szenzorok irányából. A GPS

[52] ArduPilot Mega

antenna, illetve külső iránytű modul egy dönthető árbocon kap helyet az elektromágneses interferencia kiküszöbölése végett.

17. ábra: A megépített prototípus UAV.
(A képet készítette és szerkesztette a szerző.)

A teljes rendszer akkumulátorral és mobiltelefonnal együtt nagyjából másfél kilogramm, így kiegészítő hasznos terheknek körülbelül fél kilogramm marad az UAV-ra kötött (a repültetések idején érvényes) biztosítás-konstrukció és az akkori jogszabályok által maximált két kilogrammos felszálló tömegből.

Első kérdésként felmerülhet a kézenfekvő kérdés, a mobil hálózat lefedettsége földfelszín felett. Egy, a 2019-es Drón Konferencia és Expo [92] rendezvényen elhangzott előadás részben érinti a témát, az elhangzottak alapján sikeres méréseket végeztek 1000 láb magasságig egy hasonló, de mobilhálózat alapú helymeghatározással kísérletező projekt keretein belül. Az előadó nem hivatalos álláspontjában kimondja, hogy korábbi tapasztalatai alapján 4500 láb magasságban is képes volt mobilnet kapcsolaton át kommunikálni. Emellett megemlíti későbbi lehetőségét, hogy egy telefonos operátorral együttműködve „kinyittatnak” felfelé nagyjából egy tucat bázisállomást, ezzel az LTE lefedettséget legalább FL660-ig kiterjesztik. Megjegyzi, hogy földközelben sokkal nagyobb a mobilhálózaton a rádióhullámok szórása, hiszen jóval több a zavaró jelforrás és tereptárgy, mint magasabban a légtérben.

A MAV Downlink egy Android okoseszköz alkalmazás. Egy TCP kapcsolat és az okostelefon USB soros kapcsolata között működik átjátszó szerepben. Az alkalmazás nyílt forrá-

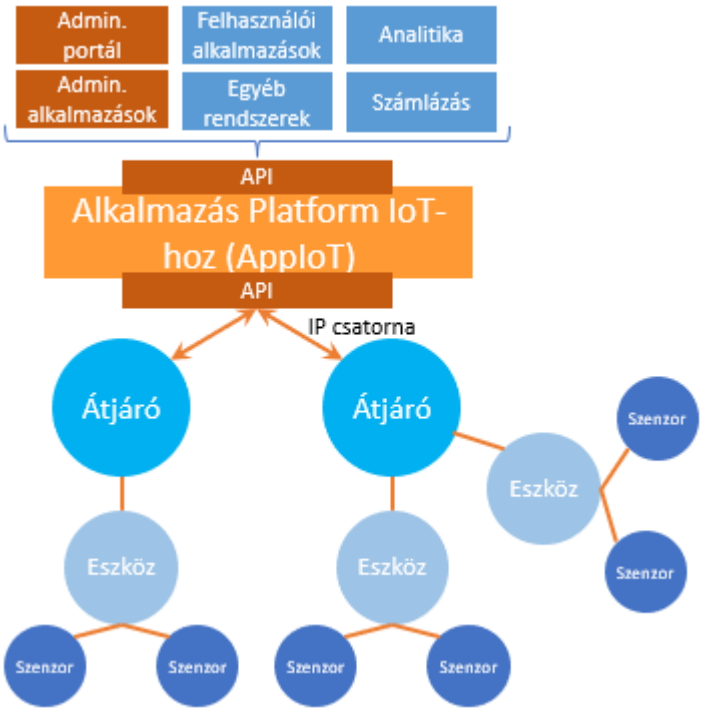
sú, így szabadon tovább fejleszthető. Az alkalmazás a TCP kapcsolat megszakadása esetén automatikusan újra csatlakozik. Az ArduPilot Mega 2.6 robotpilóta egy korábbi, mára már kifutott eszköz. Jelen UAS fejlesztésének kezdete 2015 környékére tehető, így történelmi okokból maradt meg a prototípus rendszerben. A 2.5-ös verzióval szemben ez a modul nem rendelkezik beépített iránytűvel, így külső iránytű modul csatlakoztatására szükséges. Az élesítés előtti ellenőrzések kikapcsolásával lehetséges azonban iránytű nélkül is repülni, bár az inerciális navigáció sokkal pontatlanabb – az indításkor előre mutató irányt tekinti északnak a rendszer. Természetesen távirányítóval történő, legfeljebb magasságtartást segítő repülési módokban nincs feltétlen szükség az iránytűre.

Mivel az APM 2.6-os verzió már elavult, csak MAVLink 1.0 verziót támogat. A MAVLink 2.0 2017 körül került bevezetésre. Emiatt – és az APM 2.6 hardware limitációi miatt – csak a régebbi ArduCopter firmware-ekkel kompatibilis. MAVLink adatok küldés/fogadását próbáltam Pixhawk PX4 és Pixhawk 4 Mini robotpilóta rendszerekkel is, ám ezekhez a MAV Downlink mobilalkalmazás hibája miatt sikertelen volt a kapcsolódás.

A szimulátoros tesztesetekhez a későbbiekben az APM 2.6-al gyűjtött valós MAVLink 1.0 repülési naplófájlok biztosították az alapot.

2.2.4 IoT rendszerekhez való hasonlatosság

Az IoT architektúra általában eszközöket, átjárókat, menedzsment szolgáltatást és alkalmazásokat foglal magában. A 18. ábra szemlélteti egy IoT infrastruktúra hierarchiáját. Az eszközök szenzor adatokat gyűjtenek, vagy a hálózaton át kapott utasításokat hajtanak végre. Az eszközök energiatakarékossági okokból jellemzően rövid hatótávú vagy sávszélességű kapcsolattal csatlakoznak az átjárókhoz. Az átjárók a menedzsment szolgáltatásokhoz interneten át kapcsolódnak, ahol a heterogén adathalmaz feldolgozásra, aggregálásra és tárolásra, majd szétosztásra kerül annak fogyasztói között. A fogyasztók lehetnek például egyéb szolgáltatások, végfelhasználói alkalmazások, ahol az adatok további feldolgozása és megjelenítése történik.



18. ábra: Az Ericsson AppIoT platformjának áttekintése.
(Az ábrát fordította és szerkesztette a szerző. Forrás: [93])

Vegyük észre a hasonlóságot ezen megközelítés és a távoli nyomkövető rendszerek (például az OGN[53], lásd 37. ábra) illetve a pilóta nélküli légijármű rendszerek (lásd 11. ábra) működése között. A légijárművek fedélzeti eszközei pozíció adatokat továbbítanak a többi légijármű és a földi vevőállomások felé. Ezek átjátszó állomásként, illetve átjáróként funkcionálnak, végül az adatok az interneten át kerülnek továbbításra a központi szerverek felé, melyek a központi adatbázisba gyűjtött adatok webes alapú térképes megjelenítésért felelősek. Ennek a felépítésnek egy változata, amikor az UAV fedélzetre kerül az internetes átjáró is. Ezen esetben vagy a robotpilóta valósítja meg ezt a funkcionalitást, vagy egy külső eszköz kerül elhelyezésre a fedélzeten, ami a robotpilótához kapcsolódik.

2.3 Következtetések

A felhő alapú kísérleti pilóta nélküli légijármű rendszer megtervezése során szem előtt tartottam a tesztelni kívánt speciális képességeket, melyek meglátásom szerint elősegíthetik a felhőből irányított repültetések biztonságát. Összegyűjtöttem a nyílt rendszerekben elterjedten használt irányítási és azonosítási protokollokat – a szakirodalom alapján úgy találtam, a leggyakrabban autonóm rendszerek esetén a MAVLink protokoll kerül alkalmazásra, aminek legújabb kiegészítései kísérleti jelleggel már most is lehetővé teszik

[53] Open Glider Network

OpenDroneID üzenetek küldését és fogadását, ami a pilóta nélküli légijárművek azonosítását valósítja meg.

Megállapítottam, hogy a pilóta nélküli légijármű rendszerek felépítése jelentős hasonlóságot mutat az IoT rendszerekével. Ebből arra következtetek, hogy a jövőben elképzelhető UAS rendszerek hagyományos IoT architektúrába és hálózatba integrálása is.

3 A FELHŐ ALAPÚ UAS-K TESZTELÉSI KÉRDÉSEI

3.1.1 Tesztelési megfontolások

A rendszer tesztelése során leginkább a szoftver és firmware rétegekre helyeztem a fókuszt, mivel a hardveres környezet leginkább piacon elérhető kész, vagy összeszerelésre kész komponensekből építettem fel.

A Nemzetközi Szoftvertesztelési Minősítő Testület (ISTQB[54]) meghatározása szerint a tesztinfrastruktúra *„a tesztelés elvégzéséhez szükséges szervezeti tényezők, beleértve a tesztkörnyezeteket, teszteszközöket, irodai környezetet és eljárásokat.”* [94].

Esetünkben két elkülönített megközelítést és tesztinfrastruktúrát alkalmaztam: terepen teszteltem a repülési, naplózási és megjelenítési funkcionalitást, illetve labor környezetben teszteltem az egyéb funkcionális és nem funkcionális követelményeket (például robusztusság) [S8].

Az információbiztonság klasszikus hármasára, illetve annak kibővített változatára alapozva a következő szempontokat vizsgálhatjuk példaként a rendszeren.

3.1.1.1 Bizalmasság

Biztonságos socket réteg (SSL[55]) / átviteli szint biztonság (TLS[56]) támogatást és az erre alapuló titkosítást nem valósítottam meg a szerver oldalon, mert az technikailag nem különbözik bármelyik hétköznapi webes szolgáltatástól, ennek vizsgálata nem adna új tudományos eredményeket. A MAVLinket, APM-et sem érinti a kérdés, a hálózati átjáróként szolgáló mobilappot tesztelnénk vele gyakorlatilag, ami nem saját fejlesztésű, és szintén nem várható tőle új tudományos eredmény. Általános TLS megvalósítás esetén vizsgálhatnánk például, hogy a támogatott algoritmusok naprakészek-e, illetve a megvalósító könyvtárnak vannak-e ismert sebezhetőségei?

3.1.1.2 Sértetlenség

Ismét, TLS megvalósítás esetén vizsgálhatnánk, hogy a támogatott algoritmusok naprakészek-e, a megvalósító könyvtárnak vannak-e ismert sebezhetőségei?

MAVLink 2.0 esetén megvizsgálhatjuk megbízhatóság szempontjából az (opcionálisan bekapcsolható) aláírás mezőnél alkalmazott integritásvédelem algoritmusát. Ennek részleteit lásd majd a 7.3 fejezetben. Az APM 2.6 esetén azonban csak a MAVLink 1.0 verzió

[54] International Software Testing Qualifications Board
[55] Secure Sockets Layer
[56] Transport Layer Security

támogatott, ahol még nem létezik ez a mező, így a vizsgálatokat gyakorlati, próbálkozás alapú jelszótöréses tesztek helyett matematikai alapon végzem.

A MAVLink protokoll specifikumait vizsgálva ellenőrizhetjük, hogy a hibás ellenőrzőös--szeggel érkező csomagokat hogyan kezeli a rendszer?

3.1.1.3 Rendelkezésre állás

Rendelkezésre állás szempontjából tesztelhetjük, hogy a hálózaton érkező hibás adatokat, csomagokat helyesen eldobja-e a robotpilóta, vagy esetleg ez szolgáltatáskimaradást, hibát okoz? Hasonlóan, a robotpilóta által nem támogatott, ám minden más szempontból szabványosnak tekinthető MAVLink parancsoktól esetleg összeomlik-e a rendszer? Klasszikus értelemben vett túlterheléses, szolgáltatásmegtagadást célzó támadást szimuláló tesztek esetén pedig gyors egymásutánban érkező parancsokkal próbálhatjuk túlterhelni a rendszert. A szerver oldal rendelkezésre állásának vizsgálata során megpróbálhatjuk azt nagyszámú drón szimulálásával leterhelni, illetve a terhelés okozta skálázódást és a hálózati kapcsolat stabilitását figyelemmel kísérni.

3.1.1.4 Hitelesség

Érdemes tesztelni, hogy a hamis (a hálózati forgalomba injektált) csomagokat kiszűri-e a rendszer? A MAVLink 2.0 esetén fentebb – lásd 2.1.6.2 fejezet – bemutattam az alkalmazott megoldást (aláírás), MAVLink 1.0 esetén nincs ilyen védelem, ebben az esetben csak a rendszerazonosító (`sysid`) mező azonosítja a küldőt, de ez könnyedén hamisítható. A tesztelés során nem állt rendelkezésemre olyan MAVLink 2.0-képes robotpilóta rendszer, amin ezt lehetőségem lett volna biztonsággal felkonfigurálni (a fentebb említett PX4 robotpilóta egység valós használatban volt a VOLARE projekt keretén belül), így erre a megoldásra nem terveztem teszteseteket. A hitelesség kérdésköréhez járul hozzá a PKI alkalmazásának lehetősége UAS-ek esetén, lásd majd az 5.1 fejezetben, bár erre a komplex, elkülönített infrastruktúrát is igénylő koncepcióra nem valósítottam meg gyakorlati támogatást a kísérleti rendszeren.

3.1.1.5 Számonkérhetőség

Számonkérhetőség vizsgálatakor a fő kérdés, hogy minden MAVLink üzenet esetén azonosítható-e a küldő fél? A fentieknek megfelelően csak a MAVLink 2.0-ban azonosítható jelenleg a küldő egyértelműen (a PSK alapján), az is csak abban az esetben, ha egyedi kulcs kerül kiosztásra. A meglévő, idő közben elavult robotpilóta egységgel ezt nem volt lehetőségem tesztelni. A számonkérhetőséget a PKI alkalmazása is elősegítheti, az ehhez kapcsolódó megfontolásokat lásd majd a 6.1 fejezetben.

3.1.1.6 Megbízhatóság

Vizsgálható, hogy mennyire stabil, vagy milyen gyakran szakad meg a hálózati kapcsolat, mekkora késleltetéssel működik, milyen gyakran vesznek el csomagok a hálózaton? A légi alrendszer esetén ez nem a robotpilótától függ, hanem inkább a mobilhálózati szolgáltatótól, hiszen a robotpilóta és az okostelefon között stabilnak mondható vezetékes soros kapcsolat van. Az internetes átvitel során a kommunikáció megbízhatóságát a MAV Downlink és a `pymavlink` közti TCP kapcsolat adja, annak protokollba épített képességei alapján. A 4G átvitel tesztelése leginkább a mobilhálózati szolgáltatás minőségét és lefedettségét vizsgálná, ami szolgáltatónként eltérő lehet, maga a 4G specifikáció pedig elviekben biztosítja a megfelelő kapcsolatot a drónokkal végzett műveletek során, egészen párszáz km/óra földhöz viszonyított sebességig. A bemutatott rendszer esetén a leglényegesebb megbízhatósági indikátornak a hálózati késleltetést tartottam, így ennek ellenőrzésére felszállások előtt kézi méréseket végeztem ICMP echo üzenetekkel a szerver és a drón között.

3.1.1.7 Letagadhatatlanság

Letagadhatatlanság szempontjából ellenőrizhetjük, hogy hogyan és milyen részletességgel kerülnek naplózásra a különböző események? Részletes naplófájlok kinyerhetők a robotpilóta firmware-ből, vagy akár a fedélzeti SD kártyáról (ha van ilyen), de nem minden típusnál érhető el ez a funkció. Emellett ezek a logok felülírhatók, törölhetők a felhasználó által az APM esetén. Szerver oldalon naplózhatjuk a telemetria adatokat (a beérkező MAVLink üzenetek alapján) is, ezek tartalmazzák az időbélyeget, a küldő és fogadó fél rendszerazonosítóját, a naplózott esemény típusát és paramétereit (például a drón pozícióját, szenzoradatait), a drón állapotát, és parancsvégrehajtás esetén annak eredményét. Ennek megbízhatóságát a repülések során történő adatgyűjtéssel és a naplófájlok utólagos kézi kiértékelésével ellenőriztem. Ennek a munkának eredményeként született például a később látható 22., 23. és a 24. ábra.

3.2 Repülési tesztkörnyezet

Az első repültetésre 2019. június 1-én került sor a következő eseti légtérben:

```
A1557/19
81
470603N 0201207E
470746N 0201204E
470752N 0201748E
470611N 0201753E
470603N 0201207E
```

```
(Szolnok)
GND 2500 feet AMSL
07:00 16:00
UAV flight
```

A tesztelés célja ezalkalommal a rendszer működésének alapvető verifikációja volt. Rövid, alacsony magasságú repülésekre került sor (ahogy a 19. ábrán is látható) pozíció és telemetria adatok szerveroldali gyűjtésének céljából, melyek a későbbi elemzések, vizsgálatok és szimulációk alapját képezték.

A második repültetést 2019. november 17-én hajtottam végre. Ezúttal a fő cél az autonóm repülés és útvonaltervezés verifikációja volt. Aznap a következő eseti légtérben volt használatban:

```
A4036/19
84
470603N 0201207E
470746N 0201245E
470752N 0201748E
470611N 0201753E
(Szolnok)
GND 4500 feet AMSL
07:00 15:00
UAV flight
```

A Drónpilóták Országos Egyesülete (DOE) tagsági azonosítóm: 269189, Groupama felelősségbiztosítás száma: 930/871727715 (érvényes mindkét repültetés idején).

19. ábra: Az UAV manuális repültetés közben.
(A kép a szerző saját gyűjteményéből származik.)

A terepi tesztek légi alrendszerének alapját egy egyedi, DJI F450 „Flame Wheel” keretre épített kvadrokopter adta. Az UAV ArduPilot Mega robotpilóta egységéhez univerzális soros busz (USB) irányított töltő- és adatkábellel (OTG[57]) a kiszolgáló oldalon egy okostelefon volt csatlakoztatva. A telefonon a MAV Downlink alkalmazás futott. Az app a központi rendszerhez 4G mobilinterneten át kapcsolódott. A kézi repültetés hagyományos 2,4 GHz távirányítóval történt, illetve ez adta a tartalék/vészhelyzeti irányítási lehetőséget az autonóm repülés során is. Erre azért volt szükség, mert az APM 2.6-ra elérhető legfrissebb firmware még nem támogatja a földi irányító állomással történő kapcsolatvesztés kezelését, és a kapcsolódó vészhelyzeti eljárás konfigutálását [95].

A robotpilóta az APM Planner szoftverrel került beállításra és kalibrálásra, minden szenzor automatizált állapotfelmérésen („health-check”) esett át minden egyes felszállás előtt. Az úgynevezett „geofencing” földrajzi elkerítés lehetőség is beállításra került, mely korlátozza, hogy a drón milyen messzire távolodhat el a felszállási ponttól, ezzel biztosítva, hogy az ne hagyhassa el a kijelölt eseti légteret.

A központi rendszer egy felhő alapú, Chicago VPS[58] szolgáltatótól bérelt virtuális magán szolgáltatón futott, melynek virtualizációs szervere fizikailag ténylegesen az egyesült államokbeli Chicagóban helyezkedett el.

[57] On-The-Go
[58] Virtual Private Server

A 2×7500 kilométeres távolság ellenére a hálózati késleltetés a drón és a földi állomás (notebook vagy okostelefon) között 150 ezredmásodperc körül mozgott (internet vezérlőüzenet protokoll (ICMP[59]) echo kérésekkel kimérve). A bemutatott megvalósítás csak másodpercenként – gyakorlatban a piacon elérhető megjelenítő rendszerek is ezt a frissítési sűrűséget alkalmazzák, illetve a releváns szabványok is minimálisan ezt írják elő, lásd későbbi fejezetek – szinkronizálta az UAV adatokat és a térképes felületet az adatbázison keresztül, így ez a mértékű hálózati késleltetés elhanyagolhatónak bizonyult a működés szempontjából.

Ebben az összeállításban egyetlen VM szolgálta ki az UAV kapcsolatért felelős felületet, a központi adatbázist és a küldetéstervező felületet, skálázási képességek nélkül. Ennek oka, hogy megítélésem szerint a skálázási és önjavító teszteket biztonságosabb volt elkülönítve, laborban végrehajtani.

A felhasználói felület (térkép) a terepen notebookon, vagy okostelefonon került megjelenítése mindkét esetben.

3.3 Szimulátor és tesztkörnyezet

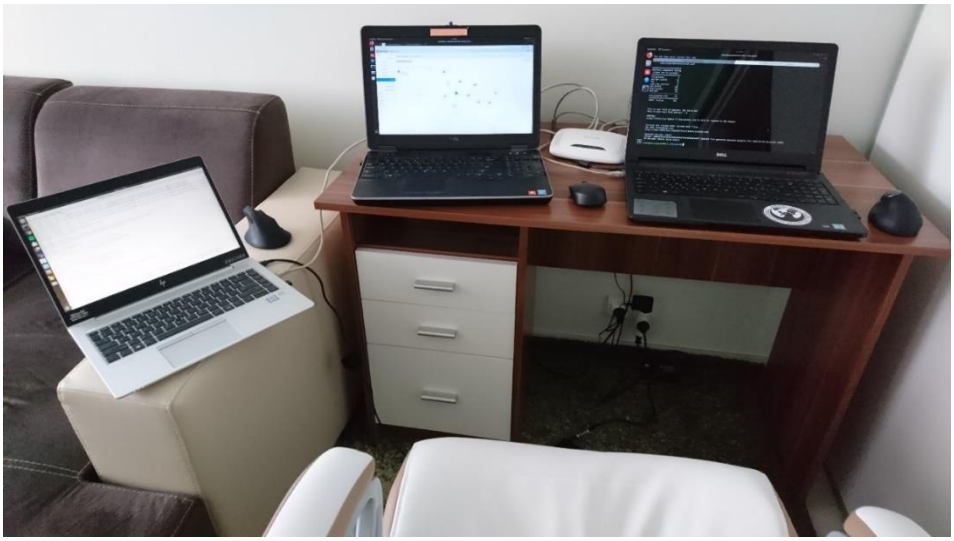
A szimulációs tesztek saját számítógépekből összeintegrált és felkonfigurált helyi felhőben kerültek végrehajtásra.

A laboros tesztek a központi infrastruktúra karakterisztikáinak vizsgálatát célozták, azon belül is kifejezetten az UAV-k felé irányuló interfészt, így a térképes felület mellőzésre került – az adatok ellenőrzése közvetlen a központi adatbázis megfigyelésével történt. A térképes felület alapvető funkcionalitásának ellenőrzésére a repülési tesztek során került sor, és mivel maga a felület a hagyományos „REST” webes kialakítást követi, új, érdekes eredmények aligha láttak volna napvilágot.

A központi rendszer elosztott számítási kapacitását két notebook biztosította, míg a harmadik notebook egy saját fejlesztésű, C++ és a 3-as verziójú teszt- és tesztvezérlés leíró (TTCN-3[60]) nyelven írt MAVLink 1.0 protokoll alapú szimulátor futtatására szolgált (lásd bővebben a következő fejezetben). Az kiküldött üzenetek sablonját a korábbi repülési tesztek során gyűjtött valós adatforgalom adta, melyet a szükséges helyeken a szoftver kódja dinamikusan töltötte ki (drón azonosítók, időbélyeg, ellenőrző összeg stb.).

A hálózati összeköttetést egy hagyományos, otthoni router szolgáltatta, ahogy a 20. ábrán is megfigyelhető.

[59] Internet Control Message Protocol
[60] Test and Test Control Notation version 3



20. ábra: A számítógépek és a router (balról jobbra): a szimulátort futtató gép, az „uascontrolnode” gép, a router és az „uascomputenode1” gép.
(A képet készítette a szerző.)

Összességében a két felhő számítógép 8 processzor szálat és nagyjából 24 GB memóriát szolgáltatott, nem feltétlen egyenlő arányban – a felhő rendszer heterogén mivoltát jól szemléltetve.

A rendszer szervezése az OpenStack infrastruktúra alkalmazásával valósult meg, melynek Heat nevű komponense lehetőséget nyújt a szolgáltatás automatikus skálázására és a virtuális gépek megfelelő terítésére.

3.3.1 UAV-k szimulálása

A „szimulátor” kifejezés első olvasatra félrevezetőnek tűnhet, nem a (táv)pilóták kiképzésére szolgáló, hagyományos értelemben vett gyakorló berendezést kell elképzelni, mint amilyen pédául az NKE szolnoki campusán került kialakításra, [96] [97] a szoftverrel pusztán nyers, sablonos protokoll adatok kerülnek küldésre és fogadásra, különösebb emberi beavatkozás nélkül. Pontosabban, az egyszerűség kedvéért térbeli elmozdulás nélkül, ám 45°/sec szögsebességgel egyhelyben, látványosan forgó kvadrokopterek pozícióadatai, illetve periodikus státuszüzenetek („`HEARTBEAT`”) kerülnek kiküldésre 1 Hz gyakorisággal.

A megvalósításhoz a korábbi ismereteim alapján és az iparban bevett gyakorlathoz igazodva a TTCN-3 tesztmodellező nyelvre esett a választásom. Ezen nyelvnek szöveges változata C++-hoz hasonló programnyelv, mely alkalmas különböző funkcionális és nemfunkcionális tesztesetek leírására.

A TTCN-3 nyelven megírt kód az eredetileg az Ericsson által kifejlesztett, mára nyílt forrású TITAN fordító és futtató környezet segítségével először specializált C++ vagy JAVA

kódra fordítható, majd a szokásos fordítóprogramokat használva ezekből futtatható állomány készíthető. A végeredmény lehet önmagában futtatható, vagy párhuzamosított program, mely a TITAN keretrendszerével konfigurálható, futtatható és menedzselhető. A tesztek lefuttatása közben a TITAN naplófájlokat generál, illetve a tesztesetek végeredményét is összegzi.

Hogy lehetőség legyen a MAVLink 1.0 protokollt TTCN-3 nyelven is alkalmazni, szükség volt egy úgynevezett protokoll modulra, ami összekötő kapocsként funkcionál a TTCN-3 teszt leíró világa és a C++ bináris adatszerkezetei között. Ez gyakorlatilag a kódoló és dekódoló függvényeket valósítja meg a MAVLink 1.0 adatszerkezeteire.

A láncolat végén egy TTCN-3 alapú szimulátor alkalmazás állt, mely 100 (ez az érték paraméterezhető) párhuzamos szálon futó kvadrokoptert szimulált szoftveresen.

3.3.2 Földi irányítórendszer szimulálása

A felhő rendszer tesztelésén túl szintén szükséges a pilóta nélküli járművek fedélzeti robotpilóta komponensének (esetünkben az APM 2.6) tesztelésére, működésének verifikálása, a robusztusság és a szabványos működés ellenőrzése. Érdemes vizsgálni, hogyan kezeli a fedélzeti rendszer a kapcsolat elvesztését, túlterhelését, hibás vagy hamis adatok injektálását a rendszerbe.

A fenti megfontolásokat, korlátokat figyelembevéve, megítélésem szerint a robotpilóta esetén főleg a rendelkezésre állás és sértetlenség tesztelésének volt érdemi haszna, létjogosultsága. Ezen célterületek lefedésére valósítottam meg egy, a fentihez hasonló TTCN-3 alapú szimulátort, ami a földi irányítórendszert hivatott helyettesíteni.

Ebben az esetben a szimulátor szekvenciálisan hajt végre különböző teszteseteket, közben naplófájlokat készít a végrehajtás részletes folyamatáról, majd kiértékeli a futási eredményeket. Ezt a szimulátort alkalmaztam a későbbi fejezetekben olvasható laboratóriumi, elektronikus biztonságot célzó tesztesetek megvalósításához. A szimulátor egy notebookon fut, ami wifi kapcsolaton keresztül kommunikál a korábbi drónra felszerelt okostelefonon futó MAV Downlink alkalmazással, ami USB kábelen keresztük továbbítja az üzeneteket az APM 2.6 robotpilóta felé.

3.4 Következtetések

Bár az általam alkalmazott robotpilóta rendszer némileg elavultnak mondható, a későbbi fejezetekben bemutatásra kerülő tesztesetek kimeneteléből látható, hogy így is értékes tapasztalatokat szolgáltatott.

A repülési tesztkörnyezet összeállítása alatt törekedtem az aktuális jogszabályoknak való megfelelésre: érvényes felelősségbiztosítás mellett, kollégáim segítségével és velük koordináltan végeztem a repültetéseket, számunkra aktivált eseti légtérben. Technikailag a lehető legbiztonságosabb konfiguráció összeállítására törekedtem: geofencing-et alkalmaztam, illetve tartalék irányítási módként kézi távirányítót tartottam készenlétben az autonóm repülési tesztek során is. A repülési tesztesetek végrehajtása alapján elmondhatom, hogy a fenti technikai biztonsági intézkedéseken túl sokat segített egy megfigyelő, segítő személy jelenléte is a repültetés során, kifejezetten a prototípus fázisban, de ajánlom ezeket a körülményeket biztosítani rutin repültetések során is.

A laboratóriumi tesztkörnyezettel megmutattam, hogy akár otthon, notebookokkal és egy egyszerű útválasztóval is összeállítható egy valódi felhő rendszer, amin később a felhő speciális képességeit hatékonyan tesztelni és demonstrálni tudtam. Ebből látható, hogy piacon elérhető hardverekkel és akár nyílt forrású, szabadszoftverekkel is kivitelezhető egyes Mission as a Service rendszerek tesztelése.

A szimulátor környezetek és a hozzájuk tartozó tesztesetek során igyekeztem mindkét oldalt, az UAV-kat és a földi irányító rendszert is releváns tesztesetekkel próbára tenni. Ehhez a szembenálló oldal szimulálására mindkét esetben külön alkalmazást, szoftverkönyvtárat és teszteseteket fejlesztettem ki, melyek kimenetei alapján a következő megállapításokat tehetem:

- Ahogy a későbbi *4.2.* fejezetből is látszik, a felhőből irányított pilóta nélküli légijármű rendszerek tesztelése eredményesen kivitelezhető a járművek tesztrendszerrel való helyettesítésével.
- Ahogy a későbbi *7.4.* fejezetből is következtethető, a felhőből irányított pilóta nélküli légijármű rendszerek tesztelése eredményesen kivitelezhető az irányítás tesztrendszerrel való helyettesítésével.

Ezeken túl kijelenthető, hogy a rendszer előzetes, szimulátorokkal történő tesztelése hozzájárul, hogy később a valósrepülések során kevesebb rejtett hiba forduljon elő, ezzel biztonságosabbá téve a repüléshez kapcsolódó általános folyamatokat.

4 FIZIKAI BIZTONSÁGI KÉRDÉSEK

Bár a felhő szolgáltatások esetén az adatközpontok telephelyeire is értelmezhető, esetünkben nem kifejezetten a biztonságtechnikára, épületek védelmére vagy beléptető rendszerekre [46] értem a fizikai biztonságot, hanem inkább a repülésbiztonság, ütközés- és balesetelkerülés, illetve a légiforgalom nyomon követhetőségének szempontjaira koncentrálok. A bemutatott Mission as a Service rendszer esetén ezek hatnak ki leginkább a fizikai világra.
Az európai U-space koncepció [26] szerves részét képezi a forgalmi információs szolgáltatás, [26, 11. cikk] a földrajzi helymeghatározási szolgáltatás [26, 9. cikk] és az UAS-repülésengedélyezési szolgáltatás [26, 10. cikk].
Az első szolgáltatásnak információkat kell nyújtania minden egyéb olyan szembetűnő légi forgalomról, amely az UAS-repülés helyéhez vagy tervezett útvonalához közel lehet. A második szolgáltatás az alkalmazandó üzemeltetési feltételekre és légtérkorlátozásokra vonatkozó információkat szolgáltat. Ezekhez kapcsolódóan, de a prototípus fázisban a követelmények részleges lefedésével, demonstrációs céllal valósítottam meg a térképes felületen az UAV forgalom és az NDZ-k megjelenítését.
A harmadik szolgáltatás keretein belül a U-space szolgáltatók minden egyes repülésre vonatkozóan UAS repülési engedélyt adnak az UAS-üzembentartóknak, és abban meghatározzák az adott repülés feltételeit. Az engedély iránti kérelem tartalmazza a tervezett röppályát, melynek megtervezéséhez a prototípus rendszer esetén a térképes felület nyújt eszközt.

4.1 Repülési tesztesetek

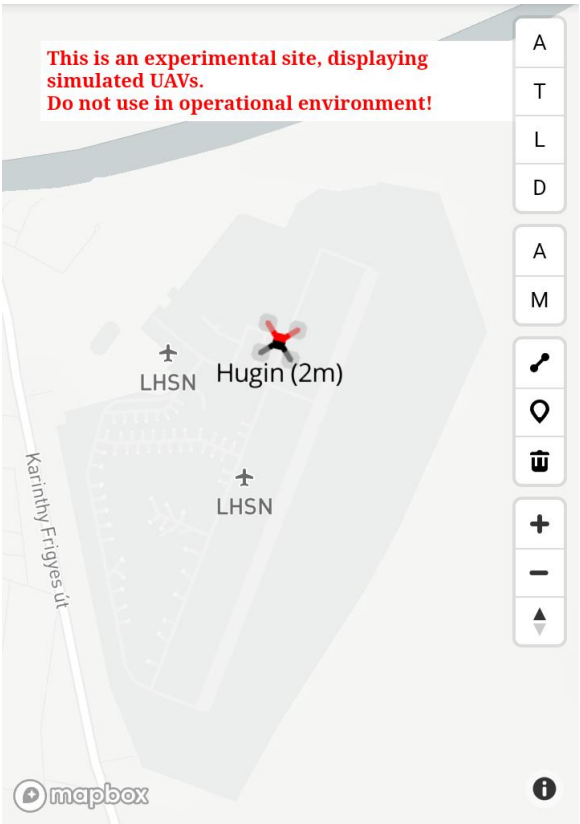
A felhő alapú irányításnál fontos a folyamatos visszajelzés és monitorozhatóság, a megbízható küldetéstervezés, illetve a felhő rendszer és a robotpilóta kompatibilitásának ellenőrzése. Mindez lényeges az ütközéselkerülés lehetőségének távoli biztosításához, az esetleges repesemények utólagos kivizsgálhatóságának támogatásához, a küldetések biztonságos és földrajzilag pontos megtervezéséhez, illetve a fedélzeti rendszerek alapvető repülési funkcionalitásának verifikációjához távoli irányítás esetén. A kevésbé komplex felhő alapú repültetési feladatok esetén meglátásom szerint ezen szempontoknak van leginkább kihatása a fizikai világ biztonságára. Azonban nem szabad elhanyagolni a repülési tesztek fontosságát, nem lehet azokat kizárólag laboratóriumi tesztesetekkel helyettesíteni.
„A repülési tesztek szükségessége azt jelenti, hogy a tesztelt légijármű rendszer vagy légijármű pontos vizsgálatára van szükség repülési környezetben ahelyett, hogy pusztán földi

verifikációs módszerekre hagyatkoznánk, mint szélcsatorna, szimulátorok és szoftveres modellek. A földi alapú módszerek, bár hasznosak, korlátolt képességekkel bírnak az igazi repülés dinamikus és valódi természetének modellezéséhez." [98].

4.1.1 Repülés naplózása

Az UAV a 2,4 GHz-es távirányítóval, `STABILIZE` módban került repültetésre. Manuális élesítés, felszállás és rövid lebegtetés után a drón távirányítva szállt le, majd a rotorok leállításával és biztosításával ért véget a művelet.

Repülés közben a szerver oldalon a térképes felület megfelelően jelenítette meg az UAV pozícióját, irányszögét és magasságát. Az adatbázisban és a konzol felületen megszakítás nélkül érkeztek meg a telemetria és pozíció adatok, amik naplózásra is kerültek. A térképes felület akkor aktuális állapotát lásd a 21. ábrán.



21. ábra: A térképes felület manuális repültetés közben. A vörös felirat felhívja a figyelmet, hogy az oldal esetenként szimulált UAV-kat is megjelenít, így nem használható valós légiforgalom nyomkövetésére.
(Az okostelefonos képernyőképet készítette a szerző.)

4.1.2 Kapcsolatmegszakadás és helyreállás

Az egyik manuális repültetés folyamán, leszállás közben a drón oldalra bukott a puha leszállófelületnek és egy hirtelen széllökésnek köszönhetően, minek következményeként az adatátvitelre szolgáló USB OTG kábel kirántódott az okostelefon csatlakozójából. Ekkor

nyilván nem volt lehetőség adattovábbításra az okostelefon oldalán. Az USB kábel újra csatlakoztatását követően az adatkapcsolat szinte azonnal helyreállt. Szerver oldalon ez alatt nem látszódott komolyabb, észlelhető hibajelenség (értsd: az adatok kimaradásától eltekintve nem volt hibaüzenet vagy szolgáltatáskiesés, -elakadás, lefagyás); a kapcsolat helyreálltakor a további adatok beérkezésével a térképes felületen is frissült az UAV állapota. A szolgáltatás utólagos állapotát megvizsgálva így elmondható, hogy a teszteset (bár az nem tervezett módon került végrehajtásra) sikeres volt.

4.1.3 Távoli élesítés/biztosítás

A drón ezesetben egyhelyben állt a talajon. A térképes felületen a felső „A” („`arm`”) gomb megnyomásával a rotorok aktiválódtak és felvették az elvárt egyenletes üresjárati teljesítményt, majd a „D” („`disarm`”) gomb megnyomásával azok leálltak és biztosított állapotba kerültek. A szerveroldali logok alapján továbbá ellenőrzésre került, hogy ténylegesen a gombnyomás váltotta ki a rotorok biztosítását, hiszen alap esetben, felszállás hiányában a rotorokat a robotpilóta is önmagától leállítja pár másodperc üresjárat után. A távirányító nem került csatlakoztatásra ezen művelet során. A teszteset kimenete sikeresnek mondható a rotorok megfigyelése és a naplófájlok elemzése alapján.

4.1.4 Távoli fel- és leszállítás

Az előző tesztesetben bemutatott élesítést követően, a második „A” gomb („`auto mode`”) került megnyomásra. Ezután a „T” („`takeoff`”) gomb megnyomására az elvárt viselkedés a felszállás lett volna. Ehelyett a drón a talajon maradt és pár másodperc után a rotorok automatikusan biztosításra kerültek. Az elvárt viselkedést a valóssal összevetve elmondható, hogy a teszteset sikertelen kimenettel zárult. Későbbi utánajárás eredményeként elmondható, hogy a dokumentáció [99] szerint az ArduCopter firmware 3.2.1-es verziója, ami az UAV APM 2.6-os [100] robotpilóta egységén fut, elvár egy kézi gázkar jelet a távirányítón a küldetés végrehajtásának megkezdéséhez, ellentétben a firmware újabb verzióinak viselkedésével, ahol a küldetések végrehajtása azonnal megkezdődik az `AUTO` módba lépést követően, vagy újabb küldetés fogadásakor. (Jelen megvalósítás egy egyelemű, felszállás típusú parancsot tartalmazó küldetést töltött fel.)

4.1.5 Útvonal feltöltése/törlése

A küldetéstervezés és feltöltés korábban ellenőrzésre került két külső, APM Planner és QGroundControl nevű szoftver alkalmazásával, melynek során küldetés (egyelemű úti célból, majd többelemű útvonalból álló küldetés) került feltöltésre a robotpilóta memóriájába

a saját fejlesztésű térképes interfészt használva, majd azt a fenti szoftverekkel (mint „etalon”) kiolvasva lehetőség volt verifikálni azok saját térképes felületein.

Ezen felszállás nélküli teszteset során kezdetben kibukott egy hiba, miszerint a MAVLink adatszerkezetei és a MapBox térképes felület adatszerkezetei egymáshoz képest fordítva reprezentálták a hosszúság-szélesség koordinátapárt, ami miatt a feltöltött küldetés úti célja hazánk területéről (pl. 47° É, 19° K) Szaúd-Arábia területére fordult át (19° É, 47° K). Szerencsére ezt a hibát még valós felszállás előtt sikerült észlelni és kijavítani, a tesztesetnek köszönhetően.

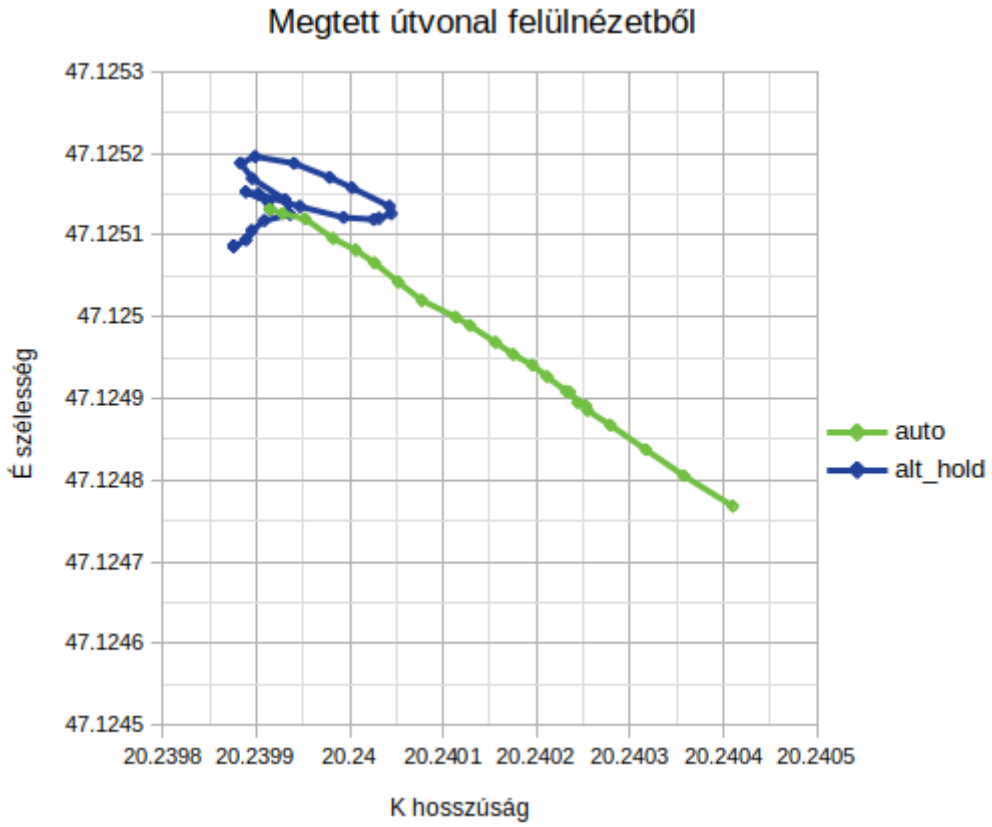
Terepen, a küldetés feltöltése és törlése egyszeri úti cél feltöltésével lett kipróbálva. A térképes felületen az úti cél kijelölő „⌾” gombra kattintás, majd a cél elhelyezésének eredményeként a szerveroldali naplóból látszódtak a robotpilóta által küldött válaszüzenetek, miszerint befogadta a küldetést. Az úti cél törlésének ellenőrzésére ezután a térképes felület szemeteskosár ikonjára kattintva volt lehetőség, ismét figyelemmel kísérve a szerveroldali konzolt és naplót. A kimeneteket figyelemmel kísérve megállapítható volt, hogy a küldetésfeltöltésből és -törlésből álló teszteset ezesetben már sikeresen zárult.

4.1.6 Küldetés felülírása

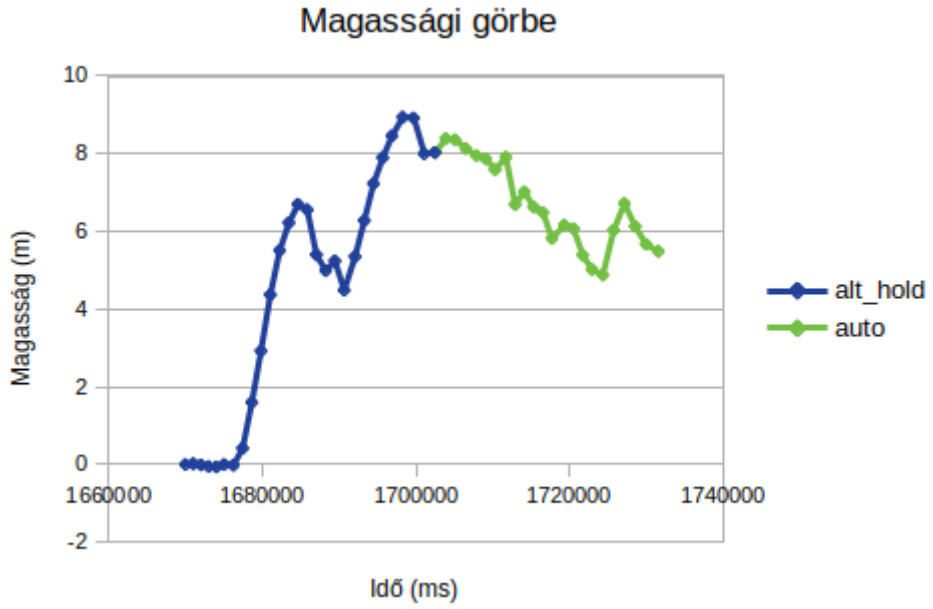
Az előző tesztesetnek megfelelő küldetés feltöltés után új küldetés került megtervezésre a térképes felület segítségével. A szerveroldali naplóban található üzenetváltások alapján ellenőrizhető volt, hogy a robotpilóta ténylegesen törölte a memóriából a korábbi küldetést, majd feltöltötte az újat, illetve ezen műveletekről megerősítést küldött. A naplózott sorokat kiértékelve elmondható, hogy a teszteset sikerrel zárult.

4.1.7 Autonóm repülés

A drónt a térképes felület „M” gombjával manuális (`ALT_HOLD`, megjegyzés: korábban ez `STABILIZE` módot jelentett, az eltérés a két repültetés közötti fejlesztés eredménye) módba kapcsolva és a gázkart a távirányítón 0 állásba állítva egy egyszeri úti cél került feltöltésre a térképes felületen keresztül. Az útvonal sikeres feltöltését a szerveroldali naplófájlok is megerősítették. A rotorok a térképes felület felső „A” gombjának megnyomására élesítésre kerültek, majd a gázkar előre tolásával történő kézi felszállást követően elérte a nagyjából 9 méteres magasságot. Ekkor a térképes felület alsó „A” gombját megnyomva az UAV `AUTO` módba váltott. A robotpilóta átvette az irányítást, és a drón elkezdte megközelíteni a kijelölt úti célt (22. ábra) és magasságot (23. ábra).



22. ábra: A repültetés alatt megtett útvonal felülnézetből.
(Az ábrát telemetria adatokból szerkesztette a szerző.)



23. ábra: A repültetés alatt bejárt magassági görbe. Az időbélyeg a bekapcsolás óta eltelt ezredmásodpercekben értendő.
(Az ábrát telemetria adatokból szerkesztette a szerző.)

Amikor elég közel ért a célhoz (ez a távolság a robotpilóta paraméterezésével konfigurálható), a robotpilóta egy MAVLink üzenettel jelezte a küldetés sikerességét, majd egyhely-

ben lebegve várta a további utasításokat, lásd 24. ábra. Ezen a ponton a tesztesetet sikeresnek értékelem az autonóm küldetés sikeres végrehajtása alapján.

24. ábra: A szerveroldali konzol a napló néhány sorával, illetve a térképes felület autonóm repültetés közben. A narancssárga pont jelöli az úti célt. A bal oldali konzol ablakban látható egy nyers státuszüzenet és egy pozícióüzenet koordinátákkal, magasság- és egyéb repülési adatokkal, majd a visszajelzés, miszerint a légijármű elérte az első számú úticélt. (A képernyőképet készítette a szerző.)

A teszteset helyreállítási szakaszában az „L” („`land`”) gomb megnyomására az UAV helyben, autonóm módon le kellett volna, hogy szálljon, de miután ez sikertelen volt, az „M” gomb ismételt megnyomásával a drónt visszaállítottam a tartalék kézi irányításra, majd a kiinduló ponthoz reptetve kézi leszállást kíséreltem meg. A leszállás során a drón felett hirtelen elvesztettem az irányítást és az tehetetlenül a földre zuhant, aminek eredményeként a rotorlapátok és a keret súlyosan megrongálódtak, lásd 25. ábra, így további tesztesetek (pl. hosszabb útvonal) kivitelezésére már nem volt lehetőség.

25. ábra: A szerző a repülési tesztelés során használt felszereléssel.
(A kép a szerző saját gyűjteményéből származik.)

A szerveroldali naplófájlok későbbi elemzése azt mutatta, a drón nem küldött több `HEARTBEAT` vagy pozíció üzenetet miután teljesítette a küldetést, így feltételezhető, hogy az első hibát a firmware egy hibája okozhatta. Ahogy láttuk, a korábbi próbák során a fel- és leszállás teszteset eddig sem volt sikeres, de mivel itt csatlakoztatva volt a távirányító, a dokumentáció szerint 0-nál nagyobb gázkar állás mellett a robotpilótának végre kellett volna hajtania a feladatot.

Végül a drónra szétcsatlakoztatott akkumulátor kábellel találtam rá, ez magyarázatot adhat a második hibára, a manuális leszállás közben megfigyelt hirtelen teljesítményvesztésre, aminek következtében az UAV végül lezuhant. Az akkumulátor úgynevezett Dean's csatlakozópárral (lásd 26. ábra) van az alaplaphoz kötve, amit gyakran használnak egyedi építésű UAV-k és modellrepülőgépek esetén. Ennek előnye a másik gyakori modellező csatlakozótípushoz, a Tamiyához képest, hogy sokkal nagyobb az érintkező felülete, így kisebb ellenállás mellett biztosítja az összeköttetést, ezzel csökkentve a nagy áramfelvétel mellett jelentkező anyagolvadás kockázatát. Hátránya viszont, hogy nincs felszerelve a Tamiyához

hasonló kampós klipsszel, ami megakadályozná az esetemben is fellépő szétcsúszásos problémát. Ennek jövőbeni elkerülésére a Dean's csatlakozók rögzítését tépőzárral erősítettem meg.

26. ábra: Dean's és Tamiya csatlakozópárok.
(Forrás: [101] [102])

4.2 Laboratóriumi tesztesetek

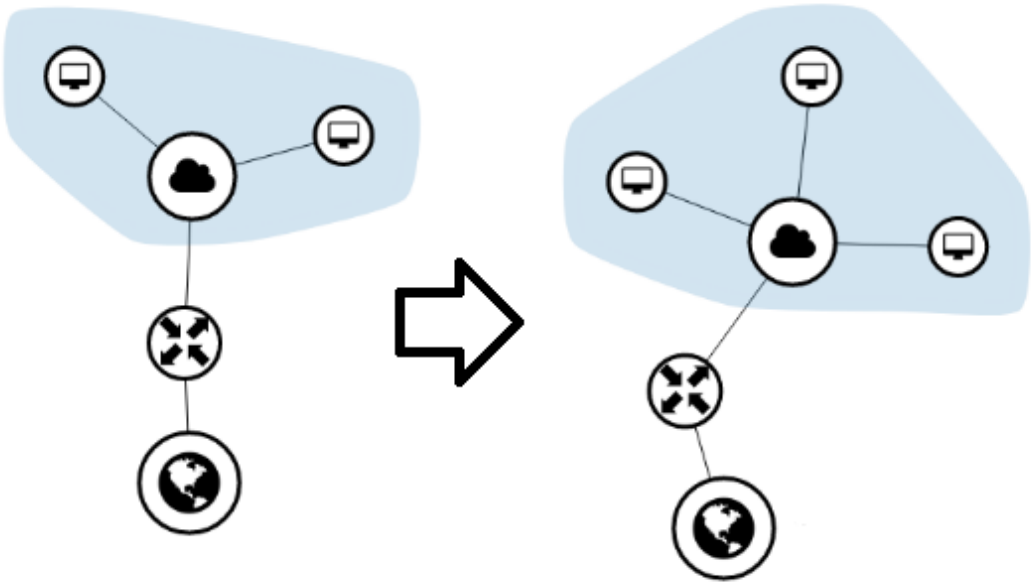
A veszélyesebb, komplex tesztesetek elbukása valós fizikai veszélyt jelenthet: a kísérleti felhő rendszer hibás működése esetén. Küldetés közben elveszhetnek, irányíthatatlanná válhatnak a drónok, ha esetleg nem áll helyre a kapcsolat, nem jól működik a skálázás vagy terheléselosztás. A nagy számú drónnal történő tesztelés valódi drónok beszerzésével és mobiltelefonok felszerelésével kivitelezhető, de költséghatékonyabb, biztonságosabb és a feladat szempontjából jobban skálázható megoldás, ha szimuláljuk a drónokat. Ehhez a manuális reptetések során gyűjtött valós, MAVLink üzeneteket tartalmazó telemetria és naplófájlokból indultam ki, majd ezt az adathalmazt paramétereztem fel több különálló drón szimulálásához.

4.2.1 Manuális skálázás

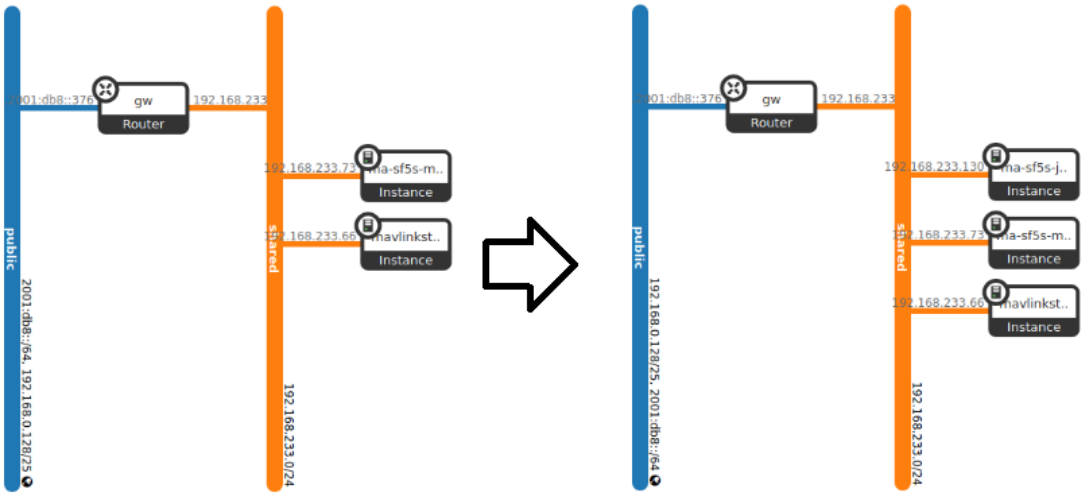
Egy OpenStack Heat `ScalingPolicy` létrehozásakor egy belső elérésű egységes erőforrás-helymeghatározó (URL[61]) generálódik. Ez az URL az erőforrások dinamikus újraelosztásának manuális kiváltására használható, például egy `AutoScalingGroup` fel- vagy leskálázására. A teszteset végrehajtása során a fenti URL-re történő csatlakozás hatására a felhő felfelé skálázódása figyelhető meg.

A teszteset sikeres kimenetele a 27. ábrán látható képernyőképeken látható, melyen egy újonnan létrejött VM látható, amint csatlakozott a szolgáltatás kiszolgálásához. A hálózatot érintő változások részleteiben a 28. ábrán láthatók.

[61] Uniform Resource Locator



27. ábra: Egy új virtuális szerver létrejötte.
(A képernyőképet készítette és szerkesztette a szerző.)



28. ábra: Az új 192.168.233.130 hálózati című virtuális szerver példány helye a „megosztott” hálózatban.
(A képernyőképet készítette és szerkesztette a szerző.)

4.2.2 Automatikus skálázás

Természetesen kényelmesebb, ha a skálázódás önmagától történik szükség esetén, ezért egy erőforrás riasztás került beállításra a fel- illetve leskálázás politikákhoz. A riasztásért felelős elem a példa kedvéért 5 percenként lekérdezi a processzor kihasználtságot, majd szükség esetén fel- vagy leskálázást vált ki, amennyiben az érték kívül esik a kívánt 20-80% közötti intervallumon. A prototípus rendszer fejlesztésének idején a processzor kihasználtságot reprezentáló metrika megvalósításának limitációja miatt nem lehetett annak granularitását 300 másodpercnél kisebbre venni, innen az 5 perces mintavételezés. A 20 és

80%-os értékek kezdetben amentén a feltételezés mentén kerültek meghatározásra, miszerint a megadott 5 perc alatt normál működés során nem várható 20%-nál nagyobb terhelésnövekedés, vagyis nem fordulhat elő olyan helyzet, hogy egy mintavételkor 80% a processzor terhelés, majd 5 percen belül már 100% kerül kihasználásra, mely esetben további drónokat nem lenne képes kiszolgálni a rendszer, ezzel szolgáltatáskiesést okozva. Természetesen mindhárom fenti paraméter konfigurációs fájlból finomítható valós rendszer esetén az aktuális rendszeren végzett terheléstesztek eredményének megfelelően.

Kezdetben a terhelést 100 UAV szimulálásával kezdeményeztem, melyek másodpercenként `HEARTBEAT` és pozíció adatokat küldtek egy felhőn kívül álló notebookról a felhő szolgáltatás felé. Ez azonban a virtualizált processzor kapacitásának mindössze 10%-ának meghajtására bizonyult elegendőnek egy egyedüli virtuális gép esetén is. Másodpercenként 2 darab MAVLink üzenettel, és a protokoll korlátaiból adódóan üzenetenként maximum 280 bájttal számolva, 100 darab UAV esetén ez mindössze 56 kB/s adatfolyamot jelent, ami napjaink internetes adatforgalmának léptékében mérve nagyon kicsinek tekinthető, egy átlagos, tömörített fénykép méretéhez viszonyítható. Ezért várhatóan a MAVLink protokoll által párhuzamosan kezelhető maximum 254 UAV (142 kB/s adatforgalom) sem lett volna elég a skálázás kiváltására, így a VM konzoljába belépve (a legegyszerűbbnek ítélt módszert választva) egy végtelen ciklus kiváltásával értem el további terhelést. Pár perc múlva, a következő ellenőrzés alkalmával a felfelé skálázás politika automatikusan életbe lépett, minek hatására egy újabb virtuális gép jött létre a felhőben. Továbbá a terhelés megszűnése a következő periodikus ellenőrzés alkalmával sikeresen kiváltotta a rendszer lefelé skálázását, minek hatására az újonnan létrejött virtuális gép leállításra, illetve törlésre került. A teszteset kimenetele ezen a ponton sikeresnek értékelhető. A manuális terhelésen kívül a felskálázás kiváltására természetesen egy másik módszer a határértékek finomítása lehetett volna: például 8% le- és 10% felskálázási határérték beállítása, de itt az alsó és felső küszöb olyan közel lenne egymáshoz, hogy más, nem kontrollált külső tényező is kiválthatta volna a megfigyelt jelenséget, például a virtuális gép naplófájljainak lapozása és tömörítése, egy háttérben futó rendszerfrissítés. Így inkább a kézi terheléskiváltás adta kontrollt választottam a teszteset kiértékeléséhez, valós, komplexebb és szolgáltatásdúsabb rendszerek (pl. távoli képelemzés) esetén már életszerű lehet a 20 és 80%-os érték.

4.2.3 Statikus elhelyezés

Ebben a tesztesetben az erőforrás-gyűjtemény felállításakor azonnal 2 virtuális gép került elindításra. A cél annak ellenőrzése volt, hogy a két virtuális gép valóban egymást „taszít-

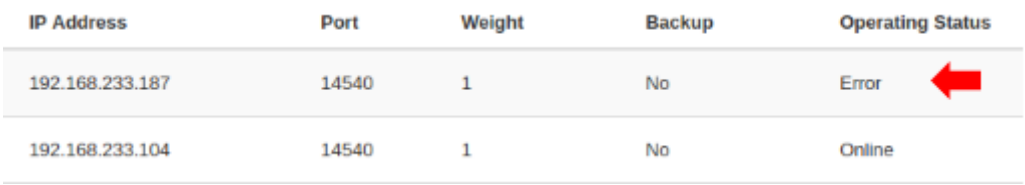
va”, az antiaffinitás szabályának megfelelően két különböző számítási egységen jön létre. A teszt sikeresen lefutott, az első UAV kezelő VM és az adatbázisért felelős VM az első („uascontrolnode” nevű) számítógépen jött létre, amíg a második UAV kezelő VM a második („uascomputenode1” nevű) számítógépen.

4.2.4 Dinamikus elhelyezés

Ez alkalommal a kezdeti egyetlen virtuális gép indulása után a 4.2.1 fejezetben leírt teszteséthez hasonlóan kézi felskálázásra került sor. A skálázódást követően a második virtuális gép megfelelően, a másik fizikai számítógépen jött létre, ennek köszönhetően a teszteset kimenetele sikeresnek tekinthető.

4.2.5 A szolgáltatás túlélőképessége

A teszteset során a szolgáltatás kezdetben két fizikai számítógépre terítve került kiosztásra. Miközben a szimulált UAV-k aktívan terhelték a szolgáltatás erőforrásait, a második fizikai számítógépből egyszerűen kihúztam a hálózati kábelt, megszakítva a kapcsolatot a számítógép és a router között, ezzel a notebook megsemmisülését vagy egyéb végzetes hálózati problémát szimulálva. Az erőforrás felügyelő komponens a háttérben (nagy gyakoriságú, 5 ezredmásodpercenkénti – ez az érték konfigurálható) periodikus TCP-alapú vizsgálatot végez a szolgáltatás állapotának ellenőrzése céljából. Ennek köszönhetően pillanatokon belül észlelte a meghibásodott számítógépen futó VM-ek elvesztését, és ezeket „`Error`” jelzéssel látta el, ahogy a 29. ábrán látható webportálról készült képernyőképen is látható. A terheléselosztó komponens ennek hatására a beérkező üzeneteket a többi futó VM között osztotta szét. Így végső soron a szolgáltatás az UAV-k által észlelhető megszakadás nélkül túlélte az egyik fizikai számítógép katasztrofális elvesztésének esetét, vagyis a teszteset sikeresen ment végbe. Amennyiben pont az 5 ezredmásodperces időablakban érkezett volna a drónoktól (valós rendszeren a MAV Downlink alkalmazástól) üzenet, azt a TCP protokoll hamarosan újraküldte volna, így ebbe az irányba nem történt volna adatvesztés. Ha a földi alrendszer irányából érkező parancs drón felé küldése során szakad meg a kapcsolat, akkor pedig az adatbázisban továbbra is új parancsként marad meg a listában, melynek hatására egy másik VM küldi ki az üzenetet a drón felé, szintén megelőzve az adatvesztést. Ennek a működésnek persze előfeltétele, hogy legalább 2 VM fusson az infrastruktúrában, más-más fizikai kiszolgálón.



IP Address	Port	Weight	Backup	Operating Status
192.168.233.187	14540	1	No	Error
192.168.233.104	14540	1	No	Online

29. ábra: A szétkapcsolt 192.168.233.187 hálózati című virtuális szerver státusza „Error-ra” vált.
(A képernyőkép részletet készítette és szerkesztette a szerző.)

4.2.6 Szolgáltatás helyreállítás

Az előző tesztesetet tovább gondolva később újra csatlakoztathatjuk az elvesztett számítógépet a hálózatba. A hálózati kábel visszahelyezését követően a kapcsolat helyreállt, és az erőforrás felügyelő komponens ezt észlelve újra „Online” státuszba helyezte a számítógépen futó virtuális gépeket. A szolgáltatás kódja úgy került megírásra, hogy a hálózat megszakadása esetén a kapcsolatokhoz tartozó erőforrások azonnal felszabadításra kerüljenek, így nem maradnak beragadt kapcsolatok, amik arra várnak, hogy a meglévő kliensek újra hálózati csomagokat küldjenek, hiszen az elvárt működés szerint az előző tesztesetnek megfelelően másik virtuális gépre kerül át a kliensek kezelése. A kapcsolat helyreálltát követően az újabb kliensek sikeresen csatlakoztak a szolgáltatásba visszaállt szerverhez is, így a teszteset kimenetele sikeresnek értékelhető.

4.2.7 Újracsatlakozó kliens

Ez alkalommal egy kliens csatlakozott a szolgáltatáshoz, ami kilépett, majd újra csatlakozott. A teszteset célja ellenőrizni, hogy a szerver oldalon az érintett erőforrások ténylegesen felszabadulnak kilépéskor, illetve újra csatlakozás esetén újfent létrejönnek. Ez a tulajdonság képezi a korábbi 4.2.6 Szolgáltatás helyreállítás és a következő 4.2.8. Kliens perzisztencia tesztesetek alapját. A teszteset a leírtaknak megfelelően ment végbe, így sikeresnek mondható.

4.2.8 Kliens perzisztencia

Kezdetben két virtuális gép indult. A kliens a szolgáltatáshoz csatlakozáskor az első szerverhez került, kijelentkezést és visszacsatlakozást követően ismét az első VM-re került kiosztásra a változatlan IP címe alapján, az elvárásoknak megfelelően így a teszteset sikeres kimenettel zárult. A perzisztencia tulajdonság akkor is hasznos lenne, ha a szolgáltatás kódja várakozna a kliensek újracsatlakozására megszakadás esetén, így megjegyezve, gyorsítótárazva annak állapotát. Esetünkben azonban más előnye van ennek a viselkedésnek, amit a következő teszteset mutat be.

4.2.9 Kliens perzisztencia migrálás után

Ismét 2 virtuális gép indult két külön fizikai számítógépre elosztva. A kapcsolódó kliens a második VM-hez került kiosztásra. A hálózati kábelt a korábbiaknak megfelelően kihúzva a kliens az első VM-hez került átirányításra. A hálózati kábel újracsatlakoztatását követően a kliens helyesen továbbra is az aktuális VM-hez csatlakozva maradt. Így nem volt szükség a kliens újracsatlakozására csak amiatt, hogy az eredeti kiszolgálója újra elérhetővé vált, megspórolva ezzel a kapcsolat lebontását és annak újbóli kiépítését. A teszteset kimenete ezzel sikeresnek tekinthető.

Megjegyzés: Amennyiben a migráció hatására a meglévő kliensek összesített tömege túlterhelte volna az egyedüli szolgáltatót, ezt az erőforrás riasztásért felelős komponens legfeljebb 5 perc alatt észlelte volna, és indított volna egy új VM-et egy másik processzor szálon, illetve lehetőség szerint másik kiszolgálón. Így a kapcsolatok elvben maximum 5 percig lehetnek instabilak. Ám az új VM az IP alapú perzisztencia miatt csak akkor kerül kihasználásra, ha friss kliensek csatlakoznak be. Az 5 perces felügyeleti periódus technikai okok miatt konstans, viszont a riasztási intervallum szűkítésével és több kezdeti VM indításával elérhető, hogy még jobban területjön a szolgáltatás és csökkenjen a túlterhelésből eredő hibaesetek száma. Ám ha úgy számolunk, hogy ez a maximum 5 perces szolgáltatás degradáció évente legfeljebb egyszer fordul elő, a szolgáltatás még mindig teljesíti az ötkilences rendelkezésre állás feltételét.

4.3 Felhő alapú repülésmeteorológiai támogatás lehetőségei

Az európai U-space koncepció [26] szerves részét képezi a meteorológiai U-Space szolgáltatás [26, 12. cikk]. Ennek keretein belül a szolgáltatók megbízható forrásból származó időjárási adatokat gyűjtenek, illetve időjárás-előrejelzéseket és tényleges időjárási információkat nyújtanak az UAS-üzembentartónak a repülés előtt vagy a repülés során. Egy európai elvárásoknak megfelelő felhő alapú UAS kialakítása során ezért fontos szerep jut a meteorológiai alrendszer kialakításának is.

4.3.1 Időjárás előrejelző modell futtatása felhőben

Korszerű szoftver konténer technológiákat, mint például a Docker, az utóbbi években egyre sikeresebben alkalmaznak nagy bonyolultságú informatikai rendszerek konfigurálásának megkönnyítésére. Lényege a szoftveres függőségek kezelésének és kielégítésének beépített lehetősége, vagyis az egymásra épülő vagy együttműködő szoftverek megfelelő verzióinak automatikus kiszolgálása. Emellett réteges felépítésének és központi repozitórium támogatásának köszönhetően hatékony és hordozható megoldáshoz juthatunk.

„A Weather Research and Forecasting (WRF, időjárás kutatási és előrejelzési) modell egy következő generációs, mezoskálájú, numerikus időjárás előrejelző rendszer, melyet úgy terveztek, hogy mind a légköri kutatások, mind az operatív előrejelzés igényeit kielégítse” [103].

Kutatásunk során kollégáimmal a VOLARE projekt keretin belül a WRF időjárási modell egy meghatározott konfigurációját (egy konkrét beállítással egy adott területre és időpontra futtatható, bemeneti adatokkal is rendelkező, önálló és hordozható szoftver- és adatcsomag) helyeztük el egy Docker szoftver konténerben, amit különböző, heterogén architektúrájú számítógépes platformok WRF modell futtató képességeinek mérésére és összehasonlítására használtunk [S7]. A vizsgált rendszerek között egyaránt szerepeltek hagyományos fizikai (nem virtualizált) szerverek, asztali és hordozható személyi számítógépek, továbbá több közösségi és publikus (kereskedelmi) felhőszolgáltatást nyújtó, sokprocesszoros virtualizált számítási rendszerek. Célunk az UTM-en belüli meteorológiai támogatás technikai lehetőségeinek vizsgálata volt.

4.3.1.1 Mérések

4.3.1.1.1 Mérőeszközök

Az összehasonlítás alapjául szolgáló szkript kimenetében kilistázza a legfontosabb metrikákat, példaképp:

```
items:149
max:  26.893060
min:  2.911170
sum:   495.158710
mean: 3.323213
mean/max:0.123571
```

Az `items` sor a feldolgozott időlépcsők darabszámát adja meg. A `max` és `min` a maximális és minimális egy időlépcsőre eső feldolgozási időt adja meg másodpercben, amíg a *sum* az időlépcsőkhöz összesen igénybe vett feldolgozási időt adja meg. Az átlagos időt a `mean` sor adja meg, ami a `sum` és az `items` sor hányadosából számolódik.

Továbbá az átlagos számítási teljesítmény (gigaFLOPS-ban, azaz milliárd lebegőpontos művelet / másodpercben) kiszámítható a konfiguráció összes lebegőpontos műveletszámának és az átlagos futásidő hányadosaként.

A szimulációs sebesség a modell időlépcsőjének aránya a mért átlagos feldolgozási időhöz mérten.

A mérés szempontjából legfontosabb metrikák a fentiek közül az átlag és az összeg (`sum`). Mivel az időlépcsők darabszáma állandó az összehasonlító mérések alatt, az összeg mezőt egyszerűen megfeleltethetjük a teljesítménynek.

4.3.1.1.2 Szoftver konfiguráció

A Docker a világ vezető nyílt forrású szoftverkonténer platformja [104]. Leegyszerűsíti a szoftveres függőségek kezelését és biztosítja a különböző hardverek, operációs rendszerek, platformok és architektúrák közötti átjárhatóságot, mindeközben biztonságos és agilis megoldást nyújt a szoftverkonfigurációk szállítására és telepítésére.

Az összehasonlító mérések és a mérési eredmények kiértékelése során fontos szempont a nagyfokú hordozhatóság, ami leegyszerűsíti és meggyorsítja a tesztkörnyezet felállítását különböző kiszolgálókon mind felhő, mind fizikai környezetben.

A Docker képfájlok magukba foglalják a szükséges környezeti beállításokat, illetve a más, szülőkonténerektől történő öröklődés útján a szoftveres függőségeket is. A Docker keretrendszer egyszerű parancssori felületet biztosít a konténerek és képfájlok menedzselésére, letöltésére és létrehozására, ám a bonyolultabb összeállítások támogatására összetettebb, folyamatorientált, átfogó erőforrásszervező megoldások is elérhetők, például a Kubernetes infrastruktúra.

Az összehasonlító mérésekhez használt képfájl a WRF 3.7.1-es verzióját tartalmazta (2015.08.14-i verzió), gcc 5.3.1 20160413 verziójú (Ubuntu 5.3.1-14ubuntu2.1) fordítóval fordítva, Ubuntu 16.04 LTS operációs rendszer alapon.

A WRF bemenő adata egy 48 órás, 12 km horizontális felbontású 425×300-as rácsot tartalmazott, 35 vertikális szinttel a Kontinentális Egyesült Államok (CONUS[62]) tartomány fölött, 2001.10.24. dátumra, 72 másodperces modell időlépcsővel. Az előrejelzés időintervalluma 3 órát ölel fel, 2001.10.25. 2001 00Z-tól kezdődően. A bemeneti adatok online is elérhetők [105].

A feldolgozott időlépcsők valós darabszáma 150, de az első mérést a futtató szkript elveti, mivel az inicializációs, és egyéb ki- és bemeneti műveleteket foglal magába, amik extremális mérési értéket adnak [106].

A mérés során elvégzett lebegőpontos műveletek száma konstans, 30,1 milliárd.

4.3.1.1.3 Számítógép konfigurációk

A Docker biztosítja a hordozhatóságot kiszolgálók között. A WRF verzió, fordító és annak verziója így azonos minden vizsgált számítógép között.

[62] Continental United States

A rendszerek legfontosabb paraméterei a következők:

- a rendszer neve (terméknév, kiszolgálónév, működtető szervezet);
- operációs rendszer és verziója;
- a processzor gyártója, típusa, frekvenciája, gyorsítótár mérete, amennyiben ismert;
- magok száma foglalatonként, foglalatok száma kiszolgálónként;
- memória mérete magonként;
- összeköttetés típusa (például Infiniband, Gigabit Ethernet), termék neve, hálózati topológia, amennyiben ismert [106].

A mérések során megvizsgált számítógépeket a 3. mellékletben található táblázat veszi sorra.

4.3.1.1.4 Mérési pontosság

Felhő infrastruktúra esetén az erőforrások megosztott mivolta és az ezzel járó erőforrás koordinációs teher miatt váratlan terheléshullámok léphetnek fel a mérés során a virtuális processzormagokon, hálózatokon stb. Ezen jelenség kiszűrésére a méréseket többször megismételtük a felhő számítógépeken.

4.3.1.2 Eredmények

4.3.1.2.1 WRF skálázhatóság

Az ismételten végrehajtott tesztek azonban azt mutatták, az eredmények közti eltérés elhanyagolható, és a mért értékek jól reprezentálják a tesztelés alatt álló rendszer teljesítményét. Ezen tapasztalat alapján egyes későbbi méréseket nem ismételtük meg többszörösen, ezeket a mellékletekben csillaggal (*) jelöltük.

Többször ismételt mérések esetén a mért értékek számtani közepét vettük és azt ábrázoltuk. A mérési eredmények a 4. melléklet táblázatában találhatók.

A mért teljesítmények karakterisztikája közel hiperbolikus mintát követ. Mivel az 5. mellékleten látható diagram a *sum* értékeket ábrázolja másodpercekben az *y* tengelyen a számítási teljesítmény (GFLOP/sec) helyett, hiperbolikus függvényt feszítettünk az adatsorra (az elvégzett számításra vonatkozó) logaritmikus helyett, hiszen y=0 másodperc számítási idő nem lehetséges.

A mérési eredmények közt azonban találhatunk olyan adatokat, amelyek némi magyarázatra szorulnak.

A Scaleway gépek teljesítménye jelentősen elmarad a többi rendszeren mért eredménytől, ennek fő oka, hogy ezekben a számítógépekben Intel Atom processzor működik, ami a

teljesítmény helyett az alacsony energiafogyasztásra és előállítási költségre van optimalizálva.

A Dell notebookon kapott futási eredmények szokatlan görbére illeszkednek az 1-4 mag közötti mérések során, magasabb 2 magos és alacsonyabb 3 magos eredmény lenne elvárt a megfigyelt trendek alapján. Ez a diszkrepancia valószínűleg a WRF kód specifikuma, a mérések ebben az esetben 7 alkalommal kerültek megismétlésre, és az eredmények minden esetben követték a fenti mintát.

Az 5. melléklet ábráján látható a hiperbolikus trendvonalak illeszkedése az adatsorokra.

Még több hasonló mérési eredmény és diagram érhető el az összehasonlító szkript hivatalos honlapján [107].

4.3.1.2.2 Fizikai hardver kontra virtualizált hardver teljesítménye

Az eredmények azt mutatják, a virtualizált szolgáltatások teljesítmény és skálázhatóság szempontjából lépést tartanak a pusztán fizikai versenytársakkal, sőt sok esetben túl is szárnyalják azokat.

Az 5. mellékletben „■” szimbólum jelöli a fizikai szervereket, míg a virtuális szervereket „♦” reprezentálja. Az illesztett trendvonalak azt mutatják, a felhő szolgáltatók (szaggatott vonallal jelölve) teljesítménye nagyon kevéssel van lemaradva a pusztán fizikai szervereketől (folytonos vonallal ábrázolva), néhány esetben jobb eredményt is mértünk virtuális kiszolgáló esetén, például a Scaleway bare metal és virtuális megfelelője esetén a 4 magos mérés utóbbi javára mutat teljesítménybeli előnyt.

A 4 magos notebook és asztali PC mért adata két felhő szolgáltatón mért érték közé esik, míg több felhő szolgáltató épphogy lemarad tőlük.

4.3.1.2.3 Felhő szolgáltatások és fizikai hardver költségének összehasonlítása

2014-ben a Wigner Adatközpont és a SZTAKI közösen indította útjára az MTA Cloud projektet közösségi felhő létrehozásának céljával kutatási tevékenységek támogatására. Főként az MTA olyan projektjeit szolgálja ki, melyek nem IT-központúak. A 2016 második negyedévében megnyílt OpenStack felhő és Docker konténer alapú infrastruktúra a Wigner és a SZTAKI erőforrásait kombinálja, az országos akadémiai internetes gerinchálózatra és más szolgáltatásokra, például az eduGain és a HEXXA nyújtotta föderált identitásmenedzsmentre, azonosításra, jogosításra támaszkodva. A két telephely összesített kapacitása magába foglal 1160 virtualizált processzor magot, 3,3 TB memóriát és 564 TB tárhelyet. A mérések készültekor még nem állt rendelkezésre a szolgáltatásokra vonatkozó árazás, így ingyenesen kaptunk lehetőséget a mérések elvégzésére. Emiatt a 3. melléklet-

ben, 6. mellékletben és 7. mellékletben az MTA Cloud-ra vonatkozó költséget 0-val tüntettük fel.

Az 5. mellékletben látható diagramon a „*” ismét az egyszer ismételt mérésekhez kapcsolódó költségeket jelöli. A „**” azonban olyan költség értékeket jelöl, amelyekre később nem végeztünk teljesítmény méréseket, ezekre a szolgáltatás csomagokra / konfigurációkra a szolgáltató honlapján található árakat tüntettük fel a (láthatóan lineáris) trendvonalak meghatározásához. Ezek a konfigurációk a későbbi mellékletekben nem szerepelnek, mert teljesítményadat hiányában. A Microsoft Azure DS3-V-re vonatkozó adatok ebben a mellékeltben nem követik a várt trendet, a kiegészítő tárhely szolgáltatás extra költsége miatt; illetve a Google Cloud valós költségei a mérések idején, a honlapon elérhetőnél alacsonyabbak voltak egy speciális kedvezmény érvényesítésének köszönhetően.

A felhő szolgáltatók esetén az üzemeltetési költség könnyedén kiszámítható, általában óránkénti, vagy havi tarifával számolnak.

(Saját) fizikai számítógépek esetén sokkal nehezebb a költségbecslés, hiszen magába kell, foglalja az áramfogyasztást, a szerverszobák állandó hőmérsékletszabályozását, váratlan meghibásodás költségét, illetve a rendszergazdák bérét. Habár ezen faktorok maximált értékkel felvehetők lehetnének a becslésbe, a végeredmény mindenképp egy elnagyolt érték lenne, így ezeket végül mellőztük a becslésekből a megbízhatatlanságuk miatt.

Néhány felhőszolgáltató, mint a Microsoft, Google és Amazon honlapján elérhető teljes tulajdonlási költség (TCO[63]) kalkulátor, részben azért, hogy a költségtervezést megkönnyítsék, részben, hogy megmutassák, 3 évre vetítve jobban megéri felhőszolgáltatást bérelni. Tapasztalatunk szerint ezek a kalkulátorok nem alkalmazhatók közvetlen az USA-n kívüli országokra (így hazánkra sem), ahol például a munkaerő és az áramszolgáltatás költsége jelentősen eltér az amerikaitól. Így az ezen kalkulátorok által adott eredmények nem hasznosíthatók számunkra, ennek orvoslására inkább kombináltuk a saját teljesítmény méréseinket óránkénti üzemeltetési költségekkel.

4.3.1.2.4 Összesített eredmények

$$C_P = \frac{C_M * t_{sum}}{O}$$

1. képlet: Teljesítmény költség.
(Szerkesztette a szerző.)

[63]Total Cost of Ownership

Az 1. képlet esetén a C_P a számolt teljesítmény költség, C_M az üzemeltetési költség, a t_{sum} a mért teljes futásidő, és az O az összes elvégzett lebegőpontos művelet darabszáma.

Ha megszorozzuk az üzemeltetési költséget (ami a mellékletekben eredetileg Euro/órában szerepel, ezért 3600-zal elosztjuk, hogy végül Euro/másodpercet kapjunk) a mért *sum* értékkel (másodpercben), akkor végül megkapjuk az aktuális mérés költségét Euróban.

Ahogy a WRF összehasonlító mérések hivatalos honlapján [107] olvasható, egy-egy mérés során a műveletszám 30,1 GFLOP. Ha elosztjuk az imént számított mérésenkénti költséget a műveletszámmal, megkapjuk az egy GFLOP-ra vonatkoztatott költséget WRF esetén, Euro/GFLOP mértékben.

A kapott értéket felszorozhatjuk 1000-rel a könnyebb olvashatóság kedvéért, így végül Euro/TFLOP-ot kapunk.

A 8. melléklet ábrázolja a 7. melléklet táblázatának értékeit. Minden *x* tengelyen ábrázolt processzor szálra vonatkoztatva az alacsonyabb *y* érték az olcsóbb, vagyis kevesebb költséggel futtatható ugyanaz a WRF modell ugyanazon paraméterekkel egy olyan számítógépes platformon, aminek *y* értéke közelebb van a 0-hoz.

Jegyezzük meg újra, hogy az MTA Cloudhoz a mérések idején nem állt rendelkezésre költségadat, mert a szolgáltatás akkor még nem volt beárazva, így továbbra is 0-val ábrázoltuk.

Érdekes megfigyelni, hogy bár a Scaleway gépek mért teljesítménye a legrosszabb volt, mégis a szokatlanul olcsó bérleti díj miatt a 4 szálas konfiguráció esetén ez a legköltséghatékonyabb platform WRF futtatásra. Erre a magyarázat az Intel Atom processzorok alacsony áramfogyasztása és költsége lehet – a Scaleway agresszívan olcsó árazási stratégiája mellett.

Ezzel szemben a Microsoft Azure megoldások bizonyultak a legdrágábbnak, valószínűleg a kiegészítő szolgáltatásaik és az árba beépített (ám esetünkben kihasználatlan) terméktámogatás költsége miatt.

Ezen értékek közt helyezkedik el az ábrán az üzleti színvonalú Dell notebook, melynek becsült költsége az egyszeri beszerzési árat (3 év gyártói garanciát beleértve), illetve a maximális áramfelvételt foglalta magába. Egyéb költségektől eltekintettünk, hiszen ez egy piacon elérhető kész notebook konfiguráció.

A 8 szálas mérések azt mutatják, a RackForest fizikai szerverének teljesítmény költsége a Google Cloud és a Cloud.hu közé esik.

A két 16 szálas Cloud.hu konfiguráció eredményei nagyon közel esnek egymáshoz, míg a Google szolgáltatása ennél költségesebb. Emellett egy növekvő trendet is mutat a szálak számával arányosan.

A 32 szálas RackForest adatok azt mutatják, ilyen sok párhuzamos szál esetén már várhatóan jobban megéri fizikai szervert bérelni virtualizált helyett hasonló konfigurációval WRF futtatásokhoz.

4.3.2 Veszélyes meteorológiai jelenségek észlelésének lehetősége

Egyes repülésre veszélyes időjárási jelenségek, mint a jegesedés vagy az erős szél észlelésének lehetősége erősen függ a pilóta nélküli légijármű fedélzeti szenzorai által szolgáltatott adatok elérhetőségétől és minőségétől. A veszélyhelyzet felismerésének, megelőzésének előfeltétele ezért egy megfelelő meteorológiai támogatórendszer kialakítása, illetve sok esetben külső szenzorok elhelyezése szükséges a drónokon.

Korábban kutatók sikeresen alkalmaztak merevszárnyas UAV-kat a planetáris határrétegben hőmérséklet, légnyomás és relatív nedvesség mérésére, illetve egyes rendszerek felszerelhetők egyéb, például széndioxid vagy ózon szenzorral is, ahogy a 9. mellékletben is látható, melyet magam egészítettem ki adatokkal Jack Steward Elston publikációja alapján [108] [S9].

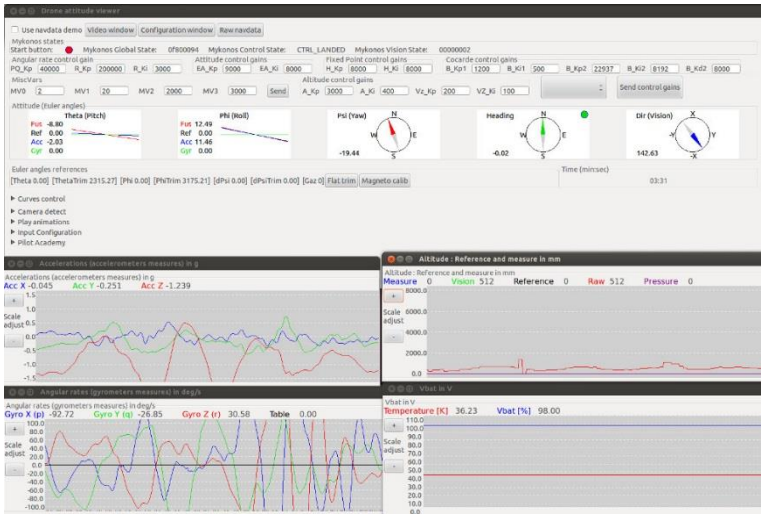
Bottyán Zsolt publikációja alapján [109] pedig elmondható, hogy a repülő eszköz felületi jegesedése leegyszerűsítve akkor kezdődhet meg, ha 0 °C alatti hőmérséklet mellett, berepül a felhőbe. Ennek a körülménynek az észlelése kiegészítő fedélzeti szenzorok (hőmérséklet, relatív nedvesség) elhelyezésével valósítható meg, hiszen drónok alapesetben csak légnyomás mérésére vannak szenzorral felszerelve a repült magasság meghatározásához.

Kvadrokopterek esetén a legújabb áttörést meteorológiai adatgyűjtés szempontjából a különböző fedélzeti, vagy a földi alrendszer által nyújtott szélmérési lehetőségek adják.

A hagyományos külső fedélzeti szenzor (Prandtl-cső, a Pitot-csövek egy altípusa [110]) elhelyezésén túl lehetőség van a szél telemetria vagy pozíció adatok alapján történőbecslésére is. A széllel való sodródásos módszer alkalmazásának előfeltétele a GPS alapú stabilizálás (`POSHOLD`) kikapcsolása az eszközön. A módszernek a nyilvánvaló hátránya, hogy a széllel való sodródáshoz, illetve a szél sebességére gyorsuláshoz az UAV tehetetlenségétől és légellenállásától függően idő és további út megtétele szükséges, így nagyobb szélben az UAV egyre inkább eltávolodik a kiindulási ponttól. Ez a módszer merevszárnyas UAV-k esetén alkalmazható akkor is, ha nem rendelkeznek Pitot-csővel.

Multikopterek esetén a giroszkóp és gyorsulásmérő alapú stabilizálás napjainkra kiegészült a GPS, esetenként kamerakép alapján történő stabilizációval, ami szeles időben is biztosítja, hogy az eszköz egyhelyben tudjon lebegni. A Parrot AR Drone 2.0 esetén a fedélzeti robotpilóta valós időben kielemzi a leszálló kamera képét, és ez alapján a rotorok teljesít-

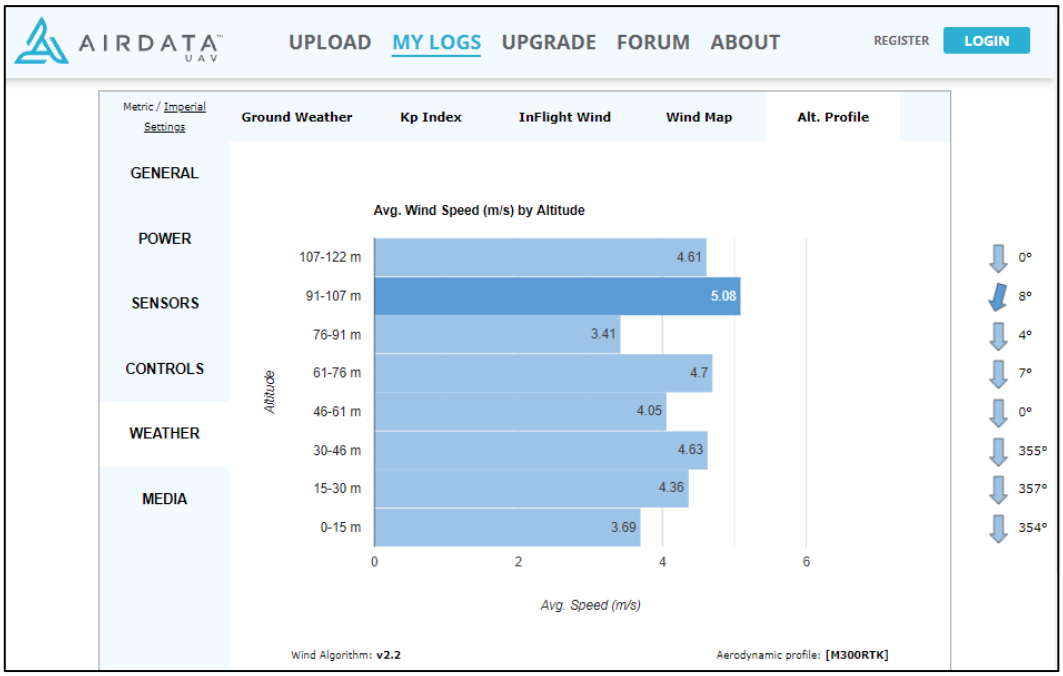
ményét korrigálva tartja a pozíciót. Az adatokat MAVLink 1.0 protokollon, wifin keresztül küldi le a földi állomásnak, ahol a 30. ábrán látható módon grafikusan meg is jeleníti a mért értékeket.



30. ábra: Képernyőkép a Parrot fejlesztői szoftveréből.
(A képernyőképet készítette a szerző.)

A térbeli tengelyeken mért dőlésszögekből kiszámolható, éppen milyen irányba tart ellen a szélnek a repülő eszköz, illetve milyen mértékben.

Ennek a módszernek az egyik előnye, hogy nincs szükség nagy út megtételére, mint a sodródásos módszer esetén, ám több valós idejű számításra van szükség a szél meghatározásához. Így a módszer akár egy városi, utcai környezetben is alkalmazható, hiszen ilyen térben az épületek és egyéb tereptárgyak keltette turbulencia könnyen befolyásolhatja akár méterről-méterre a szélirány változását. Másik előnye, hogy amennyiben a fedélzeti rendszerek számítási kapacitása nem teszi lehetővé a számítások azonnali, biztonságos elvégzését, azok távol is elvégezhetők a gyűjtött telemetria adatok alapján, akár a földi alrendszer keretein belül. A 31. ábrán és a 2. táblázaton ennek a koncepciónak egy modern, kiszolgáló oldali megvalósítása látható a földi alrendszer webes felületén. Az airdata.com weboldal a repülések végeztével (sajnos csak utólag) feltöltött telemetria adatokból a drón típusának és aerodinamikai, illetve tehetetlenségi karakterisztikájának ismeretében képes megbecsülni a szél erősségét és a szélirányt.



31. ábra: Airdata.com széladatok különböző magassági szinteken.
(A képernyőképet készítette a szerző.)

	Repülési idő	Magasság	Horiz. távol-ság	Szélirány	Szélsebesség
a	28m 25s	13.1 m	13 m	0°	4.25 m/s
b	28m 30s	13.0 m	13 m	359°	3.87 m/s
c	28m 35s	13.1 m	13 m	357°	3.70 m/s
d	28m 45s	20.2 m	13 m	351°	2.42 m/s
e	28m 50s	45.2 m	13 m	346°	3.08 m/s
f	28m 55s	55.5 m	14 m	0°	2.62 m/s
g	29m 00s	58.0 m	14 m	349°	2.73 m/s
h	29m 05s	82.6 m	13 m	11°	2.18 m/s
i	29m 10s	85.5 m	14 m	1°	2.66 m/s
j	29m 15s	85.6 m	14 m	357°	2.87 m/s
k	29m 20s	85.6 m	14 m	9°	2.64 m/s
l	29m 30s	87.9 m	14 m	3°	2.84 m/s
m	29m 35s	94.4 m	14 m	19°	2.94 m/s
n	29m 40s	115.7 m	13 m	355°	3.67 m/s

2. táblázat: Airdata.com példa széladatok táblázata.
(A táblázatot fordította és szerkesztette a szerző az airdata.com egy repülésének adatai alapján)

Egy Mission as a Service szolgáltatás meteorológiai alrendszere esetén az előnyöket figyelembevéve érdemes az utóbbi módszert alkalmazni – vagyis az elérhető, ha lehet, élő telemetria adatokból számítani a szél adatokat, jelentős széllökéseket észlelve pedig a távpilótát figyelmeztetni, az aktuális repülő eszköz útvonalát szükség esetén távolról módosítani, végszükség esetén leszállítani az UAV-t.

4.3.3 Veszélyes meteorológiai jelenségek autonóm elkerülésének lehetősége

A MAVLink 2.0 protokoll lehetőséget ad külső eszköz csatlakoztatására a robotpilótához, ami eldöntheti, engedélyezi-e felszállás előtt az élesítést. Ahogy a dokumentáció is kifejezetten példaként említi, [111] ez a külső eszköz például a helyi időjárási adatokat is ellenőrizheti, és ez alapján GO/NO GO döntést hozhat egy felszállás előtti ellenőrzőlista részeként.

Ha a robotpilóta hardverkialakítása és az UAV képességei lehetővé teszik külső eszköz csatlakoztatását a robotpilótához, további MAVLink alapú lehetőségeket is kihasználhatunk. A külső eszköz hozhat döntéseket a repülés biztonságának megítélését követően, figyelmeztetheti a távpilótát az esetleges veszélyekre, vagy akár be is avatkozhat a küldetésbe. Lehetőség nyílhat amolyan dinamikus NDZ-t létrehozni az időjárási előrejelzés alapján (előzetesen a küldetés megkezdése előtt, vagy online valós időben), elkerülve a veszélyes időjárási jelenségeket.

4.4 Következtetések

A rendszer funkcionális, repülési feladatokhoz kapcsolódó képességeit terepi repültetésekkel tettem próbára, miután egyes kritikus kérdéseket a piacon elérhető földi irányító szoftverekkel összevetve verifikáltam. A tesztesetek végrehajtása után elmondható, hogy UAV-k felhő alapú távirányítása, nyomkövetése működik még akkor is, ha az irányító szerver szó szerint a világ túloldalán van fizikailag, így minden üzenet 15 000 kilométert kellett, hogy megtegyen Szolnok és Chicago között a parancs végrehajtása, illetve a térképes felületen történő visszajelzés előtt. Az ezzel járó 150 ezredmásodperc késleltetés elfogadhatónak bizonyult a rendszer funkcionalitása szempontjából.

A maghálózat funkcionalitása és nemfunkcionális képességei egyaránt egy több számítógépből álló konfiguráció felhasználásával kerültek bemutatásra. Példaként kiemelném a skálázhatóságot, túlélőképességet és a munkamenetek perzisztenciáját több párhuzamosan működő UAV szimulálása esetén.

A hálózati kapcsolat fizikai megszakításával és a rendszer szándékos túlterhelésével, a szimulált drónok küldetés közben történő átmigrálásával megmutattam, hogy a felhő alapú

irányítás elősegíti az UAS-k fizikai biztonsági szempontból megfelelő működtetetését. Ehhez viszonyítva egy hagyományos fizikai kiszolgáló esetén a telephely megsemmisülése, a hálózat megszakadása, a rendszer túlterhelése sokkal katasztrofálisabb eredményekkel járt volna a szolgáltatás szempontjából – várhatóan ebben az esetben elveszett vagy sérült volna az épp levegőben lévő drónok távirányításának, nyomon követhetőségének lehetősége.

A konténerizált WRF-fel végrehajtott tesztek alapján elmondható, hogy a kevesebb szálon végzett modell futtatások esetén költségvetésileg jobban megéri felhő szolgáltatást bérelni, míg nagyobb párhuzamosságú esetekben olcsóbb dedikált fizikai szervert bérelni, feltéve, hogy folyamatos terhelés alatt tartjuk a rendszert hosszú távon is. Mindazonáltal nagyon nehéz meghúzni a határozott vonalat, ahol egyértelműen eldönthetjük, mikortól éri meg dedikált fizikai szerverre áttérni. A pontos meghatározáshoz még több, változatosabb konfigurációra és pontosabb mérésekre, illetve főként pontosabb költség adatokra lenne szükség.

5 ADMINISZTRATÍV BIZTONSÁGI KÉRDÉSEK

Adminisztratív biztonság alatt esetünkben a pilóta nélküli repülő eszközök és repülések személyekhez köthetőségét, számonkérhetőségét értem; illetve a hardveres, szoftveres és adatbeszállítók láncolatának lekövethetőségét, számonkérhetőségét sorolom ide. Ezen megfontolások kiemelt fontossággal bírnak a jogszabályi megfelelés szempontjából.

5.1 UAS-specifikus PKI

Itt az alapötlet kliensoldali tanúsítványok kiosztása internet-képes drónok számára, amit földi állomásokkal, egyéb drónokkal és eszközökkel való biztonságos kommunikációhoz használhatnak. Ezúton elektronikusan ellenőrizhető az identitásuk. A tanúsítvány kiállításához az üzembentartó felveszi a kapcsolatot az RA-val, ami ellenőrzi az üzembentartó személyazonosságát és jogilag hozzárendeli a drónt a rendszerben.

„A PKI-t érintő legfőbb probléma a kulcsok elosztása és kezelése, ami arányaiban egyszerű zárt, katonai rendszerekben, ám nehézkes a polgári repülés nyílt és világszintű rendszerében, ami kompatibilitási követelményeket is magával vonz.” [113].

Kulcselosztás és -kezelés szempontjából két fő irányvonal létezik a titkos privát kulcsok kezelésére. Az egyik, hogy az üzembentartók maguk generálják a kulcspárt, majd kitöltik a CSR-t és továbbítják a hatóság felé. Így csak az üzembentartó kezeli a privát kulcsot, vagyis még maga a hatóság sem élhet vissza vele vagy személyesítheti meg az üzembentartót a rendszerben – ám az üzembentartónak egy bonyolultabb, kevésbé felhasználóbarát folyamatot kell végrehajtania, hogy legenerálja a kulcspárt és biztonságosan letárolja a privát kulcsot az eszközön. A másik módszer, hogy a hatóság vagy jogi megbízottja generálja és adja ki a kulcspárt a felhasználó felé valamilyen biztonságos kommunikációs csatornán. Ez történhet például SIM kártya, SD kártya, USB pendrive kiosztásával, ami csatlakoztatható az eszközhöz; az eszköz közvetlen konfigurációjával (pl. eSIM); vagy a kulcspár az üzembentartó fizikai jelenlétében, izolált és ideiglenes informatikai környezetben történő generálásával, biztosítva, hogy azt ne lehessen később visszanyerni. Ezek a módszerek leveszik az üzembentartó válláról a kulcsgenerálás terhét, ám lehetőséget hagynak a privát kulcs kiszivárgására a folyamat során.

A fenti idézetnek megfelelően, ezeket az eljárásokat könnyebb megvalósítani egy saját, elkülönített, zárt PKI megoldás esetén, mint integrálni őket a világszintű internetes PKI rendszerébe. Azért, hogy a piaci igényeket kielégítsék, több vállalat is megoldással rukkolt elő a problémára.

Az Infineon és a PrimeKey társult, hogy biztonságos drón PKI-t szolgáltasson, OPTIGA™ Trust X és NC1023 (eSIM) alkalmazásával [114]. A rendszer nem csak a drónok azonosítására képes, hanem a rajtuk futó szoftver távoli ellenőrzésére is, hogy megelőzze például tört szoftver drónon való futtatását, amivel az NDZ-k figyelmen kívül hagyhatók lennének.
A DigiCert és AirMap szintén bemutatta saját megoldását, ami nyíltan ellenőrizhető tanúsítványt szolgáltat, DroneID fedőnév alatt. A megoldás elsőkörben az Intel® Aero fejlesztői platformmal kompatibilis drónok számára elérhető, beleértve az Intel Aero Ready to Fly drónt [115]. A megoldás a biztonságos azonosításra és kommunikációra fekteti a hangsúlyt a pilóta nélküli légijármű rendszeren belül.
Katonai felhasználás szempontjából ugyancsak vizsgálták a PKI lehetőségei IoT és UAV azonosítás és ellenőrzés területén. A Norvég Védelmi Kutató Intézet (Norwegian Defence Research Establishment) munkatársai megvizsgálták a PKI és megbízható platform modul (TPM[64]) chipek lehetőségeit érzékeny adatok hardveres tárolására és integritásvédelmére, a Gismo IdM identitásmenedzsment megoldással végzett kísérleteiken túl [116].
Szabványosítás terén az ITU-T és az ISO működik együtt egy új UAV azonosító kidolgozásán [117]. Az általuk javasolt jövőbeli megoldás az objektumazonosítók (OID[65]) [118] koncepciója, mely várhatóan majd az Nemzetközi Polgári Repülési Szervezet (ICAO[66]) által is alkalmazásra kerül. Ezeken túl Amerikai Nemzeti Szabványügyi Intézet (ANSI[67]) szabvány is létezik az UAS-k sorozatszámainak nevezéktanára [119].

5.2 Egy lehetséges európai megközelítés

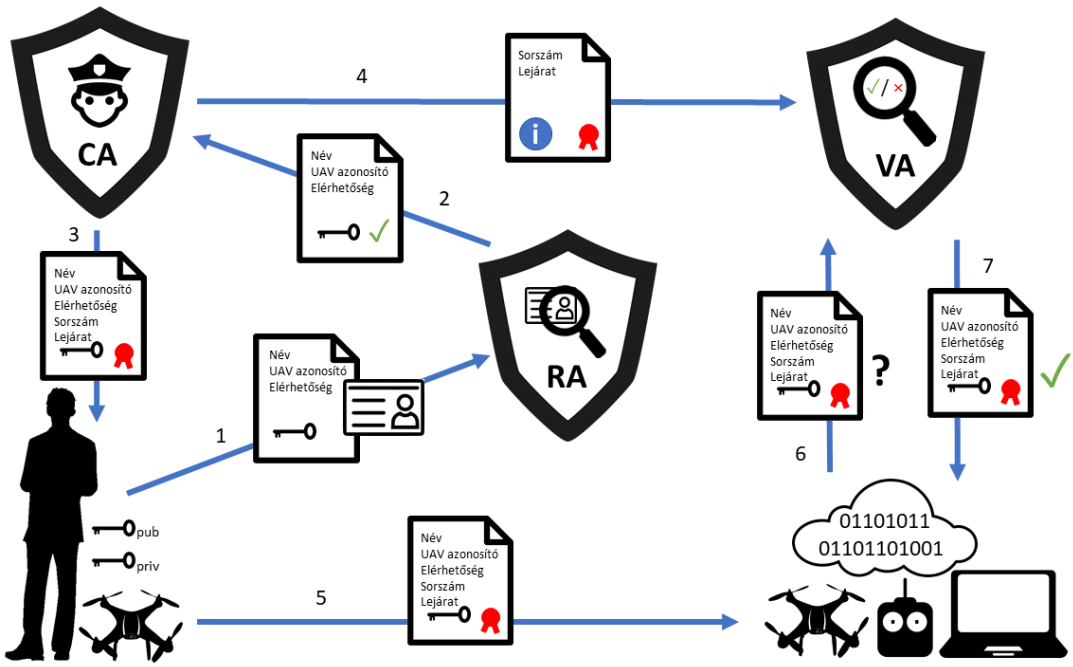
„2020. december 31-ével kötelezővé válik a drón üzembentartók és a tanúsított drónok regisztrációja." [120].

Az üzembentartók regisztrációjának megkövetelésén túl az Európai Unió előírásai különböző kategóriákat határoznak meg a művelet természetétől [24] és az UAS karakterisztikájától [25] függően. A C1, C2 és C3 kategóriájú UAS-k egyedi ANSI/CTA-2063 sorozatszámmal [119] kell, hogy rendelkezzenek, amit fizikailag és elektronikusan is el kell helyezni a drónon, illetve ezt elektronikusan is sugároznia kell a műveletek során. A regisztrációs folyamat során a sorozatszám mellett a gyártó és az üzembentartó adatai is feltöltésre kerülnek a drónra vagy egy külső fedélzeti azonosító eszközre.

[64] Trusted Platform Module
[65] Object IDentifier
[66] International Civil Aviation Organization
[67] American National Standards Institute

Hogy ezeket az előírásokat a nyilvános kulcsú infrastruktúra koncepciójába illesszük, a szükséges adatokat az internetképes UAS tanúsítványába is foglalhatjuk elektronikus azonosítás céljából, a kommunikációhoz generált nyilvános kulccsal együtt. A regisztráció elektronikus úton az üzembentartó személyazonosságának megfelelő igazolása után történhet online (például Ügyfélkapu azonosítás után), vagy személyesen egy államilag elismert drón klubban. Ezesetben az e-kormányzati szolgáltatás vagy a klub tölti be az RA szerepét a PKI nyelvén.

A CA szerepet nemzeti, európai (mint gyökér CA vagy köztes CA) vagy világszintű (ICAO mint gyökér CA) infrastruktúra tölthetné be. A gyökér CA tanúsítvány a drónra vagy az azonosító eszközre kerülne feltöltésre. Így a fedélzeti rendszer maga is képes verifikálni a hálózatra kapcsolt más rendszereket, amiket egyazon tanúsítási láncban tanúsítottak – például irányító szervereket, IP alapú távirányítókat vagy más drónokat a kommunikáció során. A felvázolt tanúsítási és azonosítási folyamat végigkövethető a 32. ábrán.



32. ábra: PKI alapú UAS biztonság.
(A képet szerkesztette a szerző.)

A drón saját tanúsítványa használható az irányító hálózatba való bejelentkezéshez élesítés és felszállás előtt. A drón platform képességeitől függően a privát kulcs tárolható a drónon PKCS12 formátumú fájlban, SIM kártyába / eSIM-be ágyazva, vagy TPM chipbe zárolva. A tanúsítvány alapú azonosítás lehetővé teszi minden naplózott kommunikációs lépés vis--szakövethetőségét, és így az üzembentartók számon kérhetőségét a rendszerben.

5.3 Releváns specifikációk

5.3.1 Amerikai Egyesült Államok

A Tesztelés és Anyagok Amerikai Társasága (ASTM[68]) F3411-es számú távoli azonosítási és nyomkövetési specifikációja az UAS-k azonosítóinak, helyzetének stb. közvetlen szórt üzenetként (Bluetooth, wifi), vagy interneten át távoli szerver felé történő közzétételének módjára tesz ajánlást.

A szabványnak jelenleg az 1.0-ás változata [121] elérhető. Hamarosan várható egy kiegészített változat is, ami az FAA által UAS-k felé támasztott követelményeknek [122] való további megfelelést célozza az Egyesült Államok területén.

Továbbá egy, a követelményeknek történő megfeleléshez szükséges további megvalósítási részleteket és tesztspecifikációkat tartalmazó különálló dokumentum is kidolgozás alatt van. A két dokumentum együttesen a gyártókat segíti abban, hogy az elvárásoknak megfelelő távoli azonosítással rendelkező drónokat vagy külső azonosítási eszközöket szállíthassanak (melyekkel a már piacon elérhető, jeladó nélküli drónok utólag felszerelhetők), és elkészíthessék a szükséges megfelelési nyilatkozatokat, amelyeket az FAA részére szükséges benyújtani.

5.3.2 Európa

Az Európai Bizottság 2019/945-ös számú felhatalmazáson alapuló rendeletében és a Bizottság 2019/947es számú végrehajtási rendeletében megszabott feltételek teljesítéséhez a Légiközlekedési és Védelmi Ipari Szereplők Szervezete – Szabványügy (ASD-STAN[69]) kidolgozta a prEN 4709-002 közvetlen távoli azonosítási szabványt. Ez a szabvány a fenti szabványhoz hasonlóan Bluetooth- és wifi-alapú távoli azonosítási módszereket határoz meg, amik kompatibilisek az ASTM F3411 specifikációjával. A véglegesített verzió jelenleg még nem elérhető, ám vázlat formájában megtalálható az ASD-STAN honlapján, [123] mely jelenleg is revízió alatt áll.

5.4 Ellátási lánc biztonság

Mission as a Service szolgáltatások esetén külön figyelmet érdemel az ellátási lánc biztonsága, mind hardver, mind szoftver és akár nyers adat szinten. A robotpilótához csatlakoztatott külső eszköz tartalmazhat hardveres biztonsági kiskapukat, amivel akár távolról átvehető felette az irányítás, vagy lehallgathatók a kiküldött adatok [124]. A firmware megva-

[68] American Society for Testing and Materials
[69] AeroSpace and Defence Industries Association of Europe - Standardization

lósításban is előfordulhatnak sebezhetőségek, a külső eszköz támogathat például elavult titkosítási algoritmusokat a kommunikáció során, aminek kihasználásával hamis adatok juttathatók az adatfolyamba, vagy lehallgathatók a küldött adatok. Ezért, amennyiben lehetőség adódik rá – online eszköz esetén –, érdemes engedélyezni az automatikus frissítés funkciót, hiszen napról napra bukkanhatnak fel újabb és újabb sebezhetőségek, amelyekre a javítás például a gyártó honlapján, vagy egy központi szoftver repozitóriumban lehet elérhető. Veszélyes időjárási jelenségek automatikus elkerülése esetén az előrejelzés elkészítéséhez szükséges bemeneti adatok is jelenthetnek egy újabb, speciális támadási felületet, például ha egy támadó sikeresen módosítja az Országos Meteorológia Szolgálat által nyújtott, Open Data Policy-n keresztül elérhető adatokat úgy, hogy a későbbi, erre épülő előrejelzések ennek hatására zivatart jósoljanak a küldetés útvonala mentén, annak hatására a külső eszköz beavatkozhat a repülésbe, és új útvonalra terelheti az UAV-t. Ha visszaemlékezünk a korábbi fejezetekben hivatkozott cikkre, [6] a publikáció szerint az RQ-170 típusú UAV eltérítése is hasonlóan zajlott, viszont ott a GPS jel fentiekhez hasonló elvű eltérítésével vették át az irányítást a támadók a légijármű felett.

5.5 A felhőben kezelt adatok

A webes alkalmazások esetén mondhatni „szokásos”, Általános adatvédelmi rendelet (GDPR[70]) [125] által lefedett személyes adatokon túlmenően egy felhő alapú UTM rendszerben a következő típusú, nem feltétlen személyes, viszont kritikus fontosságú adatok [126] kezelése is szükséges:

- nyilvántartási adatok;
- az UAS-sal összefüggő felhasználói (távpilóta, üzembentartó stb.) adatok;
- légiforgalmi tájékoztató szolgálatok (AIS[71]) adatai;
- légi infrastruktúra adatok;
- repülési terv adatok;
- forgalmi adatok;
- repülés műveleti adatok;
- berendezés adatok;
- kényszerhelyzeti adatok;
- légtérfelderítési adatok;

[70] General Data Protection Regulation
[71] Aeronautical Information Service

– hatósági adatok.

Ezek állandóságukat tekintve lehetnek statikus (repülés közben változatlan), féldinamikus (legfeljebb pár óránként változó), dinamikus (akár másodpercenként frissülő) és valós idejű adatok. Biztonság szempontjából érdemes kiemelni, hogy egy nemzetközi felhő infrastruktúrában nemzetbiztonsági kérdés lehet, hogy a fentiek közül mely adatok, mely partnerállamok földrajzi területén kerülnek tárolásra, ehhez kapcsolódóan kockázatelemzést és -kezelést kell végezni az adatokkal történő esetleges visszaélések kockázatának csökkentésére, az esetleges incidensek megelőzésére.

5.6 Következtetések

Mind az UAV műveletek nyomon követése, mind a távpilóták és drónjaik nyilvántartásba vétele kulcskérdés repülésbiztonság szempontjából. Az EU által előírt elektronikus nyomkövetés biztonsági alapjainak kiszolgálására egy járható út lehet a fent általam felvázolt kormányzati, UAS-specifikus nyilvános kulcsú infrastruktúra modell. Ehhez hasonló elven működő piaci koncepció kidolgozására, megvalósítására külföldi kutatások és piacvezető ipari szereplőkből álló társulások is alapultak, melyek a drónok kommunikációs csatornáinak biztonságossá tételére is nagy hangsúlyt fektetnek. Ezek a megoldások piacon megvásárolható megoldásokra épülnek; miközben arra is láthattunk példát, hogy katonai IoT és drón rendszerek zárt PKI alapokra helyezésére is folynak kísérletek.

A felhő rendszerek belső kommunikációjának biztosítása is általában hasonló nyílt vagy zárt PKI alapokon történik, tanúsítványok felhasználásával, így ez az általam kidolgozott megközelítés a felhő infrastruktúra szintjén is sikerrel alkalmazható, de ezen túlmenően a felhőhöz csatlakozó UAV-k, mint kliensek azonosítása is integrálható ebbe a megoldásba.

A fenti megállapításoknak megfelelően kimondható, hogy a felhő alapú irányítás elősegítheti az UAS-k adminisztratív biztonsági szempontból megfelelő működtetetését, amennyiben alkalmazzuk az iparban felhő rendszerek esetén elterjedten használt PKI megoldást a csatlakozó kliens eszközök (drónok) hitelesítésére is.

Egy összetett hardver, firmware, szoftver komponensekből és változatos adatforrásokból álló Mission as a Service rendszer esetén fontos kérdés ezeknek az ellátási láncát a biztonságot kiemelten szem előtt tartva megtervezni. A bemutatott példák rávilágítanak arra, hogy az ilyen rendszerek esetén korábban nem látott támadási felületek létezhetnek, illetve a korábban felismert, általánosan a felhőhöz kapcsolódó kockázatokat esetenként át kell értékelni, mivel az irányított UAV-kon keresztül a támadásoknak közvetlen kihatása lehet

a fizikai világra is, ezzel magában hordozva a személyi sérülés kockázatát, ezzel súlyosbítva a kockázat hatásfaktorát.

Különleges megfontolást igényelnek a felsorolt, felhő rendszerekben tárolt repüléshez kapcsoló adatcsoportok, melyek hozzáférhetőségi és kockázati szintjeit körültekintően szükséges megállapítani egy ilyen repülésbiztonságilag kritikus rendszerben. Nemzetközi rendszerek esetén ezen adatok elhelyezése akár nemzetbiztonsági kérdés is lehet.

6 SZEMÉLYI BIZTONSÁGI KÉRDÉSEK

Személyi biztonság alatt a drónok illetéktelenek általi eltérítésének, jogosulatlan vagy jogtalan használatának megelőzését értem. Biztosítani kell a rendszerben, hogy a drónokhoz a kizárólag a megfelelő személyek férjenek hozzá, csak ők aktiválhassák, ez a jogosultság távolról visszavonható legyen, illetve szükség esetén a hatóság beavatkozhasson a repülésbe. A PKI koncepciót elterjedten és sikeresen alkalmazzák felhő infrastruktúra kialakítása kapcsán, [127] így ebben a fejezetben inkább az UAV oldal kihívásaira koncentrálok.

6.1 Személyre szóló tanúsítvány

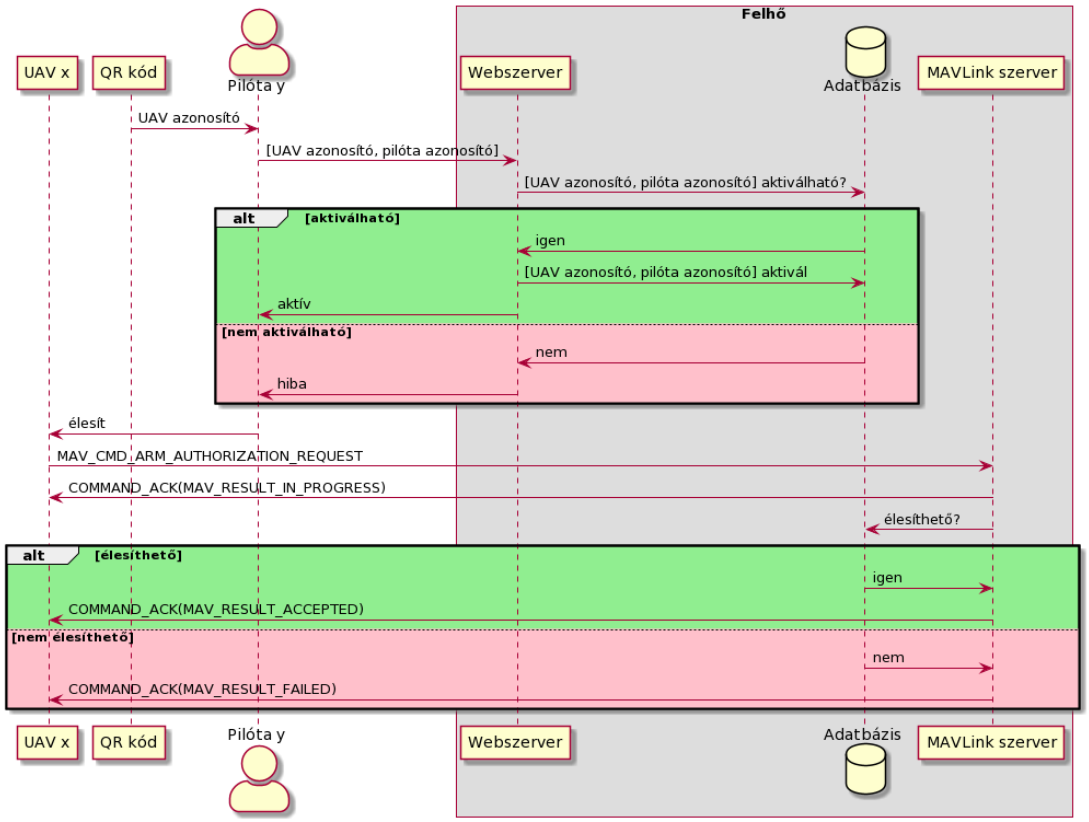
Az 5.2 fejezetben bemutatott koncepciót alkalmazva lehetőség nyílik a pilóta nélküli légijárművek elektronikus regisztrációjára és az üzembentartók nyilvántartására, egyértelmű beazonosítására.

6.2 Külső engedélyező eszköz

A MAVLink 2.0 lehetőséget ad egy külső engedélyező eszköz beiktatására is a drón élesítésének folyamatába. Ez a külső eszköz tetszőleges kiértékeléseket végezhet, melyek alapján eldönti, hogy engedélyezi-e az élesítést vagy nem. A döntés során figyelembe veheti például a meteorológiai előrejelzést vagy a valós körülményeket ahogy korábban a 4.3.2 fejezetben említettem, vagy akár a légtér állapotát is ellenőrizheti, lehetőség szerint aktiválhatja azt felszálláskor. Megoldást nyújthat arra az esetre is, hogy elektronikusan hogyan lehet az egyes drónokat a távpilótához rendelni közvetlen a felszállás előtt, illetve aktiválni azt, biztosítva, hogy csak arra jogosultak tudják élesíteni a drónt. Ahogy a 33. ábrán látható, a távpilóta például egy alkalmazásba belépve beüthetne egy a drónon elhelyezett azonosító számot, vagy beszkennelhetne egy QR kódot, ezzel magához rendelve azt. A távpilóta és a drón összerendelésének feltételeit egy központi (akár felhő alapú) webes alkalmazás tudja ellenőrizni, melynek eredményét az élesítést jóváhagyó külső eszköz lekérdezheti. Hasonló elképzelésen alapul a Lime elektromos roller bérlő rendszer működése is [128].

33. ábra: QR-kód alapú UAV aktiválás interneten át.
(Az ábrát szerkesztette a szerző.)

Ennek az elképzelésnek egy előnye, hogy elektronikusan, gyorsan és kényelmesen aktiválni lehet a drónt, ami egyértelműen az aktuális távpilótához lesz kötve, így például egy céges drón flottán belül osztozni lehet a légijárművön, miközben annak használata folyamatosan nyomon követhető, és a számonkérhetőség is biztosított. Ezen túlmenően, a flottához tartozó pilóták listája az adatbázisban központilag menedzselhető ezzel a módszerrel, vagyis tetszőlegesen oszthatók ki a jogosultságok, azok megvonhatók, ha például a távpilóta elhagyja a szervezetet, vagy ha valaki illetéktelenül fér hozzá a drónhoz, nem lesz képes aktiválni azt. Az aktiválás és élesítés folyamata különböző döntési lehetőségekkel végigkövethető a 34. ábrán, melyet magam dolgoztam ki a Lime koncepciója alapján, azt drónokra és MAVLinkre kiterjesztve.



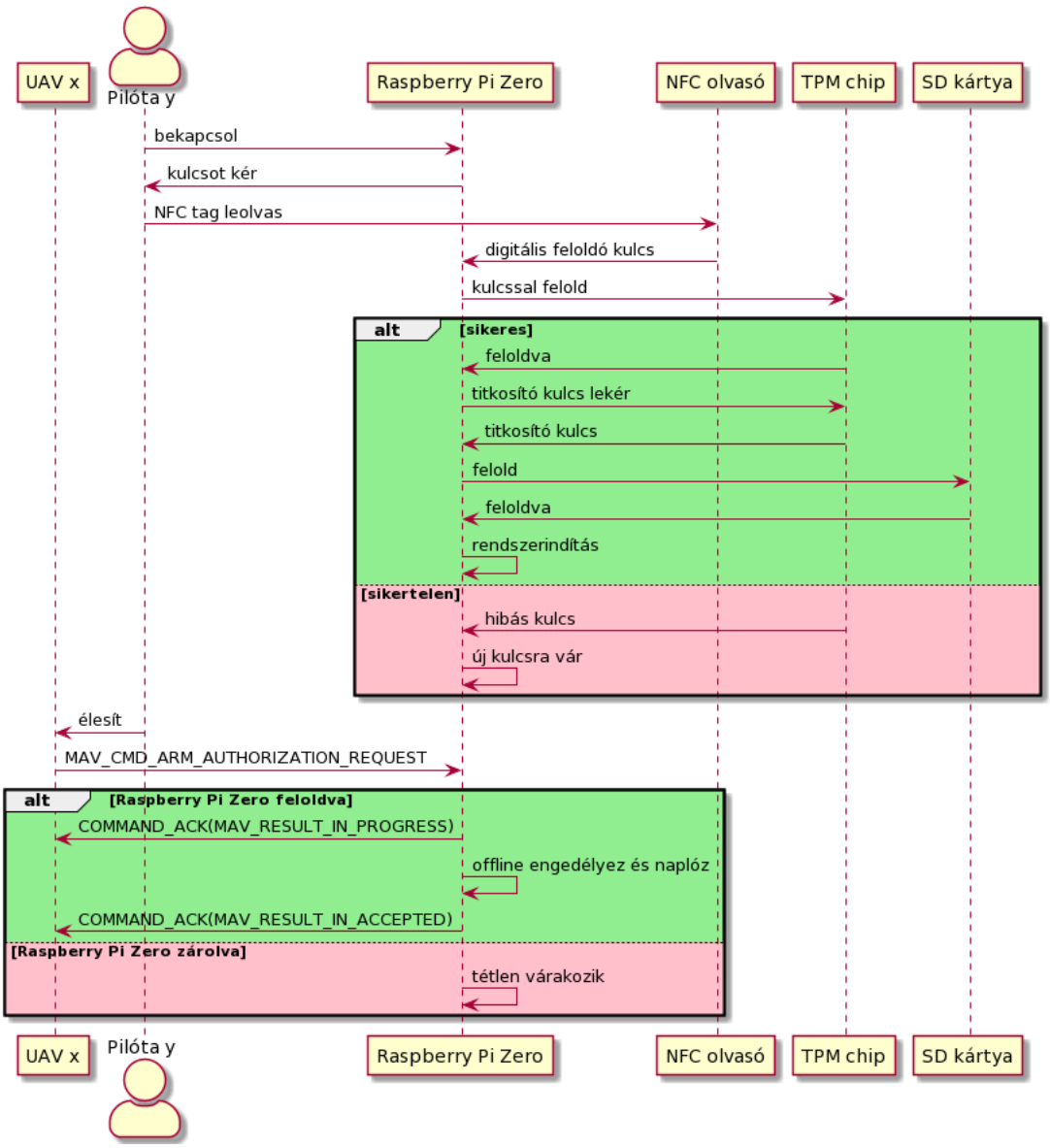
34. ábra: QR-kód alapú UAV aktiválás folyamata interneten át.
(Az ábrát szerkesztette a szerző.)

Ahogy korábban az 5.1 fejezetben említettem, kutatók kísérleti jelleggel már helyeztek el TPM chipet UAV-k fedélzetén. Ez a megközelítés alkalmazható például a külső engedélyező eszköz védelmére is, a rajta futó szoftver módosítás elleni védelmének és az eszközön tárolt kulcsok bizalmasságának biztosítására. A drónok általános felhasználása esetén nem lenne túl kényelmes a terepen külső billentyűzetet vagy egyéb hagyományos beviteli módot alkalmazni a TPM chip feloldásához, ezért érdemes lehet inkább kis hatótávolságú rádiófrekvenciás azonosító (RFID[72]) technológiával, például rövid hatótávú kommunikációs (NFC[73]) olvasóval kibővíteni a külső engedélyező eszközt – például egy közkedvelt Raspberry Pi Zero-t, ahogy azt a 35. ábra szemlélteti. Kollégáimmal jelenleg is erre a mikroszámítógép platformra alapozzuk a különböző fedélzeti meteorológiai rendszert érintő fejlesztéseket [129].

[72] Radio Frequency IDentification
[73] Near Field Communication

35. ábra: UAS NFC alapú feloldása repülés előtt.
(Az ábrát szerkesztette a szerző.)

A kártya vagy egyéb NFC címke (matrica, kulcstartó, okostelefon) leolvasóhoz közelítésével a TPM chip feloldható, így abból a rendszerindítás során kinyerhető a memóriakártya feloldásához szükséges kulcs. Ennek a megközelítésnek egy előnye, hogy egyszerű jelszavak vagy pin-kódok helyek nagyobb komplexitású kulcsok alkalmazhatók, melyeket mégsem kell a felhasználónak (távpilótának) fejben tartania. Az eszköz ilyesfajta feloldásának egy lehetséges folyamata a 36. ábrán látható, melyet magam dolgoztam ki a korábban említett TPM-mel támogatott rendszerbetöltés koncepciójának kiterjesztésével, kézi jelszó bevitel helyett NFC címke leolvasást alkalmazva, és MAVLink alapú engedélyezéssel kiegészítve.



36. ábra: UAS NFC alapú feloldásának folyamata repülés előtt.
(Az ábrát szerkesztette a szerző.)

A memóriakártya titkosításán túl a TPM chipbe speciális, rendszerindítás alatt futó szoftverekkel lenyomatok is letárolhatók az indítás különböző szintjeiről (BIOS, kernel, rendszerbetöltő stb.), így a lenyomatok változásának akár távoli észlelésekor következtethetünk boot-idejű kártékony programok jelenlétére az eszközön, melynek hatására az kitiltható a hálózatból [130].

6.3 Repülési szabályok ellenőrzése és hatósági beavatkozás

„A U-space szolgáltatóknak folyamatosan ellenőrizniük kell a már kiadott repülési engedélyeket, szem előtt tartva az új dinamikus légtérkorlátozásokat és egyéb korlátozásokat, valamint az érintett légiforgalmi szolgálati egységek által a pilótával rendelkező légi járművekre vonatkozóan megosztott információkat és különösen azokat, amelyek szerint egy piló-

távval rendelkező légi jármű biztosan vagy feltételezhetően vészhelyzetben van, ideértve a jogellenes beavatkozást is, és a körülményeknek megfelelően frissíteniük kell vagy vissza kell vonniuk az engedélyeket." [26, 10. cikk].

„Amennyiben a megfelelőség-ellenőrzési szolgálat a repülési engedélytől való eltérést észlel, a U-space szolgáltató figyelmezteti az érintett UAS közelében működő többi UAS-üzembentartót, az ugyanabban a légtérben szolgáltatásokat nyújtó többi U-space szolgáltatót és az érintett légiforgalmi szolgálati egységeket, és ezeknek vissza kell igazolniuk a riasztást." [26, 13. cikk].

Ha a hatóság előírja egy saját publikus kulcsának engedélyezését a drón fedélzetén amolyan kiskapuként veszély esetére, lehetősége adódik távolról beavatkozni a repülésbe is, például visszafordítani vagy leszállítani a pilóta nélküli légijárművet légtérsértés vagy veszélyes repülési helyzet kialakulása miatt.

„*A U-space szolgáltatók minden UAS repülési engedélyhez egyedi engedélyszámot rendelnek. Ennek a számnak lehetővé kell tennie az engedélyezett repülés, az UAS-üzembentartó és az UAS repülési engedélyét kiállító U-space szolgáltató azonosítását."* [26, 10. cikk].

Amennyiben a drón vagy külső engedélyező eszköz bejelentkezik egy központi rendszerbe felszállás előtt, hogy elektronikusan aktiválja a drónt, adott a lehetőség a regisztrált üzembentartójához vagy az aktivált távpilótához tartozó légtér(rendszer) azonnali aktiválására is a jelenlegi pozíció vagy a küldetés útvonalterve alapján. Ha a légtér geometriája is lekérhető elektronikusan, a robotpilótában akár ez földrajzi elkerítés („geofence") formájában is felkonfigurálható automatikusan, melyet nem enged elhagyni a robotpilóta szoftver. MAVLink esetén lehetőség van inkluzív és exkluzív kerítés definiálására is: előbbi biztosítva, hogy a drón ne hagyja el a számára kijelölt légteret, utóbbival pedig gyakorlatilag egy NDZ valósítható meg.

6.4 OpenDroneID üzenettípusok MAVLink 2.0 esetén

Az európai U-space koncepció [26] szerves részét képezi a hálózatazonosító szolgáltatás [26, 8. cikk]. A hálózatazonosító szolgáltatásnak lehetővé kell tennie az UAS-ek távoli azonosítása során nyert adatok folyamatos feldolgozását a repülés teljes időtartama alatt, és az UAS-ek távoli azonosítására vonatkozó adatok rendelkezésre állását a következő jogosult felhasználók számára:

- A nyilvánosság, az alkalmazandó uniós és nemzeti szabályokkal összhangban nyilvánosnak minősülő információk tekintetében.

- Egyéb U-space szolgáltatók, a U-space légtérben végzett műveletek biztonságának garantálása érdekében.
- Az érintett légiforgalmi szolgáltatók.
- A kizárólagos közös információs szolgáltató, amennyiben kijelölésre került ilyen.
- Az érintett, illetékes hatóságok.

Az előírt, UAS-ek azonosítására vonatkozó adatokat a következő OpenDroneID üzenetek hordozzák MAVLink 2.0 esetén.

Megjegyzés: A következő összefoglalás az OpenDroneID MAVLink 2.0-ra vonatkozó dokumentációjának munkapéldánya alapján készült, [131] aminek tartalma időközben változhatott. A legfrissebb specifikációért javaslom felkeresni az eredeti forrást.

6.4.1 BASIC_ID

Ez az üzenet azonosítót biztosít az UAS számára, leírja az azonosító és az UAV típusát. Az üzenet megfelel az ASTM távoli azonosítás és ASD-STAN közvetlen távoli azonosítás szabványoknak.

Az UAV azonosítója a következő formátumoknak felelhet meg:

1. Gyártói sorozatszám (ANSI/CTA-2063 formátumban).
2. Polgári Légügyi Hatóság (CAA[74]) regisztrációs szám ([ICAO országkód].[CAA által kiosztott azonosító] formátumban).
3. UTM által kiosztott univerzális egyedi azonosító (UUID[75]) (RFC4122 formátumban).
4. Típusfüggő repülés/munkamenet azonosító 20 bájt terjedelemben. A pontos típust az UAS azonosító első bájtja szabja meg, melyet az ICAO állapít meg.

Az átjátszott üzenetek visszakövetésének biztosítására az eredeti küldő azonosítója az `id_or_mac` mezőben kerül feltüntetésre.

6.4.2 LOCATION

Az UAS pozícióját, repülési magasságát, haladási irányát és sebességét, illetve azok pontosságát adja meg, egy időbélyeggel együtt.

6.4.3 AUTHENTICATION

Az UAV hitelesítésre ad lehetőséget. Két különböző formátumot vehet fel, több részletből álló üzenet esetén:

[74] Civil Aviation Authority
[75] Universally Unique IDentifier

1. Az első csomag a darabszám, hossz és időbélyegen kívül 17 bájt hitelesítésre szolgáló adatot tartalmazhat.
2. A további csomagokban nem szerepel darabszám, hossz és időbélyeg, cserébe 23 bájtnyi hitelesítési adatot hordozhatnak.

Az `AUTHENTICATION` üzenetek biztonsága jelenleg kevéssé kidolgozott, a szükséges lenyomatok/aláírások elkészítésére, a kulcscserére/kiosztásra, hitelesítésre és a túloldal azonosítására irányuló eljárások még kidolgozás alatt állnak. Ezekre megoldást nyújthat az internetes erőforrások (pl. honlapok) esetén évtizedek óta elterjedten használt PKI megoldás.

6.4.4 SELF_ID

Nyíltszövegű üzenet, amivel a távpilóták opcionálisan azonosíthatják magukat és a művelet célját. Az üzenet további információkkal szolgálhat, ami bizonyos esetekben segíthet csökkenteni a művelet kockázati besorolását.

6.4.5 SYSTEM

Tartalmazza a távpilóta helyzetét és egyéb információkat, például drónrajjal végzett művelet részleteit, ha az értelmezhető, például a raj által használt henger alakú légtér paramétereit, a műveletben résztvevő UAV EU kategória és osztálybesorolását.

6.4.6 OPERATOR_ID

A távpilóta CAA által kiosztott távpilóta azonosítóját szolgáltatja, jelenleg ez az egy formátum támogatott.

6.4.7 MESSAGE_PACK

Több, fent felsorolt üzenet kombinálására szolgáló mechanizmus. Bluetooth 5 és wifi alapú továbbítás esetén használható. 1-9 darab bináris formátumba kódolt és tömörített OpenDroneID üzenet egy összesített üzenetben történő továbbítására szolgál. Jelenleg fixen, 25 bájtonként kerülnek összefűzésre az üzenetek, mivel egyelőre ez az előírt üzenethossz OpenDroneID esetén, a fennmaradó üres biteket pedig 0-val kell feltölteni.

6.5 Következtetések

A MAVLink protokoll és az egyéb biztonsági technológiák nyújtotta lehetőségeket számba véve megállapítható, hogy az OpenDroneID PKI kiegészítéssel megvalósítva teljeskörű megoldást adhat az UAV-k és távpilóták mind európai uniós, mind egyesült államokbeli szabályozásoknak megfelelő elektronikus azonosítására. Az OpenDroneID nyomkövetés biztosítja az egyértelmű visszakövethetőséget, de ezen túlmenően a háttérben PKI megol-

dást és (akár felhő alapú) adatbázist alkalmazva adott a lehetőség, hogy a hatóságok akár technikailag kényszerítsék ki a légterek biztonságos használatát.

Megmutattam, hogy a drón fedélzetén külső eszköz elhelyezésével és annak biztonságának garantálásával a felhő alapú irányítás a felhozott példáknak megfelelően elősegítheti az UAS-k személyi biztonsági szempontból megfelelő működtetetését: beleértve a drónok és távpilóták elektronikus, dinamikus regisztrációját és összerendelését; a jogosultságok távoli visszavonását.

7 ELEKTRONIKUS BIZTONSÁGI KÉRDÉSEK

Elektronikus biztonság alatt esetünkben leginkább az átviteli biztonság (TRANSEC[76]) biztosítását értem, hiszen a földi és légi alrendszer közti rádiós irányító kapcsolat a repülésbiztonság szempontjából leginkább támadható rendszerelem. Emellett a földi vevőegység és a felhő infrastruktúra közti, illetve a felhőn belüli internetes adatátvitel során ugyanúgy védendő az információ biztonsága.

„[Az átviteli biztonság] mindazon védelmi rendszabályok összességének az eredménye, amelyek végrehajtásával biztosítjuk a híradó adatátviteli utakon, csatornákon az információk sértetlenségének, rendelkezésre állásának, bizalmasságának meglétét, valamint adott esetekben a hitelességét, illetve letagadhatatlanságát." [132].

7.1 Az Open Glider Network rendszere

7.1.1 Az OGN röviden

Az OGN nyílt, vitorlázó repülést támogató rendszer, mely egyre nagyobb népszerűségnek örvend világszerte. Jelenleg több mint 10 000 fedélzeti jeladó eszköz [133] van regisztrálva a hálózatba, vitorlázó repülőgépektől kezdve, kisméretű légcsavaros repülőgépeken át pilóta nélküli légijárművekig. A rendszer kifejlesztésének célja az volt, hogy azokról a repülőgépekről, melyek nem rendelkeznek transzponderrel, közel valós idejű 3D pozíció és alapvető telemetriai adatok legyenek elérhetők egy publikus web felületen. A vitorlázó repülő közösségtől eredő kezdeményezés, ma már széles körben elterjedt és az OGN hálózatból nyert adatok, akár bajba jutott légijárművek felkutatásakor is felhasználásra kerülhetnek.

A VOLARE projekt keretein belül kutatócsoportunkkal azon dolgoztunk, hogy a fenti rendszert felhasználva, meteorológiai információt juttassunk el magába az OGN rendszerbe, illetve ezzel párhuzamosan, az OGN hálózat felhasználásával egy új repüléstámogatási rendszer numerikus prognosztikai alrendszerét is támogassuk ezzel az információval [134] [135] [136].

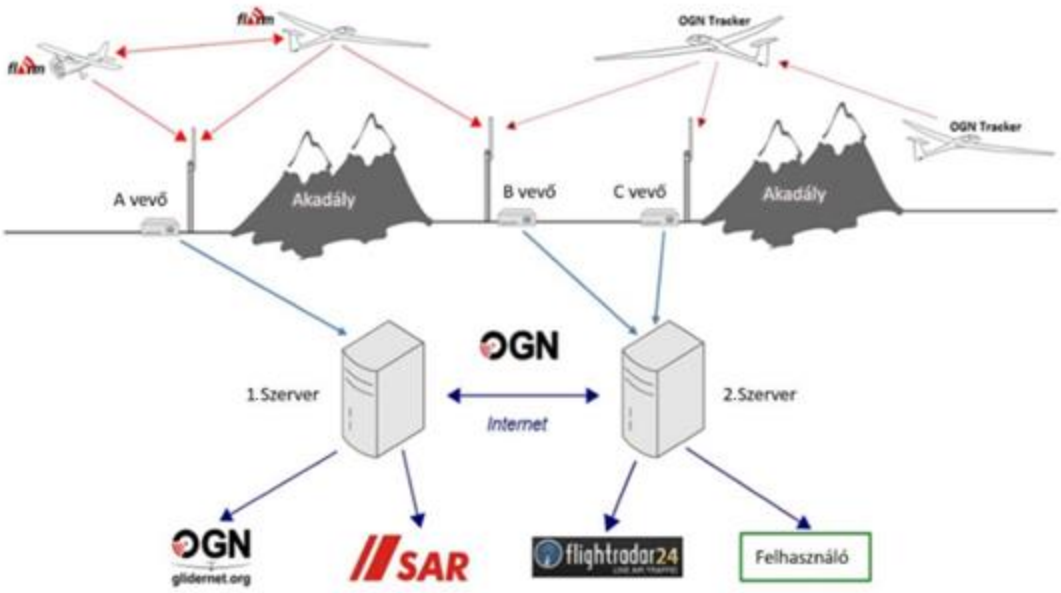
A hálózat [137] a „légi riasztó" (FLARM[77]) rendszerre épül. Utóbbinak alapvető célja a kisgépes repülés támogatása ütközés elkerülés lehetőségének megvalósításával. Az OGN ennek kiterjesztése, földi vevő állomások beiktatásával biztosítja interneten keresztül a

[76] Transport Security
[77] Flight Alarm

légijárművek „láthatóságát”, online térképes felületet biztosítva a biztonságosabb repülés tervezéséhez és végrehajtásához.

7.1.2 Az OGN hálózat felépítése

A repüléstámogató, köztük a Mission as a Service rendszereket légi, földi és adatkapcsolati alrendszerekre oszthatjuk [11]. Az OGN hálózat felépítését szemléltető 37. ábrán is felfedezhető ez a séma.



37. ábra: FLARM és OGN nyomkövető (tracker) az OGN-hálózatban.
(Fordította a szerző. Forrás: [138])

Az OGN és FLARM esetén a légi alrendszer alapeleme a tracker (nyomkövető egység), ami a pozíció és egyéb repülési adatok továbbítására képes. Ez általában egy kis méretű, kis energia igényű, 868 MHz-en üzemelő rádiós eszköz, ahogy a 38. ábrán is látható.

A kihelyezett földi vevőállomás a rádiós jeleket fogadja és dekódolja, majd ezeket automata csomagjelentő rendszer (APRS[78]) csomagok formájában, interneten át továbbítja a központi szerverekre.

[78] Automatic Packet Reporting System

38. ábra: Az „InfoPark” vevő (balra) és a „PETRA-D” tracker (jobbra),
(A képet készítette a szerző.)

A szerverekre különböző kliens alkalmazások iratkozhatnak fel és jeleníthetik meg tetszőleges formában az adatokat.

7.1.3 Az „OGN flavoured APRS” protokoll

Az APRS egy szöveges protokoll, eredetileg pozíció, időjárás adatok és egyéb szöveges közlemények rádió alapú digitális átvitelére lett tervezve.

Az OGN rendszeren belüli kommunikáció egységesítésére különböző üzenetformátumok kerültek rögzítésre [139].

Köztük szerepelnek a szerverre történő bejelentkezéshez, a vevő azonosítására használt üzenetek, vagy éppen a vevő státuszát, technikai információit (földrajzi pozíció, rendelkezésre álló processzor és memória, hőmérséklet stb.) közlő üzenetek. Ezeken felül természetesen a közeli nyomkövetőktől vett pozíció, vagy időjárási adatok is APRS formában továbbításra kerülnek.

7.1.4 A sebezhető pontok

7.1.4.1 Gyenge hitelesítés

A jelszó valójában a felhasználónév (vevő azonosító) hasításával jön létre [140]. A vevő azonosítók maximum 10 alfanumerikus karakter hosszúak, a jelszó generáló algoritmus kis és nagybetűre nem érzékeny. Első lépésként maximum 10 karakter hosszúvá és nagybetűssé alakítjuk a vevő azonosítót. Ezután vesszük a 73e2 hexadecimális kezdőszámot, és az azonosítóval 2 bájtonként (azaz 2 karakterenként) az elejétől kezdve „kizáró vagyoljuk”, melynek lépéseit a 2. képlet vezeti le. A végén maszkoljuk az előjelbitet, hogy biztosan pozitív legyen a szám, azaz a jelszó.

Az algoritmus levezetve az „InfoPark” vevőkódra:

a jelszó *kezdőszám XOR „IN” XOR „FO” XOR „PA” XOR „RK”* azaz

$$73e2_{16} \oplus 494e_{16} \oplus 464f_{16} \oplus 5041_{16} \oplus 524b_{16} = 32489_{10}$$

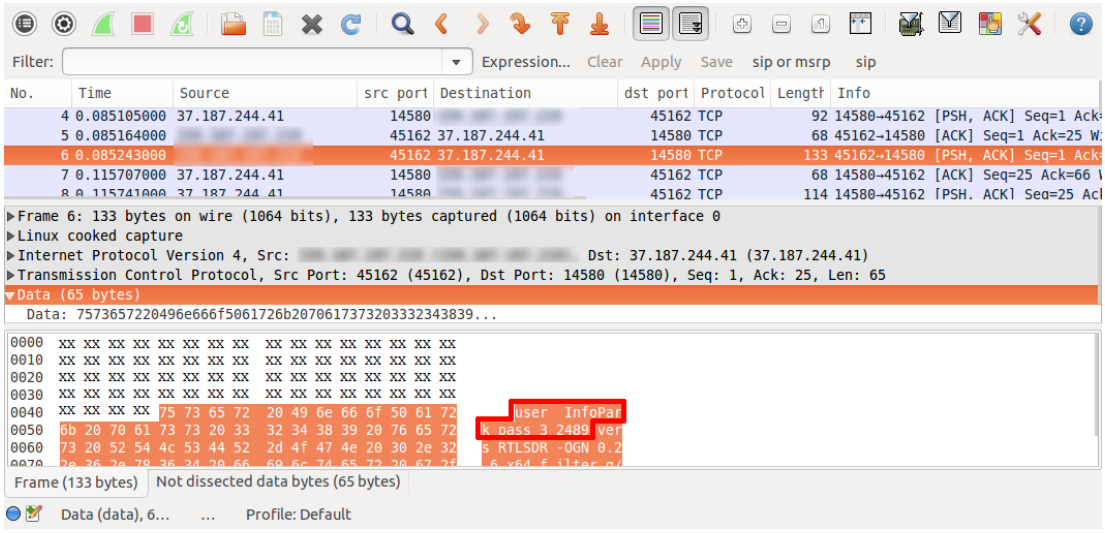
2. képlet: A jelszó kiszámítása az „InfoPark” vevőkódra.
(Szerkesztette a szerző.)

7.1.4.2 Titkosítatlan átvitel

Ha egy kiszolgálón vagyunk a vevőt megvalósító `ogn-rf` és `ogn-decode` szoftverrel, könnyedén kielemezhetjük a vevő és az APRS szerver közti adatforgalmat.

Ugyanígy lehallgathatjuk egy hálózati forgalom analizáló eszközzel, például Wiresharkkal, ha egy hálózaton vagyunk vele, és sikerül egy közbeékelődéses támadással például tartománynév rendszer (DNS[79]) gyorsítótár mérgezés vagy cím feloldási protokoll (ARP[80]) mérgezés [141] módszerével a két végpont közé férkőznünk. Ezután akár egyszerűen le is másolhatjuk, meghamisíthatjuk és meg is módosíthatjuk a csomagokat.

Vegyük észre, hogy a 39. ábrán kiemelt részben tényleg a fentebb általunk is kiszámolt jelszó található.



39. ábra: APRS csomag megjelenítése a Wireshark eszközzel.
(A képernyőképet készítette, szerkesztette a szerző.)

Tapasztalataim szerint a légiirányítás fenntartásokkal kezeli az OGN-t emiatt a sebezhetőség miatt.

7.1.4.3 Gyenge engedélyezés

Adatküldés során nem is kell online lennie a vevőnek, azaz nem kell státusz üzeneteket küldenie. Elég, ha a vevő egyszer bejelentkezik az APRS szerverre felhasználónév/jelszó

[79] Domain Name System
[80] Address Resolution Protocol

párossal, onnantól nincs is szükség sem a földrajzi hely megadására konfigurációs csomagokkal, sem státuszüzenetek küldésére, vagyis elég légi eszközök adatait továbbítania. Így előállhat az a furcsa helyzet, hogy a megjelenítő alkalmazásokon a vevőállomás vörösen, offline, vagy egyáltalán meg sem jelenik, viszont az általa továbbított adatok alapján megjelennek légijárművek.
A légijármű adatok sincsenek igazán validálva, az eszköz által sugárzott, a fizika törvényeit meghazudtoló hamis vagy hibás adatokat is megjeleníti a legtöbb kliens alkalmazás. Lásd bekeretezve a 40. ábrán.

7.1.4.4 Egy támadás vektora

- Kiválasztjuk az trackert a regisztrált eszközök listájából [133]. Legyen ez a példa kedvéért OGN132528 (a tracker bármelyik lehetne, ez az általam használt, kölcsön kapott valódi tracker).
- Kiválasztjuk a vevőt a vevők listájából, [142] vagy egy térképes megjelenítőből [143]. Legyen ez most InfoPark (a vevő bármelyik lehetne, ez az általam telepített valós, ideiglenes vevő a munkahelyemnél).
- Kitöltjük a bejelentkező csomagot.
    - Felhasználónév a vevő azonosító; a jelszó generálható online, [144] vagy a korábbi fejezetben mutatott módszerrel ki is számolható, sőt, akár lehallgatható, ezért nem is féltem jelen cikkben nyilvánossá tenni.

```
user InfoPark pass 32489 vers RTLSDR-OGN 0.2.6.x64 filter g/ALL
```

- A további csomagokban időbélyeg dinamikus előállítására, megfelelő formázására van szükség. Ez Linux operációs rendszereken, bash-ben például a következőképp történhet.

```
date +%H%M%S
```

- Kitöltünk egy konfigurációs sort, hogy megjelenjünk a térképen. GPS pozíciót, és egyéb paramétereket adunk meg a vevőről, a protokollnak megfelelően [139].

```
InfoPark>APRS,TCPIP*,qAC,GLIDERN2:/`date
+%H%M%S`h4728.26NI01903.78E&000/000/A=000390
```

- Kitöltünk egy státusz riport sort is, hogy online-nak tűnjünk.

```
InfoPark>APRS:>`date +%H%M%S`h v0.2.6.x64 CPU:0.2
RAM:13350.9/16730.0MB NTP:0.1ms/+11.9ppm +25.0C 1/1Acfts[1h] RF:-
2+0.3ppm/+9.16dB
```

– Kitöltünk pár eszköz által lesugárzott sort. Nem muszáj a valódi eszköznek bejelentkezve lennie. Nem is muszáj logikus adatoknak lennie (például szürreális 999 csomó sebességet is megadhatunk egy szimulált vitorlázó vagy pilóta nélküli repülőgépnek). Lásd majd a 40. ábrán.

```
OGN132528>APRS,qAR:/`date
+%H%M%S`h4728.26N/01903.80E'000/999/A=000390 !W54! id07132528
+000fpm +0.0rot 45.2dB 0e -2.6kHz gps5x7
```

– Csatlakozunk az egyik APRS szerverhez a listából, példaként a másodikhoz, a megfelelő publikus, ismert portjára.
  - glidern1.glidernet.org
  - glidern2.glidernet.org
  - glidern3.glidernet.org
  - glidern4.glidernet.org

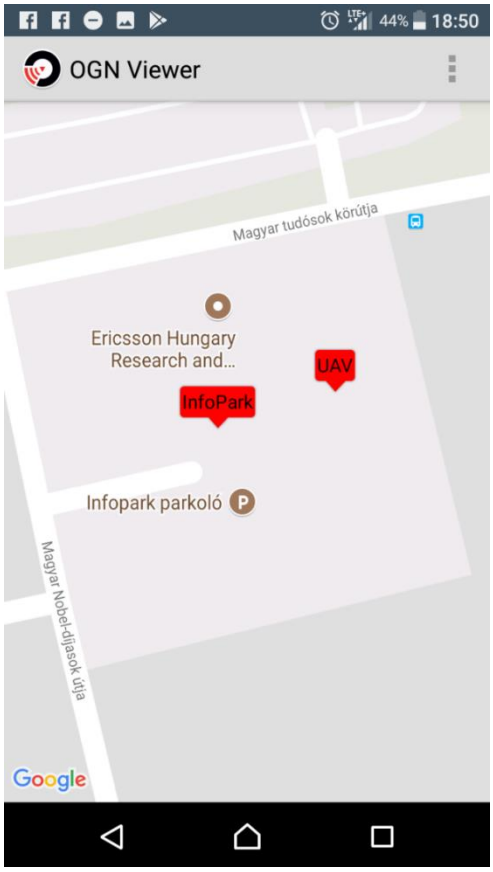
```
telnet 37.187.244.41 14580
```

– Beküldjük az összeállított csomagokat.
– Sikeresen eltérítettük vagy megzavartuk a céltárgy nyomkövető jelét a rendszerben.

Tapasztalataim szerint a glidertracker.org megjelenítő jobban megengedő. A live.glidernet.org csak akkor jeleníti meg a vevőt, ha hosszabb ideje aktív.

40. ábra: Sikeres megjelenítés a glidertracker.org honlapon.
(A képernyőképet készítette és szerkesztette a szerző.)

Az OGN Viewer App-on is látszik a sikeres támadás, lásd 41. ábra.



41. ábra: Sikeres megjelenítés az OGN Viewer alkalmazáson.
(A képernyőképet készítette a szerző.)

7.2 Az OpenDroneID rendszere

A következő összegző fejezet a specifikáció egy munkapéldánya alapján készült, [131] melynek részletei idővel változhatnak.

Az OpenDroneID esetén elektronikus biztonság szempontjából a következő technológiai lehetőségek és felhasználási esetek adottak. Ez a technológia az OGN funkcionalitásához hasonló, de azon túlmutató lehetőségeket ad az elektronikus biztonság kérdésének kezelésére.

7.2.1 Üzenetszórási módszerek

Négy különböző üzenetszórási módszer került specifikálásra:

- Bluetooth hagyományos szórt üzenet (Bluetooth 4.x).
- Nagy hatótávú Bluetooth kibővített szórással (Long Range with Extended Advertising) (Bluetooth 5.x).
- Wifi szomszédtudatos hálózat (NaN[81]).
- Wifi Beacon (gyártóspecifikus információs elem formájában a szolgáltatáskészlet-azonosító (SSID[82]) jeladó keretben).

Az első módszer erősen korlátozza a rádión küldhető adat mennyiségét, így az adatokat különféle kategóriákra osztották fel, és ennek megfelelően mindegyik kategória külön üzenettípusban kerül továbbításra.

A 6.4 fejezetben bemutatott felbontásnak megfelelően az ASTM távoli azonosítási szabvány 6 ilyen alap üzenettípust határoz meg, illetve egy hetedik speciális típust, ami több üzenet egybecsomagolását teszi lehetővé a fenti 2., 3. és 4. átviteli lehetőség esetén.

Az egyszerűbb OpenDroneID adók és vevők közötti adattovábbítás támogatására a MAVLink 2.0 protokollban is megvalósításra kerültek az üzenetek.

7.2.2 Példák az alkalmazásra

Több felhasználási lehetőség is adódik a specifikált azonosító üzenetekhez:

- Egy földi irányító azonosító, pozíció stb. adatokat küld egy fedélzeti Bluetooth- vagy wifi-képes adóvevő modulnak.
- A fedélzeti Bluetooth- vagy wifi-képes vevő fogadja a környékén működő egyéb légijárművek OpenDroneID adatait, majd ezeket átjátssza MAVLink

[81] Neighbor-aware Network
[82] Service Set IDentifier

kapcsolaton keresztül a földi irányítás részére, ami ezt az információt veszély-felismerési és ütközéselkerülési számításokhoz használhatja.

- Egy drón MAVLink kapcsolaton keresztül küld OpenDroneID üzeneteket az irányítására szolgáló csatornán keresztül a földi irányítóállomásnak, ami tárolja és közzéteszi a drón azonosítóját, pozícióját stb.
- Ennek fordítottja: a földi irányítóállomás továbbít ismert, a közelben aktív azonosítókat a drón felé fedélzeti ütközéselkerülési számításokhoz.
- Egy, a földi irányítóállomáson futó alkalmazás megjeleníti a rádión fogadott azonosítókat a távpilóta számára, például térképen.

7.2.3 Üzenetek

A MAVLink nyers, bájtszintű felépítése nem egyezik meg azzal, ami végül az OpenDroneID üzenetekben Bluetooth-on vagy wifin keresztül kerül rádiós továbbításra, kisebb mértékű tömörítés is történik az átalakítás folyamán. Az OpenDroneID csomagok valódi, nyers felépítésére annak hivatalos C könyvtárának kódjában található példa [145].

Ebben a könyvtárban találhatunk szoftveres támogatást a MAVLink üzenetek dekódolásához és az üzenetek tömörítéséhez, ami a Bluetooth- vagy wifi-alapú küldést lehetővé teszi; illetve a rádiós üzenetek fordított irányú feldolgozására is.

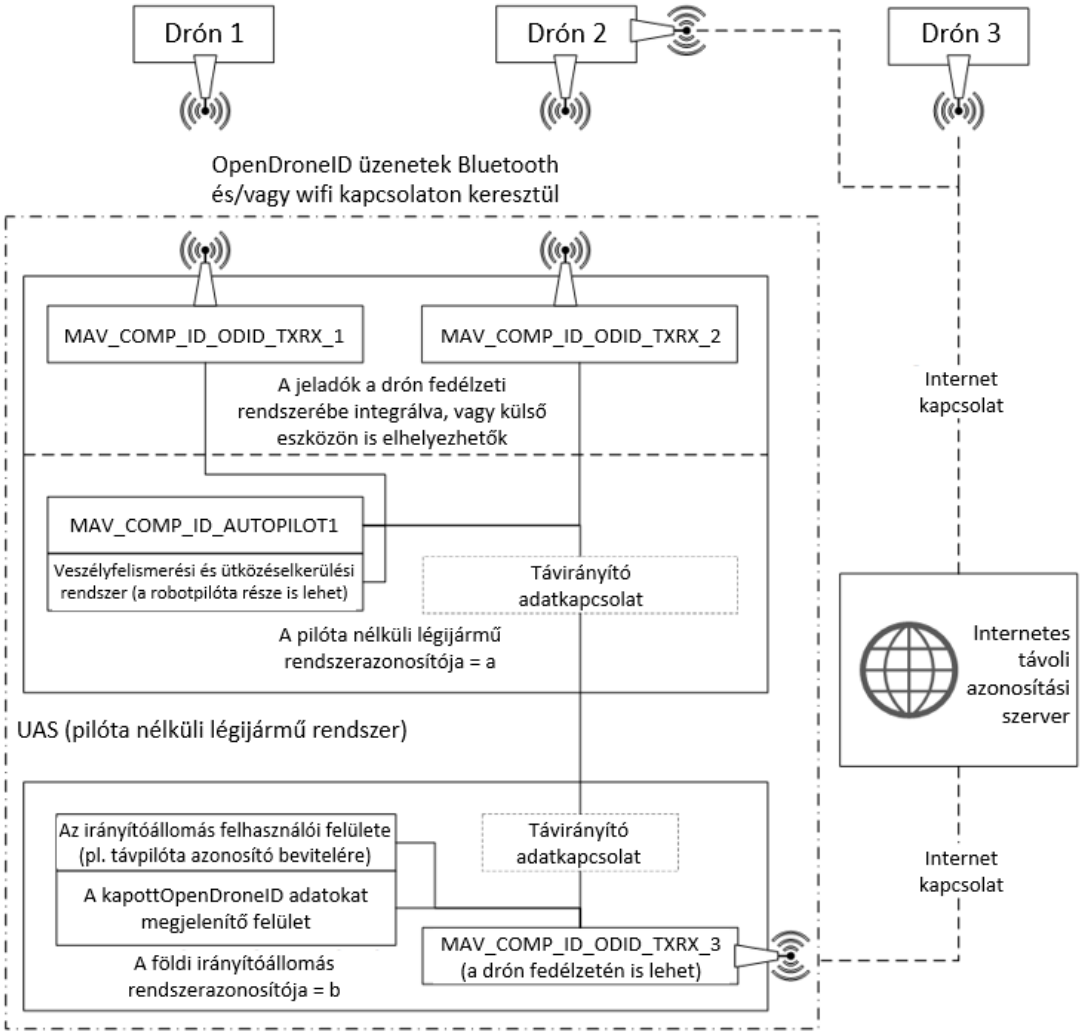
Az ASTM távoli azonosítási szabvány kiköti, hogy a pozícióüzeneteket legalább 1 Hz frekvenciával szükséges sugározni. A többi üzenettípust 3 másodperc időközönként (vagy az ennél esetleg szigorúbb helyi szabályozásnak megfelelően sűrűbben) szükséges szórni. Nem minden üzenettípus szórása kötelező.

A szabvány nem írja elő, hogy bármely drón kötelezően képes legyen fogadni, átjátszani, feldolgozni, értelmezni, lereagálni azonosító üzeneteket, kizárólag a rendszeres küldést köti ki. (Ám ettől a helyi szabályozások hozhatnak szigorúbb megkötéseket.)

Android operációs rendszerre példa megvalósítás már elérhető ugyancsak az OpenDroneID központi repozitóriumban [146].

7.2.4 Útválasztás

Egy pilóta nélküli légijármű rendszer több eleme is képes lehet OpenDroneID üzenetek kezelésére, erre egy példa a 42. ábrán látható. Ezen az ábrán is észre vehetjük az IoT rendszerekhez való hasonlóságot, bár nem minden implementáció tartalmazza ilyen formában az összes komponenst, az egyes funkciók más szinteken is megvalósításra kerülhetnek rendszertől függően.



42. ábra: Az OpenDroneID áttekintése.
(Az ábrát fordította a szerző. Forrás: [147])

A MAVLink protokolloknak megfelelően minden üzenet esetén kötelező a `sysid` kitöltése a küldő rendszer hálózati azonosítójával, illetve a `compid` mező a pontos küldő alrendszer, komponens azonosítójával.

A MAVLink protokoll által kiosztott nevesített komponens azonosítók a következő táblázatban olvashatók (csillaggal megjelölve az OpenDroneID esetén leginkább relevánsak).

Komponens azonosító	**Leírás**
0*	Szórt üzenet. Minden fogadó fél próbálja feldolgozni az ezzel az azonosítóval érkező üzeneteket, és továbbítja a többi, vele összeköttetésben lévő komponens számára is.
1*	A robotpilóta. Rendszerenként maximum 1 db robotpilóta a várt.
25-67	Belső komponens, bármilyen funkciót betölthet, de az üzenetei nem feltétlen továbbítódnak a külvilág felé.
68	Telemetria rádió komponens.
69-99	Belső komponens, bármilyen funkciót betölthet, de az üzenetei nem feltétlen további-

Komponens azonosító	Leírás
	tódnak a külvilág felé.
100-105	Kamera.
140-153	Szervo.
154	Gimbal.
155	Naplózó komponens.
156	ADSB
157	Képernyő kijelzésért felelős komponens.
158	Általános periféria.
160	FLARM.
161	Mentőernyő.
171-175	Gimbal.
180-181	Akkumulátor.
189	MAVLink vezérlőközeli hálózat (CAN) kliens.
190*	Földi irányítóállomás.
191-194	Kiegészítő fedélzeti számítógép.
195	Külső útvonaltervező.
196	Külső akadályelkerülő komponens.
197	Vizuális inerciális odometria (VIO[83])-elven működő pozíciófelismerő komponens.
198	A drónt és a földi állomást párosító eszköz.
200-202	Inerciális mérőegység (IMU[84]).
220-221	GPS.
236-238*	OpenDroneID adóvevő (Bluetooth, wifi, internet).
240	Felhasználói datagram protokoll (UDP[85]) híd.
241	Univerzális aszinkron adóvevő (UART[86]) híd.
242	TUNNEL-kezelő komponens (pl. gyártóspecifikus grafikus interfész).

3. táblázat: A MAVLink protokoll komponens azonosítói.
(Készítette a szerző a hivatalos MAVLink dokumentáció [148] alapján)

Tipikusan a robotpilóta komponens van a `BASIC_ID` és `LOCATION` üzenetek előállításához szükséges adatok birtokában. Köteles ezen üzeneteket rendszeresen, MAVLinken át továbbítani a többi rendszer felé. Ellenben nem köteles OpenDroneID MAVLink üzeneteket fogadnia a hálózaton.

[83] Visual Inertial Odometry
[84] Inertial Measurement Unit
[85] User Datagram Protocol
[86] Universal Asynchronous Receiver-Transmitter

A földi irányítóállomás a távpilóta azon felülete, amin keresztül az UAV-t irányítani tudja. A távpilóta rendelkezik a SELF_ID, SYSTEM és OPERATOR_ID üzenetek előállításához szükséges adatokkal, ezért azokat neki kell megadnia felszállás előtt. A földi irányítóállomás ezeket az üzeneteket MAVLinken át továbbítja. Amennyiben a földi irányítóállomás rendelkezik pozicionálási képességgel, a helyzetadatait is szórt üzenetként továbbítja. A drónhoz hasonlóan az állomásnak sem feltétlen kötelessége fogadni és feldolgozni OpenDroneID üzeneteket.

Az UAV egy vagy több adóval rendelkezik, amik az adatait megosztják a külvilággal, Bluetooth-on, wifin vagy interneten át egy távoli kiszolgálóval. Az OpenDroneID adó (de nem vevő) komponensek figyelik a beérkező MAVLink üzeneteket, ám eldobják azokat, amik a 236-238 indexű komponens azonosítóra érkeznek a robotpilótától és földi irányítóállomástól. A vevő oldali komponensek és a földi irányítóállomás kommunikációjára vonatkozó részletek alább, a 7.2.6 fejezetben olvashatók.

A target_system és/vagy target_component mező kitöltésével opcionálisan további szigorítások alkalmazhatók az üzenetek feldolgozására. A vevők csak olyan üzeneteket kell, feldolgozzanak, amik esetén ezek a mezők 0-ra (szórt üzenet) vannak beállítva, vagy kifejezetten a vevő rendszer/komponens azonosítójának vannak címezve.

Ez akkor hasznos, ha egy földi irányítóállomáshoz több UAV is kapcsolódik. Az állomás ez alapján célzott üzeneteket küldhet a kiválasztott 236-238 indexű OpenDroneID komponenseknek az adott fedélzeti rendszeren. A target_system és target_component mezők értéke alapértelmezésben 0, jelezve, hogy egy szórt üzenetről van szó.

7.2.5 Státuszüzenetek

A MAVLink üzenetváltásokban résztvevő komponensek mindegyikétől elvárt, hogy rendszeres időközönként, általában másodpercenként státuszüzeneteket, úgynevezett HEARTBEAT üzeneteket osszon meg, ezzel lehetőséget adva képességeinek és állapotának felmérésére a rendszeren belül.

MAVLink esetén a 236-238 azonosítójú OpenDroneID adóvevő komponensek esetén a fenti üzenet type mezőjében a 34-es indexű MAV_TYPE ODID értéket kell feltüntetni.

A HEARTBEAT üzenet segít beazonosítani a rendszerek között a földi irányítóállomást is, ahol a type mező a 6-os indexű MAV_TYPE_GCS enumerált értékkel kerül kitöltésre.

7.2.6 Más UAV-któl származó adatok

Amikor belső üzenetküldésre van szükség a rendszeren belül, a dokumentáció szerint a compid mezőt a saját 236-238 azonosítójú OpenDroneID komponensnek kell címezni,

hogy lehetőség legyen megkülönböztetni a rendszernek címzett többi üzenettől. A `sysid` mezőt pedig a fogadó oldal részére kell címezni. Megjegyzés: Megítélésem szerint a dokumentáció ezen része hibás, inkább az OpenDroneID üzenetek `target_system` és `target_component` mezőit kellene a fenti módon kitölteni, miközben a `sysid` és a `compid` a küldő fél azonosítóit kell, hogy tartalmazzák. Egyazon rendszeren belüli üzenetküldés esetén pedig a `sysid` azonos a `target_systemmel`.

Elképzelhető, hogy egy adó komponens rendelkezik vételi képességekkel is, hogy adatot gyűjthessen a környezetében tevékenykedő egyéb rendszerektől. A közelben működő drónok fedélzeten vett adatait veszélyfelismerési és ütközéselkerülési céllal megoszthatja a robotpilótával vagy egyéb útvonaltervező komponenssel. Így ezeknek a komponenseknek lehetősége adódik dinamikusan reagálni a közeli pilóta nélküli forgalomra és akár előre lefektetett szabályok szerint döntéseket hozni különböző forgalmi helyzetekben (például elsőbbségadás jobbkézszabállyal). A vett adatok a távpilótát is segíthetik döntési helyzetekben, ha a fedélzeten vett adatokat a légi alrendszer lesugározza a földi irányítóállomásnak, ahol az, megjelenítésre kerül, például a többi drón helyzetének és eddig bejárt vagy tervezett/számított útvonalának kijelzésével.

OpenDroneID esetén a küldött üzenetek nem minden esetben azonosítják egyértelműen a küldő rendszert. Például Bluetooth Legacy Advertising (Bluetooth 4.x) alapú átvitel esetén a kapott üzenetek nagy része nem tartalmaz egyedi azonosítót, a technológia korlátai miatt legfeljebb 25 bájtos darabokban közlekednek az üzenetek. Ezesetben egyedül a Bluetooth rádió média hozzáférés vezérlő (MAC[87]) címe azonosítja a küldő felet. Bluetooth 5.x és wifi esetén hasonló eset csak ritkán állhat elő, például a több részből álló `AUTHENTICATION` üzenetek esetén, hiszen minden más esetben kötelező több üzenet `MESSAGE_PACK` üzenetekbe történő csomagolása.

Az interneten kapott üzenetek tartalmaznak egyedi azonosítót magasabb szinten, de az eredeti MAC cím nem visszakövethető.

Hogy a veszélyfelismerésért és ütközéselkerülésért felelős komponensek szét tudják válogatni az üzeneteket és azonosítani tudják az egyes küldő rendszereket, a küldő oldal a MAVLink üzenetek `id_or_mac` mezőjének kitöltésével tudja egyértelműen azonosítani magát a hálózatban.

[87] Media Access Control

Ha ez a mező azonosítóval kerül kitöltésre, annak tartalma megegyezik az `uas_id` mező értékével (az üres, nem használt bitek 0-val kerülnek kitöltésre). MAC cím esetén amerikai szabványos kódolás információátadásra (ASCII[88]) formátumban kell kitölteni, elválasztó karakterek nélkül, ugyancsak 0 bitekkel kiegészítve. Ha a mező nincs használatban, szintén 0-kal kell kitölteni.

7.2.7 Több adóvevővel rendelkező rendszerek

Mivel több adatátviteli technológia is támogatott az OpenDroneID üzenetek szórására, lehetséges, hogy egy rendszer egy időben, több spektrumban is kommunikáljon.

Ez a képesség nem előírás, azonban lehetséges, hogy egyes UAV-k más technológiát alkalmaznak a megvalósításra, mint mások, ezért a legkritikusabb rendszerek esetén érdemes egy időben mindhárom technológia (Bluetooth, wifi, internet) jeleit felismerni és támogatni.

7.2.8 Duplikált üzenetek kezelése

A fogadó rendszer vagy komponens a különböző támogatott technológiák miatt képes kell, hogy legyen felismerni a duplikált üzeneteket, amennyiben azok esetlegesen más úton érkeztek ugyanabból a forrásból. A duplikált adatok szűrése és összefésülése során nyilván kell tartani az összetartozó azonosítókat és MAC címeket, hogy egyes csatornák kimaradása esetén is egyértelműen nyomon követhető maradjon a küldő rendszer állapota.

Az egyes átviteli módok mechanizmusaitól függően a `LOCATION` üzenet időbélyeg mezője alapján szükség lehet az üzenetek utólagos sorba rendezésére, szűrésére is.

7.3 A MAVLink 2.0 aláírás mezőjének támadhatósága

Az esetleges meteorológiai vagy ütközéselkerülő alrendszer biztonságának biztosításához mindenképp szükséges a MAVLink 2.0 aláírás-alapú integritásvédelmi funkciójának kihasználása a különböző rádiós csatornákon, illetve ezen túlmenően további lépések is szükségesek lehetnek a külső eszköz biztonságának biztosítására, hiszen, ha külső eszköz képes beavatkozni a repülésbe, ez egy új, közvetlen támadási felületet jelent.

Ahogy a 2.1.6.2 fejezetben említettem, a MAVLink 2.0 üzenetek SHA256 aláírás mezőjének 48 bitre csonkítása ront a hasító algoritmus ütközéstűrő tulajdonságán. Igaz, az eredeti kulcs tartós, biztos visszafejtéséhez még mindig 2^{256} lehetséges bemenetet kellene egy támadónak végig próbálnia, viszont ahhoz, hogy 50% valószínűséggel a 48 bites aláírással rendelkező adatfolyamba injektáljon egy hitelesnek tűnő üzenetet, matematikailag már

[88] American Standard Code for Information Interchange

csak kb. 20 millió próbálkozásra van szüksége – ez példaként másodpercenként 1000 próbálkozással számolva azt jelenti, hogy nagyjából 5 és fél óra próbálkozás után 50% valószínűséggel el lehet téríteni a kiválasztott drónt! Ennek az első pillantásra aránytalanul nagy különbségnek az oka a születésnap-paradoxon [149] matematikai problémára vezethető vissza. Az eredeti paradoxon szerint, ha egy teremben 23 ember tartózkodik, már 50% a valószínűsége, hogy találunk köztük kettőt, akinek egy napra esik a születésnapja. A paradoxont általánosítva a MAVLink 2.0 aláírás $k=2^{48}$ lehetséges értékének (az év napjai esetén ez 365 volt) 3. képletbe helyettesítésével felülről becsülhető az aláírás ütköztetéséhez szükséges próbálkozások száma ($Q(k)$) 50% kívánt várható sikeresség esetén.

$$Q(k) \leq 1{,}2\sqrt{k}$$

3. képlet: 50% valószínűségű ütközéshez szükséges próbálkozások számának felső becslése a születésnap-támadás esetén k lehetséges értékre.
(Szerkesztette a szerző. Forrás: [150])

Kiszámolva ezt az eredeti SHA256 algoritmusra vonatkoztatva azt láthatjuk, hogy az aláírás csonkításával arányaiban 2×10^{31}-szeres, mondhatni csillagászati nagyságrendekkel mérhető mértékben romlott az algoritmus ütközéstűrése. Az aláírás mező megrövidítése mögötti technikai érv érthető, hiszen a MAVLink üzenetek általában korlátozott átviteli sebességű rádiós adatcsatornán kerülnek kiküldésre. Ez, és a hasonló elven működő születésnap-támadások viszonylag könnyen észlelhetők az áldozat által, hiszen nagyon „zajosak", a sok próbálkozás kitűnik a megszokott hálózati forgalomból. Mindazonáltal ennek detektálására, elhárítására nem találtam törekvést a MAVLink protokoll kapcsán.

Ez a támadás nagyobb sávszélességű TCP/IP (rendszerünk esetén mobilinternetes) átvitel esetén kivitelezhető leginkább. A példában említett 1000 próbálkozás/másodperc intenzitású támadás az alap, (Európában) 868 MHz-es rádión annak – mind technikailag, mind jogszabályilag – korlátozott átviteli képessége miatt nem kivitelezhető. MAVLink protokoll esetén a maximális csomagméret 280 bájt, 1000 ilyen csomag 280 kB adatforgalmat jelent. A 868 MHz-es rádiócsatorna ilyen mértékű telítése inkább már az elektronikai zavarás témakörébe tartozik. Mobilinternetes átvitel esetén viszont érdemes SSL/TLS-t alkalmazni a MAVLink aláírás helyett, illetve mellett a bemutatott támadás kivédésére, hiszen a fenti példában említett legfeljebb 280 kB/s intenzitású adatforgalmat napjaink mobilinternetes hálózatai megfelelő térerő esetén már könnyedén kiszolgálják.

7.4 Laboratóriumi tesztesetek

Az elektronikus biztonság témaköréhez a korábban bemutatott laboratóriumi tesztesetek is kapcsolódhatnak, ám a most következő tesztesetek inkább a robotpilóta és a mobilalkalma-

zás, mint hálózati átjáró viselkedését, túlélőképességét teszik próbára célzottan, némely esetben elektronikus támadási módszereket szimulálva. A lenti tesztesetek leginkább a rendelkezésre állás, vagyis a robotpilóta és a mobilalkalmazás működés közben folyamatos elérhetőségének szempontját vizsgálják.

7.4.1 GPS adatfolyam lekérése

Ez az alapvető pozitív, funkcionális teszteset a GPS adatfolyam elérhetőségét vizsgálja. A teszteset kódja az első `HEARTBEAT` üzenet megérkezésekor összeállít egy `MAV_CMD_SET_MESSAGE_INTERVAL` MAVLink üzenetet, mellyel `MAV_DATA_STREAM_POSITION` adatfolyamot kér 1 Hz frekvenciával. Erre `GLOBAL_POSITION_INT` csomagot kap válaszként, minek hatására utasítja a robotpilótát az adatfolyam leállítására. A teszteset elbukik, ha megszakad a kapcsolat, illetve nem érkezik időben `HEARTBEAT` üzenet vagy pozícióadat. Ez az egyszerű teszteset sikeresen lefutott minden futtatás során.

7.4.2 Túlterhelés

Ez a teszteset az első `HEARTBEAT` megérkezése után 100 db GPS adatfolyam lekérést küld a robotpilóta felé gyors egymásutánban. A teszteset elbukik, megszakad a kapcsolat, illetve ha a további `HEARTBEAT` üzenetek 1 tizedmásodpercnél többet késnek – utalva a robotpilóta túlterhelődésére, vagy 2 percen belül nem érkezik egy pozícióadat sem (egyes esetekben ennyi időt is igénybe vehet a megfelelő GPS jel elérése, ezért a 2 perc ráhagyás). Esetemben többszöri újra futtatás alatt sem sikerült túlterhelni a rendszert ezzel a 100 üzenettel. Az 1. és 2. mellékletben látható, hogy MAVLink esetén 0-255 az üzenet sorszámának megengedett értéke, így érdemben párhuzamosan legfeljebb ennyi csomaggal lenne tesztelhető a rendszer, 256-tól kezdődően a sorszám „túlcsordulna," hogy a $\mathbb{Z}_{255}$ maradékosztályon belül maradjon, az ütköző sorszámú csomagokat a protokoll elveti.

7.4.3 Sérült adatcsomag

Ez a negatív teszteset az első `HEARTBEAT` megérkezése után a korábbiakhoz hasonlóan lekér egy pozíció adatfolyamot. Az első pozícióadat megérkezésekor összeállít egy az adatfolyam leállítását célzó üzenetet, aminek végül szándékosan elrontja az ellenőrzőösszeg mezőt (ha ez eredetileg 00_{16}, akkor 01_{16}-re állítja, minden más esetben 00_{16}-ra), majd kiküldi a csomagot. Ha ezen üzenet hatására megszakad a pozícióadatok leküldése, az azt jelenti, a robotpilóta a hibás ellenőrző összeg ellenére végrehajtotta a parancsot (a protokoll előírásainak ellentmondva), ami egyes esetekben hibás működést is eredményezhet,

ezért ekkor a teszteset bukik. Esetemben a robotpilóta helyesen eldobta a hibás üzenetet, és folytatta a leküldést. Ennek hatására a teszteset újra kérte az adatfolyam leállítását, ez alkalommal, helyes ellenőrzőösszeggel, hogy visszaállítsa a robotpilóta eredeti állapotát, így a teszteset lefutása sikeresnek értékelhető.

7.4.4 Nem támogatott üzenettípus

Ez a negatív teszteset egy a robotpilóta által nem ismert parancsot küld ki (`MAVLINK_MSG_ID_SERIAL_UDB_EXTRA_F22`, ami egy másik, MatrixPilot robotpilóta firmware-hez tartozó üzenettípus, illetve a mezői is hibás adatokkal lettek kitöltve). Amennyiben a robotpilóta továbbra is időben küldi a `HEARTBEAT` üzeneteket, a teszt sikeresnek mondható. MatrixPilot firmware esetén ez sérült adatcsomagnak minősülne az előző tesztesetben leírtaknak megfelelően; egyéb rendszerek esetén, mint az APM 2.6 is, a fel nem ismert üzenet eldobásra kell, kerüljön. APM esetén az elvárt viselkedés volt tapasztalható, így átment a teszteseten.

7.5 Következtetések

Az Open Glider Network megvalósítását megvizsgálva arra a következtetésre jutottam, hogy a hálózat – bár széles körben elterjedt és a vitorlázórepülő pilótáktól a helikopterpilótákig sok légiközlekedésben résztvevő szereplő előszeretettel használja –, jelen formájában sajnos nem elégíti ki a 21. század szigorú biztonsági követelményeit. A bemutatott esettanulmánynak megfelelően a légijárművek és a földi vevőállomások jelei/adatai is könnyedén meghamisíthatók az internetes átvitel során, aminek okai alapvető koncepcionális hiányosságokra vezethetők vissza.

Az OpenDroneID koncepciója láthatóan összefonódott a MAVLink protokollal. Jelenleg, mivel részleteiben még kidolgozás alatt van, ez sem ad még kész megoldást a csomagok hitelesítésére, de sok fennmaradt kérdésre választ adhat a PKI koncepcióval való integráció (hitelesítéshez használt kulcsok kiosztása, visszavonása, lejárata, konfigurációja stb.). Ettől eltekintve a Bluetooth és wifi, illetve internetes átvitel miatt nem jelentkeznek az OGN-t sújtó (pl. kis sávszélességben megmutatkozó) technikai korlátok és az ezekből eredő biztonsági limitációk, viszont önmagában a rendszerrel nem kivitelezhető az OGN által nyújtott több kilométeres hatótávolság.

A MAVLink 2.0 aláírás mezőjét megvizsgálva elmondható, hogy az aláírás mező önmagában nem teszi teljes mértékben ellenállóvá a protokollt eltérítési kísérletekkel szemben, azonban hagyományos, alacsony sávszélességű rádiós adatcsatornák esetén hozzájárul a csomagok sértetlenségének biztosításához, hiszen az erre irányuló támadások a valószínű-

ségeket figyelembe véve előbb kezdenék ki a rendelkezésre állás dimenzióját, mintsem sikerülne a drónt eltéríteni. Nagyobb sávszélességű modern rádiós hálózatokon viszont érdemesebb emellett vagy ezen túlmenően SSL/TLS technológiát alkalmazni az adatcsatorna biztosítására.

Megállapítható, hogy ha a korábbi fejezetekben vázolt technológiákkal (MAVLink 2.0, PKI, TPM stb.) összhangban az OpenDroneID koncepciója a jövőben felhasználásra kerül (habár jelenleg még nem véglegesített), és a felhő rendszer kialakítása során figyelembe vesszük a releváns szabványokat (mint az ISO/IEC 27017 [42] rejtjelzésre vonatkozó fejezete), a felhő alapú irányítás elősegítheti az UAS-k elektronikus biztonsági szempontból megfelelő működtetetését.

Végül az APM 2.6 robotpilóta irányába futtatott különböző pozitív és negatív funkcionális teszteseteket mutattam be, illetve vizsgáltam a rendszer túlterhelésének esetét is. Ezek kimenetele alapján úgy ítéltem meg, hogy a választott robotpilóta-rendszer robusztussága elektronikus biztonsági szempontból ténylegesen megfelel a kísérleti repülési tesztek lefolytatásához elvárható szintnek.

ÖSSZEGZETT KÖVETKEZTETÉSEK

1. Az elvégzett repülési tesztesetek rávilágítottak a rendszer egyes hiányosságaira (pl. az elavult firmware által nem támogatott automatikus fel- és leszállás, koordinátarendszerek közti átváltás szükségessége) és lehetőségeire (pl. a 4G adatkapcsolaton elérhető meglepően gyors válaszidő). Az ezekből leszűrt tanulságok alapján a későbbi fejezetek során javaslatokat teszek a hasonló rendszerek kialakításának részleteire.
2. A szimulátoros laboratóriumi tesztesetek során demonstráltam a felhő rendszer skálázódási és túlélőképességét, túlterhelt helyzetben és hálózati katasztrófa esetén, mely rámutatott, hogy akár védelmi vagy kormányzati alkalmazás során a felhő alapú UAS szolgáltatások nagyfokú megbízhatóságot adnak, miközben gazdaságosan szervezik az erőforráskészletet.
3. A felhő és fizikai rendszereket érintő teljesítmény- és költségbeli összehasonlítás eredményeként elmondható, hogy kisebb meteorológiai kutató projektek esetén megéri felhő szolgáltatást bérelni, hosszabb távú, nagyobb párhuzamosítást igénylő projektek esetén pedig pénzügyileg inkább megéri dedikált fizikai számítógép(ek)et fenntartani. Mindazonáltal a mérési eredmények alapján elmondható, hogy kizárólag a számítási teljesítményt figyelembevéve a felhő rendszerek felveszik a versenyt a hasonló konfigurációjú dedikált, fizikai társaikkal, illetve sok esetben még meg is előzik azokat, akár komolyabb párhuzamosságot igénylő feladatok végrehajtása során is.
4. A rendszer tervezése során a nyílt forrású és szabad szoftverek alkalmazására törekedtem, a sikeres implementáció rámutatott, hogy a szabályzói feltételek és technikai lehetőségek szabják meg leginkább a hasonló rendszerek tesztelésének korlátait – a szükséges infrastruktúra kialakítása kivitelezhető költséghatékonyan, javarészt ingyenes szoftverrendszer alkalmazásával.
5. Az UAS-specifikus publikus kulcsú infrastruktúra lehetőségeit megvizsgálva arra a következtetésre jutottam, hogy egy európai szintű eljárásrend lehetőséget adhat a távpilóták és drónok ad-hoc elektronikus összerendelésére, a felszállások távoli engedélyezésére, illetve a hatósági beavatkozásra. Erre célzott technikai megoldást adhat az OpenDroneID rendszere, kiegészítve egy PKI-alapú bizalmi láncolattal, ami jelenleg még nincs kidolgozva a specifikációban. A

koncepció piaci drónok esetén általánosítható külső, központilag bevizsgált és jóváhagyott fedélzeti eszköz alkalmazásával.

ÚJ TUDOMÁNYOS EREDMÉNYEK

1. **Definiáltam** a *Mission as a Service*, vagyis szolgáltatásként nyújtott küldetés fogalmát, mely felhő támogatással tervezett és (akár felszínen, felszín alatt, levegőben vagy a világűrben) végrehajtott pilóta vagy járművezető nélküli küldetéseket takar. A definícióm alapján **megállapítottam**, hogy a létező felhőszolgáltatási csoportok közül egyik sem fedi le a definiált feladatkört.
2. Saját felhő alapú pilóta nélküli légijármű-rendszert fejlesztettem ki, melyen változatos, ám célzott tesztesetek végrehajtásával, kimenetelük értékelésével **bizonyítottam**, hogy a földi alrendszer felhő infrastruktúrába szervezése hozzájárul a fizikai és az elektronikus biztonság kialakításához UAS-k esetén. Összehasonlítva, egy hagyományos fizikai kiszolgáló esetén az elvégzett tesztesetek lefolytatása várhatóan a szolgáltatás folyamatosságának jelentős sérülését, megszakadását okozta volna, míg a felhő szolgáltatás túlélőképességét a leírt kimenetek demonstrálják.
3. Átfogó **modellt alkottam** a pilóta nélküli légijárművek PKI és OpenDroneID alapú, európai uniós irányelveknek megfelelő azonosítására és regisztrációjára, mely folyamatainak példáin keresztül **levezettem**, hogy a modell alkalmazása hozzájárulna a pilóta nélküli légijármű-rendszereket érintő személyi és adminisztratív folyamatok biztonságos kialakításához.
4. **Megállapítottam**, hogy egy UTM repülésmeteorológiai támogató alrendszer megvalósítása esetén, habár költséghatékonyságban a felhő infrastruktúra elmarad a fizikai kiszolgálókhoz képest nagy párhuzamosságot igénylő számítások esetén; a felhő alapú számítás teljesítményben eléri, esetenként túl is teljesíti a dedikált fizikai kiszolgálókat még nagy párhuzamosság esetén is.

AJÁNLÁSOK

Megítélésem szerint a kutatás eredményei nemcsak a jelenlegi oktatás és képzés elméletében és gyakorlatában, hanem hasonló rendszerek védelmi, közszolgálati és polgári megvalósításának gyakorlatában is alkalmazhatók:

- Az értekezés releváns lehet Egyetemünk oktatási tevékenysége során, kifejezetten a Repülésirányító és Repülő-hajózó Tanszék, Repülőfedélzeti Rendszerek Tanszék, az Informatikai Tanszék, a Híradó Tanszék, illetve az Elektronikai Hadviselés Tanszék alap- és mesterképzésein.
- A felvázolt rendszer általánosítható felhő helyett szoftverkonténer technológián alapuló rendszerek megtervezéséhez is, ennek vizsgálata akár érdekes diplomamunka téma lehet.
- Az OGN hálózaton bemutatott esettanulmány azt gondolom, (negatív) iskolapélda kritikus rendszerek biztonsági tervezése szempontjából. A vizsgálat tanulságait, a felismert sebezhetőségeket ajánlom nem csak technikai, de döntéshozói szinten is szem előtt tartani.
- A rendszer bemutatott tulajdonságai, képességei iránymutatást adhatnak különféle egyéb közszolgálati, felhő alapú rendszerek megtervezéséhez.
- A javasolt PKI és OpenDroneID alapú modellben rejlő lehetőségek ölteteket adhatnak a Nemzeti Közlekedési Hatóság Légügyi Hivatala munkatársainak és a Törvényhozóknak a drónokhoz kapcsolódó adminisztráció ügymenetének javarészt elektronikus alapokra fektetéséhez, az európai uniós előírásoknak történő megfelelés mellett.
- A WRF-specifikus teljesítmény költség meghatározás általánosítása érdekes lehet kutatótársaim számára, saját és pályázati kutató projektek beszerzéseinek tervezéséhez.

KUTATÁSI EREDMÉNYEK GYAKORLATI FELHASZNÁLHATÓSÁGA

Mission as a Service szolgáltatások biztonságos megvalósításához a következő kiemelt gyakorlati szempontokat, javaslatokat és jövőbeli lehetőségeket fogalmazom meg.

Kompatibilitás

A fejlesztés és tesztek során tapasztaltam, hogy az alkalmazott APM 2.6 robotpilóta és a MapBox térképes keretrendszer egymáshoz képest fordított sorrendben kezeli a hosszúság-szélesség koordinátapárokat, emiatt például egy a térképen megjelenő magyarországi koordinátapárt a robotpilóta szaúd-arábiai úticélként értelmez. Egy ilyen hiba esetlegesen az irányítás teljes elvesztéséhez is vezethet, melynek következményei repülésbiztonság szempontjából végzetesek lehetnek. A koordinátarendszert érintően egyéb problémák is felmerülhetnek a különböző számábrázolási módok különbségeiből adódóan, például a fokok, fokpercek és fokmásodpercek megadása szemben a tizedes fokok megadásával, illetve az előjeles megadás szemben az észak-dél-kelet-nyugat notációval. A koordinátarendszereken túl az időformátumok és a választott epoch eltérései, illetve a szinkronizálatlan időforrások is jelenthetnek problémát.

Érdemes a hardver, firmware és protokoll specifikációkat már az integráció előtt részletesen áttanulmányozni: az elavult hardware kombinálása új firmware-el ugyanolyan problémás lehet, mint az új hardveren futtatott elavult firmware esete. Esetemben a drón egyszerűen csak nem szállt fel automatikusan, de gondoljunk bele, ha vészhelyzetben a hazatérés parancsot vagy a leszállás parancsot utasította volna vissza.

A MAV Downlink applikáció megfelelően működik Ardupilot APM 2.6-tal, viszont egy Pixhawk PX4-gyel folytatott próba során az alkalmazás nem ismerte fel a robotpilótát kliens eszközként, egy másik nyílt forrású alkalmazás, a QGroundControl viszont sikeresen felismerte a PX4-et. A kód további feltárása alapján, a hiba kijavításához elég lenne a MAV Downlink kódjában frissíteni az USB soros kapcsolatért felelős `usbserial` könyvtárat.

Védelmi és kormányzati alkalmazás

A bemutatott tesztesetek közül kiemelném a skálázásra, illetve a szolgáltatás túlélőképességére és helyreállására vonatkozókat, melyek leginkább védelmi vagy kormányzati alkalmazás során fontosak, hiszen főként ezeken a területeken jellemzőek a hálózati elemek és telephelyek megsemmisítésére irányuló fizikai és kibertámadások. Egy másik érv a felhő

alapú rendszerek alkalmazása mellett védelmi szférában a meglévő, akár különböző gyártóktól származó, heterogén gépparkok újrahasznosításának lehetősége.

Adatkapcsolat

A 4G mobilkommunikáció meglepően jól működött a tesztek során, mindössze 150 ezredmásodperc késleltetéssel a drón és a chicagói szerver között. Ez az érték elhanyagolható az (ASTM által előírt) 1 Hz gyakoriságú adatküldéshez és térkép frissítéshez viszonyítva. Természetesen ez az 1 másodperces intervallum megfelelő konfigurációval szűkíthető, de úgy tapasztaltam, ez gyakorlatban elég a pozíció-, szenzor- és státuszadatok esetén a helyzet megítélésére autonóm repülés esetén is.

Természetesen kézi irányításhoz ennél kisebb válaszidő az elvárható, illetve, ha videókép is leküldésre kerül, a sávszélesség is jelentős korlátot szab az élőkép minőségére, tömörítéstől függően. Ezek a korlátok feloldhatók 5G adatátvitel alkalmazásával: a rendszer megtervezése során törekedtem arra, hogy a moduláris felépítésből adódóan könnyedén tovább fejleszthető legyen, így mindössze az okostelefon lecserélésével 5G képessé tehető a fedélzeti rendszer.

Megítélésem szerint a hasonló autonóm kíséreli repülések esetén elengedhetetlen a vészhelyzeti kézi távirányítás lehetősége, illetve a geofencing beállítása.

Elkülönített szerepek

A repülési tesztek során a távpilótán kívül egy megfigyelő kolléga jelenléte nagyban hozzájárul a megfelelő helyzetismeret kialakításához és fenntartásához. Kézi repültetés esetén egyedül nem biztonságos az adatokat élőben elemezni a képernyőn, illetve szükség esetén a légtérrel kapcsolatban telefonon veszik fel a távpilótával a kapcsolatot – ezek mind könnyen elterelhetik a figyelmét a repülésről.

Nyílt forrás

A rendszer megvalósításához alkalmazott összes technológia nyílt forrású vagy szabad technológia. 2014-ben, amikor elkezdtem ennek a rendszernek az előkészítését, a piacon elérhető drónok még nem voltak olyan kifinomultak, mint ma, és sokan kételkedtek benne, hogy egy felhő alapú pilóta nélküli légijármű rendszert érdemes, vagy egyáltalán lehetséges lenne megvalósítani. Manapság már világszerte léteznek zárt rendszerek, melyek hasonló elven működnek, ám remélem, hamarosan nyílt rendszerek is megjelennek a piacon, melyek bárki által szabadon ellenőrizhetők és kipróbálhatók, vagy akár tovább fejleszthetők.

A nyílt/szabad forrás hozzájárul az ellátási lánc biztonságos tervezéséhez, szoftver-, hardver- és adatforrások szempontjából is. Jövőbeni rendszerek esetén, ahol a például veszélyes meteorológiai jelenségek autonóm elkerülésére is lehetőség nyílik, szintén fontos a meteorológiai adatok védelme az átvitel, tárolás és felhasználás során, hiszen, ha egy támadó hamis időjárási adatokat juttathat az előrejelzésbe, azzal akár az UAV-kat is eltérítheti.

OGN-re vonatkozó ajánlások [S4]

Hitelesítés

Az APRS jelszó a már ismertetett okok miatt nem megbízható, ezért egy regisztrációs felület megvalósítását javaslom.

Az átviteli biztonság fenti megvalósítása igaz, nyújt hitelesítési lehetőségeket, de gondoljunk bele, ez átviteli, nem alkalmazói szinten történik a hálózatban, vagyis csak azt biztosítja alap esetben, hogy a szerver oldal az, akinek mondja magát. Ezért az APRS bejelentkezést is erősíteni érdemes, vagy bevezetni a kliens oldali tanúsítványok alkalmazását a SSL/TLS hitelesítés során.

Az APRS jelszót generáló algoritmus kifejlesztése során a fejlesztők elkövettek egy rég óta felismert hibát. A Kerckhoff-elv [151] alapján a titkosítási algoritmusok során egyedül a kulcsok kellene, hogy titkosak legyenek. Auguste Kerckhoff, a 19. századi matematikus szerint nem szabad egyedül arra alapozni egy eljárást, hogy a lehetséges támadók nem ismerik az algoritmust. Sőt, az algoritmus legyen publikus, hogy minél többen használhassák, illetve megismerhessék, ez is hozzájárul ahhoz, hogy biztonságosan lehessen alkalmazni, hiszen, ha valami sérülékenység van az algoritmusban, annál hamarabb kiderül. A fejlesztők pont fordított logika mentén az algoritmust tartották titokban, és igazi jelszót nem is kérnek a felhasználótól. Felteszik, hogy mert „ismeri” az algoritmust, biztosan a megbízható, hivatalos szoftvert használja, aminek titokban tartják a forráskódját.

Ha már javaslom a vevő regisztráció megvalósítását választott jelszóval, érdemes említést tenni a jelszavak tárolásának módjáról. Ne tároljunk a kiszolgálón nyers jelszavakat, hiszen, ha ezeket megszerzi valaki, máris be tud jelentkezni a felhasználók nevében. Ebből az okból kifolyólag szokás a jelszavakat szerver oldalon hasítva, vagyis hash, lenyomat formájában tárolni.

A hasító eljárások jellemzője, hogy olyan függvények (egy bemenő adatból determinisztikusan ugyanaz az egy kimenet képződik minden esetben), amelyek nagy valószínűséggel nem generálják több különböző bemenetből ugyanazt a lenyomatot (csekély az ütközés esélye), illetve nem invertálhatók (a kimenetet nem lehet, illetve nehéz közvetlen vissza-

alakítani az eredeti bemenetté). Még egy gyakori jellemzőjük, hogy a bemenő adatok kis mértékű módosítása a lenyomat nagy mértékű módosulásával jár, így nem lehet következtetni „ránézésre hasonló”, ismert bemenetű lenyomatok alapján az eredeti bemenetre.
Megjegyzés: a lenyomat általában jóval rövidebb, mint a bemenet volt [151].

Engedélyezés

Heurisztikával segített mesterséges intelligenciával vizsgálható lehet, hogy valós adatokat küld-e a légijármű vagy az adó egység. Akár neuronhálóval, tanuló, evolúciós algoritmussal felkészíthetjük a szervereket, hogy kiszűrjék a valótlan adatokat. Megfelelő mennyiségű valós adat betáplálásával megtanítható a szűrő algoritmus, hogy melyek a valósnak tűnő adatok, így nem lehetne például a korábban bemutatott módszerrel szuperszonikus vitorlázó repülőgépet szimulálni a rendszerben.
Kísérletezéseim során kezdetleges szűrési próbálkozást véltem felfedezni, amikor a Budapesten bejelentkezett vevőhöz Szolnok környékén mozgó járművet próbáltam szimulálni. Bár az is lehetséges, hogy csak egy újabb programhibát fedeztem fel, hiszen egy idő után furcsa módon a szimulált légijármű hirtelen megjelent Szlovákia fölött, pontosan északi irányban a vevőállomástól, Szolnok helyett. Ennek az is lehet egy feltételezhető oka, hogy a gyakran használt előjel nélküli, 16 biten ábrázolt egész számok maximális értéke 65535. A vevő és a légijármű közti távolságot az OGN megjelenítők általában méterben számolják, Budapest és Szolnok távolsága nagyjából 90 kilométer, vagyis a 16 biten ábrázolt egész szám vélhetően túlcsordult, és ez ábrázolási hibákat okozott. Ez gyakorlatban nem szokott előfordulni, hiszen a szokásos 868 MHz antennák hatótávolsága általában csak pár kilométer.

Átviteli biztonság

A megvalósításhoz javaslom a MAVLink üzenetek és az OGN vevő-kiszolgálók közti kommunikáció esetén is az SSL/TLS rejtjelzési eljárás alkalmazását TCP fölött.
Az SSL/TLS eljárás az üzenetek digitális aláírásának és titkosításának informatikai megvalósítását, biztonságos kulcscserét, illetve további képességeket biztosít a megfelelő biztonsági szint kialakításához.

OpenDroneID bevezetése

Ahogy bemutattam, a MAVLinken keresztüli OpenDroneID szórás kielégíti az EU és USA leglényegesebb technikai ajánlásait az elektronikus azonosítás területén. A nyíltforrású technológia pedig élénkítheti mind a gyártói, mind a felhasználói közösség tevékenységét a szoftveres és hardveres megoldások optimalizálása és frissen tartása terén.

Nyílt technológián alapuló nyomkövető rendszer

Az OpenDroneID nyílt forrása lehetővé teszi annak különböző számítógépes platformokra történő egyszerű portolását, például Android/iOS okostelefonra, Raspberry Pi mikroszámítógépre vagy hagyományos asztali vagy hordozható számítógépekre is. A nyomkövető képességen túl kiegészíthető meteorológiai, környezetvédelmi (szálló por, levegőminőség, ózon szenzor stb.) vagy egyéb adatgyűjtő és -továbbító rendszerrel is az alkalmazott kommunikációs megoldás, ezzel hozzájárulva a meteorológiai előrejelzések pontosságának javításához.

Nyilvános kulcsú infrastruktúra kialakítása

A PKI megoldást nyújthat akár nemzetközi szinten a drónok, üzembentartók és távpilóták elektronikus tanúsítására, nyilvántartására. A PKI tanúsítványai az OpenDroneID jelenleg befejezetlen hitelesítési eljárását is teljessé tehetik, biztosítva az EU jogszabályok által megkövetelt elektronikus azonosításhoz szükséges sorozatszámok kiosztását is.

Pilóta-UAV ad-hoc egymáshoz rendelése

A bemutatott módon akár QR-kód vagy NFC címke beolvasásával azonosítható és azonnal egymáshoz rendelhető az aktuális távpilóta és UAV felszállás előtt, illetve feloldható a drónra szerelt külső azonosító eszköz, ezzel biztosítva, hogy csak az illetékes személyek férjenek hozzá.

Biztonság tervezése

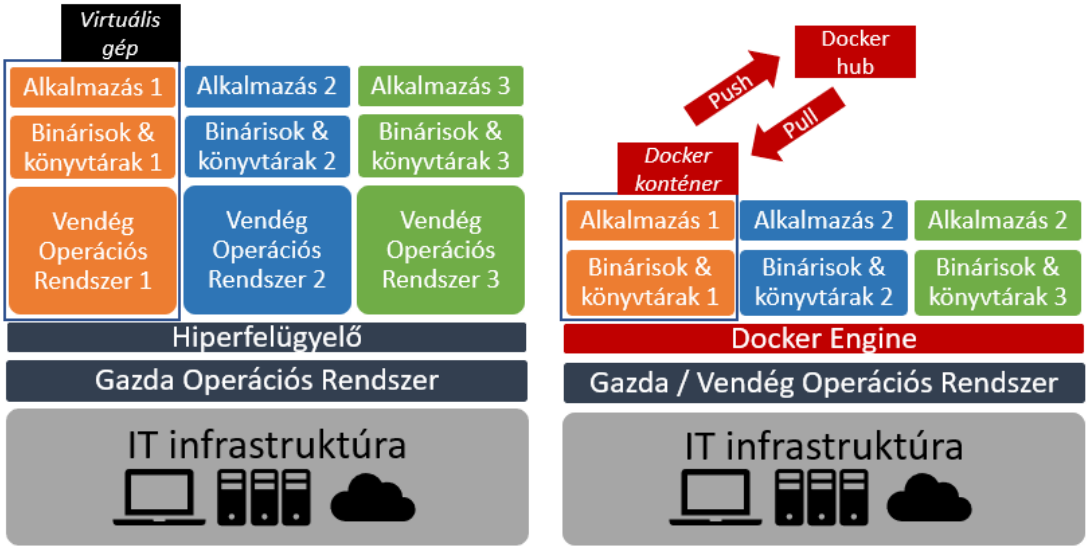
A hasonló rendszerek megtervezése esetén érdemes mielőbb szemügyre venni a biztonsági szempontokat, illetve kockázatelemzést készíteni a műveletek és a kezelt adatok kritikusságának figyelembevételével [31].

Adatok osztályozása

Valós megvalósítások során mindenképp fontos a küldés, feldolgozás alatt lévő és tárolt adatok osztályozása aszerint, hogy azok személyes adatnak minősülnek-e. Fontos még a repülési adatok csoportjainak hozzáférhetőségi és kockázati szintjeinek meghatározása is.

Várható jövő

A szakértők sokáig versenytársakként tekintettek a felhő és szoftverkonténer technológiákra, hiszen képességek terén nagyjából ugyanazt nyújtják. A felhő és a Docker szoftverkonténer technológia közti alapelvbeli eltéréseket a 43. ábra szemléleti.



43. ábra: Felhő kontra Docker.
(Az ábrát Lovas Róberttel közös munkájuk alapján fordította a szerző.)

Napjainkra a tendencia azt mutatja, ezeknek egy kombinált, hibrid megoldása lehet a jövő, ahol felhő infrastruktúrában menedzselt szoftverkonténerek futtatják a szolgáltatásokat, illetve akár a felhő egyes alacsonyszintű komponenseit is szoftverkonténerekben izolálják el a többitől. A kifejlesztett kísérleti rendszer rugalmasságának köszönhetően átalakítható ilyen hibrid infrastruktúrában történő futtatásra is.

További lehetőségek

A MapBox támogatást nyújt különböző kiterjesztett valóság (AR[89]) és virtuális valóság (VR[90]) megoldások integrálására, akár amolyan virtuális terepasztal megvalósítására is, ahogy a 44. ábrán látható. Ez a lehetőség a légiforgalmi irányítók munkáját is megkönnyítheti.

[89] Augmented Reality
[90] Virtual Reality

44. ábra: Képernyőkép egy MapBox Unity alapú kiterjesztett valóság alkalmazásból. Az app a felhasználó szobájában virtuálisan a dohányzóasztal fölé vetíti a domborzatot, ami az okostelefon segítségével tetszőlegesen körbejárható.
(Forrás: [152])

A térképen tetszőleges számú réteg megjeleníthető, így akár ultra rövidtávú meteorológiai előrejelzésekkel is segíthetjük a küldetések tervezését ugyanazon a felületen.

Később dinamikus (járművek körüli vagy időjárásfüggő) és statikus NDZ-k kiszámítására is alkalmas lehet a rendszer, hiszen a bejelentkezett járművek adatai szinte valós időben jelen vannak a rendszerben. Ütközésveszélyes helyzet észlelése esetén a rendszer automatikusan be is avatkozhat a küldetésbe, hiszen a bejelentkezett légijármű közvetlenül fogad parancsokat a felhőből. Jelvesztés esetén az UAV-k folytatják a küldetést a tervezett útvonalon haladva, így legtöbb esetben csak offline eszközök között lehetséges ütközéses baleset.

A MAVLink 254 rendszer azonosító limitációja még mindig fennáll. Ez részben mérsékelhető lenne azzal, ha az első bejelentkezéskor egy szabad rendszer azonosítót választanánk az UAV-nak, vagyis a jelenlegi statikus kiosztás helyett mindig újat kaphatna a légijármű, amikor bejelentkezik, így párhuzamosan 254 légijármű lehetne bejelentkezve.

Jelenleg az adatbázist strukturált lekérdezőnyelv (SQL[91]) alapon MySQL szolgálja ki egy virtuális gépen. Ezt bevett gyakorlat szerint később érdemes lehet átmozgatni az OpenStack adatbázis szolgáltatásába („Trove”). Megfontolandó, hogy a későbbiekben SQL helyett a pozíció és szenzor adatok naplózását noSQL adatbázisba mozgassuk, idősoros

[91] Structured Query Language

adatok tárolására ugyanis ezek sok esetben jobb megoldást adnak az SQL alapú adatbázisoknál.

A szerver virtuális gépeinek konfigurációját első körben egyszerű `cloudinit` szkript injektálással oldottam meg, későbbiekben képfájlba telepítve vagy szoftverkonténer technológiával lehet ezt tovább fejleszteni.

A két elkészített szimulátort némileg tovább fejlesztve akár egymással szembe is állíthatjuk, így zárt rendszerben verifikálhatnánk a két oldal működését. Arra számítok, ez az elképzelés egyelőre egy UAV-t szimulálva részben működne, jelenleg az irányító oldal egy csatlakoztatott UAV tesztelésére van felkészítve. Az UAV oldalon a GPS küldés és a periodikus „életjel küldés” működne, viszont a harmadik tesztesetben a hibás ellenőrző összeg ellenére feldolgozná a csomagokat, illetve a nem támogatott csomagokat nem tudná dekódolni, így hibára futna. A túlterheléses teszteset során várhatóan a szimulált UAV néhány figyelmeztető üzenetet naplózna, de teljesítené a parancsot.

Budapest, 2022. július

Vránics Dávid Ferenc

TÉMAKÖRBEN KÉSZÜLT PUBLIKÁCIÓIM

Lektorált folyóiratban megjelent cikkek

S1 Vránics Dávid, Üveges András: Pilóta nélküli légi járművek fejlődése, Felderítő Szemle XIV: (2) pp. 124-140.

S2 Vránics Dávid Ferenc: Felhő alapú rendszerekkel irányított pilóta nélküli légijármű rendszerek szakirodalmának kutatása, Hadmérnök XII.: (1. különszám) pp. 217-233.

S3 Vránics Dávid Ferenc: Egy felhőalapú, pilóta nélküli légijármű-tesztrendszer bemutatása, Bolyai Szemle XXVI.: (2) pp. 37-44.

S4 Vránics Dávid Ferenc, Palik Mátyás, Bottyán Zsolt: Esettanulmány egy nyílt repüléstámogató rendszer biztonságáról, Repüléstudományi Közlemények (1997-től) 30: (1) pp. 185-194.

S5 Vránics Dávid Ferenc, Palik Mátyás: Mission as a Service: Egy felhőalapú UAS megvalósítása, Repüléstudományi Közlemények (1997-től) 31: (3) pp. 153–167.

Idegen nyelvű kiadványban megjelent cikkek

S6 Vránics Dávid Ferenc, Palik Mátyás, Bottyán Zsolt: Electronic administration of unmanned aviation with public key infrastructure (PKI), International Scientific Journal Security & Future III: (4) pp. 152-155.

S7 Vránics Dávid Ferenc, Lovas Róbert, Kardos Péter, Bottyán Zsolt, Palik Mátyás: WRF Benchmark Measurements and Cost Comparison. Virtualized Environment Versus Physical Hardware, REPÜLÉSTUDOMÁNYI KÖZLEMÉNYEK (1997-TŐL) 29: (2) pp. 257-272.

S8 Vránics Dávid Ferenc: Testing of a cloud-based unmanned aircraft system, REPÜLÉSTUDOMÁNYI KÖZLEMÉNYEK (1997-TŐL) 32: (1) pp. 175–190.

Konferencia kiadványban meg nem jelent előadás

S9 VRÁNICS Dávid Ferenc, BALOGH Miklós, GYÖNGYÖSI András Zénó, ISTENES Zoltán, WEIDINGER Tamás, MAKKAY Imre, BOTTYÁN Zsolt, PALIK Mátyás: Meteorological sensor placement considerations for a fixed-wing Unmanned Aircraft System, In: ISARRA Conference 2019, Lugo (Spanyolország), 2019.07.16., prezentáció online elérhető: http://www.isarra.org/wp-content/uploads/2019/08/ISARRA_2019_Tue_Vranics.pdf

IRODALOMJEGYZÉK

[1] Unmanned airspace: EU-China APP Drone Workshop highlights UTM progress in China, url: https://www.unmannedairspace.info/uncategorized/eu-china-app-drone-workshop-highlights-utm-progress-china/ (elérhető online 2022.06.27.)

[2] Gutma.org: China - Map of UTM Implementation, url: http://gutma.org/maps/index.php?title=China (elérhető online 2022.06.27.)

[3] Koubaa A.: [Demo3] Dronemap Planner Mission Control of MAVLink Drone Through the Internet, url: https://www.youtube.com/watch?v=ackjmXTtvrk (elérhető online 2022.06.27.)

[4] Békési B., Makkay I., Palik M., Bottyán Zs., Dunai P., Halászné T A., Restás Á., Wührl T.: Pilóta nélküli repülés profiknak és amatőröknek. Budapest, Nemzeti Közszolgálati Egyetem, 2013., url: www.repulestudomany.hu/kiadvanyok/UAV_handbook_Secon_edition.pdf (elérhető online 2019.01.07.)

[5] Ványa L.: Hogyan védekezzünk a drónok ellen? Repüléstudományi Közlemények, XXV 2 (2013), 255-261., url: www.repulestudomany.hu/kulonszamok/2013_cikkek/2013-2-17-Vanya_Laszlo.pdf (elérhető online 2022.06.27.)

[6] Ványa L.: Kérdések és válaszok a szupertitkos RQ-170 iráni kézre kerüléséről. Repüléstudományi Közlemények, XXIV 2 (2012), 634-641., url: www.repulestudomany.hu/kulonszamok/2012_cikkek/52_Vanya_Laszlo.pdf (elérhető online 2022.06.27.)

[7] Ványa L., Kovács L.: Pilóta nélküli repülőgépek a terrorizmus elleni harcban. Repüléstudományi Közlemények, XIX (2007), 1-16., url: www.repulestudomany.hu/kulonszamok/2007_cikkek/kovacs_laszlo_vanya_laszlo.pdf (elérhető online 2022.06.27.)

[8] Papp I.: Pilóta nélküli légijármű típusok jellemzése. Repüléstudományi Közlemények, XXIV 2 (2012), 53-68., url: www.repulestudomany.hu/kulonszamok/2013_cikkek/2013-2-04-Papp_Istvan.pdf (elérhető online 2022.06.27.)

[9] Palik M.: Need for Unmanned Aircraft System. HADMÉRNÖK, II 2 (2007), 145-148., url: www.hadmernok.hu/archivum/2007/2/2007_2_palik.pdf (elérhető online 2022.06.27.)

[10] Dunai P.: Energiafelhasználás, a keringési és légzőrendszer terhelési paramétereinek elemző vizsgálata UAV kezelőszemélyzet munkavégzése során. Repüléstudományi Közlemények, XXV 3 (2013), 13-17., url: www.repulestudomany.hu/folyoirat/2013_3/2013-3-02-Dunai_Pal.pdf (elérhető online 2022.06.27.)

[11] Palik M.: Pilóta nélküli légijármű rendszerek légi felderítésre történő alkalmazásának lehetőségei a légierő haderőnem repülőcsapatai katonai műveleteiben. Budapest, Zrínyi Miklós Nemzetvédelmi Egyetem, Hadtudományi Doktori Iskola, 2007. (PhD értekezés), url: uni-nke.hu/downloads/konyvtar/digitgy/phd/2007/palik_matyas.pdf (elérhető online 2022.06.27.)

[12] Fekete Cs., Palik M.: Introduction of the Hungarian Unmanned Aerial Vehicle operator's training course. Defense resources management in the 21st century, 1 1 (2012), 55-68., url: conference.dresmara.ro/conferences/2012/CoDRM%202012.pdf (elérhető online 2022.06.27.)

[13] Fekete Cs., Palik M.: A hazai UAV kezelő személyzet képzésének tapasztalatai. Repüléstudományi Közlemények, XXIV 2 (2012), 61-69., url: ludita.uni-nke.hu/repozitorium/bitstream/handle/11410/1148/04_Fekete_Csaba-Palik_Matyas.pdf (elérhető online 2022.06.27.)
[14] Palik M., Pongrácz G.: Communication issues of UAV1 integration into non segregated airspace. Defense resources management in the 21st century, 1 1 (2012), 69-74., url: conference.dresmara.ro/conferences/2012/CoDRM%202012.pdf (elérhető online 2022.06.27.)
[15] Vas T., Palik M.: UAV operation in aerodrome safety and ACS procedures. Defense resources management in the 21st century, 1 1 (2012), 75-89., url: conference.dresmara.ro/conferences/2012/CoDRM%202012.pdf (elérhető online 2022.06.27.)
[16] Palik M.: Pilóta nélküli repülés - légi közlekedés biztonság. Repüléstudományi Közlemények, XX különszám (2008), 9., url: www.repulestudomany.hu/kulonszamok/2008_cikkek/Palik_Matyas.pdf (elérhető online 2022.06.27.)
[17] Bali T.: Ajánlások az UAV-k biztonságos légi és földi üzemeltetéséhez szükséges (repülési) szabályokra. Repüléstudományi Közlemények, XXV 3 (2013), 7-12., url: ludita.uni-nke.hu/repozitorium/bitstream/handle/11410/1716/2013-3-01-Bali_Tamas.pdf (elérhető online 2022.06.27.)
[18] Turóczi A.: Négyrotoros pilóta nélküli helikopter fedélzeti automatikus repülésszabályozó berendezései. Budapest, Zrínyi Miklós Nemzetvédelmi Egyetem, Hadtudományi Doktori Iskola, 2008. (PhD értekezés), url: ludita.uni-nke.hu/repozitorium/bitstream/handle/11410/10039/Teljes%20sz%c3%b6veg%21 (elérhető online 2022.06.27.)
[19] Hadobács K., Vidnyánszky Z., Bottyán Zs., Wantuch F., Tuba Z.: A pilóta nélküli légijárművek meteorológiai támogató rendszerének kialakítása és alkalmazhatóságának bemutatása esettanulmányokon keresztül. Repüléstudományi Közlemények, XXV 2 (2013), 405-421., url: www.repulestudomany.hu/kulonszamok/2013_cikkek/2013-2-31-Hadobacs_Katalin_es_a_tobbiek.pdf (elérhető online 2022.06.27.)
[20] Bottyán Zs., Wantuch F., Tuba Z., Hadobács K., Jámbor K.: Repülésmeteorológiai klíma adatbázis kialakítása az UAV-k komplex meteorológiai támogató rendszeréhez. Repüléstudományi Közlemények, XXIV 3 (2012), 11-28., url: www.repulestudomany.hu/folyoirat/2012_3/2012-3-02-Bottyan_Zs_es_a_tobbiek.pdf (elérhető online 2022.06.27.)
[21] Légügyi Hivatal: Összefoglaló az UAV-t érintő jogszabályokról. www.nkh.gov.hu/dokumentumtar/pdf-elonezet/-/p/232180 (elérhető online 2017. 04. 30.)
[22] Nemzeti Adatvédelmi és Információszabadság Hatóság: A Nemzeti Adatvédelmi és Információszabadság Hatóság ajánlása a drónokkal megvalósított adatkezelésekről. www.naih.hu/files/ajanlas_dronok_vegleges_www1.pdf (elérhető online 2017. 04. 30.)
[23] Magyarország Kormánya: A Kormány …/2016. (… ...) Korm. Rendelete az egyes légiközlekedéssel összefüggő kormányrendeletek módosításáról. www.kormany.hu/download/8/db/e0000/RPAS__honlapra.pdf (elérhető online 2017. 05. 25.)
[24] Európai Bizottság: A Bizottság (EU) 2019/947 Végrehajtási Rendelete a pilóta nélküli légi járművekkel végzett műveletekre vonatkozó szabályokról és eljárásokról (2019. május 24.) https://eur-lex.europa.eu/legal-

content/HU/TXT/HTML/?uri=CELEX:32019R0947&from=EN (elérhető online 2022.06.27.)
[25] Európai Bizottság: A Bizottság (EU) 2019/945 Felhatalmazáson Alapuló Rendelete a pilóta nélküli légijármű-rendszerekről és a pilóta nélküli légijármű-rendszerek harmadik országbeli üzembentartóiról, (2019. március 12.), https://eur-lex.europa.eu/legal-content/HU/TXT/HTML/?uri=CELEX:32019R0945&from=EN (elérhető online 2022.06.27.)
[26] Európai Bizottság: A Bizottság (EU) 2021/664 Végrehajtási Rendelete a U-space szabályozási keretéről, (2021. április 22.) https://eur-lex.europa.eu/legal-content/HU/TXT/HTML/?uri=CELEX:32021R0664&from=EN (elérhető online 2022.06.27.)
[27] Hann, R.: Are drones going to be banned from Svalbard?, url: https://www.ntnu.no/blogger/richard-hann/2021/10/19/are-drones-going-to-be-banned-from-svalbard/ (elérhető online 2022.06.27.)
[28] DoD: Unmanned Systems Integrated Roadmap. Washington, D.C.: Department of Defense, 2013., url: www.defense.gov/Portals/1/Documents/pubs/DOD-USRM-2013.pdf (elérhető online 2022.06.27.)
[29] Marty, J. A.: Vulnerability analysis of the MAVLINK protocol for command and control of unmanned aircraft. Wright-Patterson Air Force Base: Air University, Department of the Air Force, 2014. (PhD értekezés), url: www.dtic.mil/cgi-bin/GetTRDoc?AD=ADA598977 (elérhető online 2022.06.27.)
[30] The Executive Director of the Joint Air Power Competence Centre (JAPCC): Strategic Concept of Employment for Unmanned Aircraft Systems in NATO. Kalkar, Joint Air Power Competence Centre, 2010., url: www.japcc.org/portfolio/strategic-concept-of-employment-for-unmanned-aircraft-systems-in-nato/ (elérhető online 2022.06.27.)
[31] Allouch, A., Koubâa A., Khalgui M., Abbes T.: Qualitative and Quantitative Risk Analysis and Safety Assessment of Unmanned Aerial Vehicles Missions Over the Internet. in IEEE Access, vol. 7, pp. 53392-53410, 2019, doi: 10.1109/ACCESS.2019.2911980.
[32] Nemzetközi Szabványügyi Szervezet: Gépek biztonsága. Vezérlőrendszerek biztonsággal összefüggő részei. 1. rész: A tervezés általános alapelvei (ISO 13849-1:2015) Genf, Svájc, ISO, 2015.
[33] Nemzetközi Szabványügyi Szervezet: Gépek biztonsága. A kialakítás általános elvei. Kockázatfelmérés és kockázatcsökkentés (ISO 12100:2010), Genf, Svájc, ISO, 2010.
[34] Tóth A.: A hálózat nyújtotta képesség megvalósításának lehetőségei a Magyar Honvédség kommunikációs rendszerében. Budapest, Nemzeti Közszolgálati Egyetem, Hadtudományi Doktori Iskola, 2015. (PhD értekezés), url: m.ludita.uninke.hu/repozitorium/bitstream/handle/11410/10106/T%c3%b3th%20Andr%c3%a1s%20%c3%a9rtekez%c3%a9s (elérhető online 2022.06.27.)
[35] Racskó P.: A felhő alapú számítástechnika biztonsági kérdései a közigazgatásban. Budapest, Nemzeti Közszolgálati Egyetem, 2014., url: m.ludita.uninke.hu/repozitorium/bitstream/handle/11410/10376/08_kozigazgatasi_felho.pdf (elérhető online 2022.06.27.)
[36] Brainhub: Cloud: IaaS vs PaaS vs SaaS vs DaaS vs FaaS vs DBaaS. url: https://brainhub.eu/library/cloud-architecture-saas-faas-xaas (elérhető online 2022.06.27.)
[37] Dibbern, L: Drones As a Service: Strategy, Technical Concepts and Legal Aspects. 1. kiadás, ISBN-13: 978-1533618726, Createspace Independent Pub, 2016

[38] Werner D.: Software-as-a-Service model takes the space sector by storm. url: https://spacenews.com/space-as-a-service-model/ (elérhető online 2022.06.27.)
[39] Messier D.: Kleos Announces New Mission-as-a-Service Offering. url: http://www.parabolicarc.com/2022/05/02/kleos-announces-new-mission-as-a-service-offering/ (elérhető online 2022.06.27.)
[40] Defense Information Systems Agency: Cloud computing Security Requirements Guide (SRG). Washington, D.C., Department of Defense, 2015., url: iase.disa.mil/cloud_security/Documents/u-cloud_computing_srg_v1r1_final.pdf (elérhető online 2022.06.27.)
[41] Chief Information Officer: Cloud Security Information Impact Level Matrix. Washington, D.C., Department of the Navy, 2015. www.doncio.navy.mil/Download.aspx?AttachID=6393 (elérhető online 2017. 04. 30.)
[42] Nemzetközi Szabványügyi Szervezet, Nemzetközi Elektrotechnikai Bizottság: Informatika. Biztonságtechnika. Gyakorlati útmutató a felhőszolgáltatások ISO/IEC 27002-n alapuló információbiztonsági kontrolljaihoz/intézkedéseihez (ISO/IEC 27017:2015), Genf, Svájc, ISO/IEC, 2015.
[43] Nemzetközi Szabványügyi Szervezet, Nemzetközi Elektrotechnikai Bizottság: Informatika. Biztonságtechnika. Gyakorlati útmutató az információbiztonsági kontrollokhoz/intézkedésekhez (ISO/IEC 27002:2013, tartalmazza a 2014. évi 1. és a 2015. évi 2. helyesbítést), Genf, Svájc, ISO/IEC, 2017.
[44] European Telecommunications Standards Institute: Network Functions Virtualisation (NFV); NFV Security; Security and Trust Guidance. Sophia Antipolis, ETSI, 2014., url: www.etsi.org/deliver/etsi_gs/NFV-SEC/001_099/003/01.01.01_60/gs_NFV-SEC003v010101p.pdf (elérhető online 2022.06.27.)
[45] National Institute of Standards and Technology: Guidelines on Security and Privacy in Public Cloud Computing. NIST Special Publication 800-144, Gaithersburg, NIST, 2011., url: dx.doi.org/10.6028/NIST.SP.800-144 (elérhető online 2022.06.27.)
[46] Kuris Z., Pándi E.: Komplex információbiztonság megvalósítási lehetőségeinek megközelítése. Hadmérnök IV. Évfolyam 2. szám, 2009. június url: http://real.mtak.hu/40798/1/2009_2_kuris.pdf (elérhető online 2022.06.27.)
[47] Tóth L.: Tájékoztató a pilóta nélküli légijármű-rendszerek (UAS) frekvenciahasználatáról és engedélyezési kérdéseiről. Nemzeti Média- és Hírközlési Hatóság, Spektrumgazdálkodási Osztály, 2018. január 29. url: https://nmhh.hu/dokumentum/193162/UAV_tajekoztato.pdf (elérhető online 2022.06.27.)
[48] Desert Wolf: SkunkRiotControlCopter, url: http://www.desert-wolf.com/dw/products/unmanned-aerial-systems/skunk-riot-control-copter.html (elérhető online 2015.04.27.)
[49] The Times Of India: Now, drones to be used to disperse mobs in Luck now. url: http://timesofindia.indiatimes.com/city/lucknow/Now-drones-to-be-used-to-disperse-mobs-in-Lucknow/articleshow/46794530.cms (elérhető online: 2015.04.27.)
[50] Federal Aviaiton Administration: Package Delivery by Drone (Part 135), url: https://www.faa.gov/uas/advanced_operations/package_delivery_drone/ (elérhető online 2022.06.27.)
[51] Cao, K., Liu, Y., Meng, G., Sun, Q.: An Overview on Edge Computing Research. IEEE Access. PP. 1-1. 10.1109/ACCESS.2020.2991734, 2020
[52] Vránics D. F.: „A felhő alapú rendszerekből vezérelt pilóta nélküli repülőgépek biztonsági kockázatai," Diplomamunka, Nemzeti Közszolgálati Egyetem, Hadtudományi és Honvédtisztképző Kar, Katonai Üzemeltető Intézet, 2015.

[53] NVIDIA Developer: Jetson Nano Developer Kit, url: https://developer.nvidia.com/embedded/jetson-nano-developer-kit (elérhető online 2022.06.27.)
[54] Rober M.: Using Drones to Plant 20,000,000 Trees. url: https://www.youtube.com/watch?v=U7nJBFjKqAY (elérhető online 2022.06.27.)
[55] Corrigan F.: 7 Top Anti-Poaching Drones For Critical Wildlife Protection, url: https://www.dronezon.com/drones-for-good/wildlife-conservation-protection-using-anti-poaching-drones-technology/ (elérhető online 2022.06.27.)
[56] Chilson P. B., et al: Ten years of atmospheric research with UAS at the University of Oklahoma: Takeaways and lessons learned (A History of Hubris, Humility, and Hope), In: ISARRA Conference 2019, Lugo (Spanyolország), 2019.07.16., url: http://www.isarra.org/wp-content/uploads/2019/08/ISARRA_2019_Tue_Chilson.pdf (elérhető online 2022.06.27.)
[57] Reuder J. et al: The ISOBAR project on stable boundary layers - Current Status on Data Analysis and Results, In: ISARRA Conference 2019, Lugo (Spanyolország), 2019.07.16., url: http://www.isarra.org/wp-content/uploads/2019/08/ISARRA_2019_Tue_Reuder.pdf (elérhető online 2022.06.27.)
[58] Cione J., Bryan G.: Recent and Future NOAA operations using small Unmanned Aircraft Systems in Tropical Cyclones, In: ISARRA Conference 2019, Lugo (Spanyolország), 2019.07.16., url: http://www.isarra.org/wp-content/uploads/2019/08/ISARRA_2019_Tue_Cione.pdf (elérhető online 2022.06.27.)
[59] Békési B., Palik M., Vas T., Tóth A. H.: Aviation Safety Aspects of the Use of Unmanned Aerial Vehicles (UAV). In: Nádai, L., Padányi, J. (eds) Critical Infrastructure Protection Research. Topics in Intelligent Engineering and Informatics, vol 12. Springer, Cham. (2016). url: https://doi.org/10.1007/978-3-319-28091-2_10 (elérhető online 2022.06.27.)
[60] Palik M.: LÉGIKÖZLEKEDÉS-BIZTONSÁGI KUTATÁSOK, url: http://ginop.szrf.hu/doc-pdf/GINOP_Legikozl_Bizt_Kutatasok.pdf (elérhető online 2022.06.27.)
[61] Rattay W.: Dronedelivery: DHL 'parcelcopter' flies to Germanisle, url: http://www.reuters.com/article/2014/09/24/us-deutsche-post-drones-idUSKCN0HJ1ED20140924 (elérhető online 2015.04.27.)
[62] DHL: How medical drones help save lives in Tanzania, url: https://www.dhl.com/global-en/home/about-us/delivered-magazine/articles/2019/issue-3-2019/medical-drones-save-lives-tanzania.html (elérhető online 2022.06.27.)
[63] Zuckerberg, M.: Facebook post. url: https://www.facebook.com/zuck/posts/10101322049893211 (elérhető online 2022.06.27.)
[64] Maguire Y.: High altitude connectivity: The next chapter, url: https://engineering.fb.com/2018/06/27/connectivity/high-altitude-connectivity-the-next-chapter/ (elérhető online 2022.06.27.)
[65] Lockheed Martin Corporation: K-MAX® Unmanned Aircraft System, url: https://www.lockheedmartin.com/content/dam/lockheed-martin/rms/documents/k-max/K-MAX-brochure.pdf (elérhető online 2022.06.27.)
[66] Northrop Grumman: X-47B UCAS. url: https://www.northropgrumman.com/what-we-do/air/x-47b-ucas/ (elérhető online 2022.06.27.)

[67] Eckstein, M.: US Navy, Boeing conduct first-ever aerial refueling with unmanned tanker. url: https://www.defensenews.com/naval/2021/06/07/us-navy-boeing-conduct-first-ever-aerial-refueling-with-unmanned-tanker/ (elérhető online 2022.06.27.)
[68] Aerorozvidka: Aerorozvidka NGO, url: https://aerorozvidka.xyz/ (elérhető online 2022.06.27.)
[69] Kovacsik Á: Drónokkal üldözheti a bűnt a magyar rendőrség, url: https://mno.hu/belfold/dronokkal-uldozheti-a-bunt-a-magyar-rendorseg-1363601 (elérhető online 2018.04.15.)
[70] Berek T.: ABV (CBRN) védelmi alapismeretek, Zrínyi Miklós Nemzetvédelmi Egyetem, egyetemi jegyzet, 2010.
[71] DJI: Fly safe geo zone map. url: https://www.dji.com/hu/flysafe/geo-map (elérhető online 2022.06.27.)
[72] Минобороны России: Facebook post. url: https://www.facebook.com/mod.mil.rus/posts/2031218563787556 (elérhető online 2022.06.27.)
[73] Минобороны России: Facebook post. url: https://www.facebook.com/mod.mil.rus/photos/pcb.2031218563787556/2031214087121337/ (elérhető online 2022.06.27.)
[74] Fóthi Á., Horváth Z.: Bevezetés a programozásba, III. rész, egyetemi jegyzet, ISBN: 963 463 757 4, ELTE Informatikai Kar, 2005
[75] Google: Innovations – Data Centers – Google. url: https://www.google.com/about/datacenters/innovations/ (elérhető online 2022.04.19)
[76] Szabó G.: Hálózati szolgáltatások OpenStack környezetben. Networkshop XXIII, 2014. április 23-25. https://docplayer.hu/1587381-Halozati-szolgaltatasok-openstack-kornyezetben.html (elérhető online 2019. 03. 31.)
[77] European Union Agency for Network and Information Security, Cloud Security Incident Reporting - Framework for reporting about major cloud security incidents, US: European Union Agency for Network and Information Security, 2013.
[78] Cloutage.org: Honlap, url: http://cloutage.org/ (elérhető online 2022.06.27.)
[79] Coty S.: „Computer Forensics and Incident Response in the Cloud," in RSA Conference, Egyesült Államok, 2014.
[80] Internet Engineering Task Force: Internet X.509 Public Key Infrastructure Certificate and Certificate Revocation List (CRL) Profile. RFC 5280 Szabvány javaslat, Fremont, Egyesült Államok, 2008.
[81] Magyarország Kormánya: 1995. évi XCVII. törvény a légiközlekedésről, url: https://net.jogtar.hu/jogszabaly?docid=99500097.tv (elérhető online 2022.06.27.)
[82] Kiwi Quads: What Are Drone Radio Protocols and Which One Should I Use? url: https://www.kiwiquads.co.nz/what-are-drone-radio-protocols-and-which-one-should-i-use/ (elérhető online 2022.06.27.)
[83] Ardupilot: CAN Bus Setup. url: https://ardupilot.org/copter/docs/common-canbus-setup-advanced.html (elérhető online 2022.06.27.)
[84] Khan, N., Zaman, N., Brohi, S., Nayyar, A.: Emerging use of UAV's: secure communication protocol issues and challenges. Drones in Smart-Cities (pp.37-55), 2020, 10.1016/B978-0-12-819972-5.00003-3
[85] Domin, K., Marin, E., Symeonidis, I.: Security Analysis of the Drone Communication Protocol: Fuzzing the MAVLink protocol. ESAT-COSIC and iMinds, KU Leuven, Leuven-Heverlee, Belgium, 2016. url: https://www.esat.kuleuven.be/cosic/publications/article-2667.pdf (elérhető online 2022.06.27.)

[86] Mavlink.io: Serialization · MAVLink Developer Guide, https://mavlink.io/en/guide/serialization.html (elérhető online 2022.06.27.)
[87] Message Signing – MAVLink Developer Guide. url: https://MAVLink.io/en/guide/message_signing.html (elérhető online 2022.06.27.)
[88] National Institute of Standards and Technology: Transitioning the Use of Cryptographic Algorithms and Key Lengths, NIST Special Publication 800-131A Revision 2, Gaithersburg, Egyesült Államok, NIST, 2019., url: https://doi.org/10.6028/NIST.SP.800-131Ar2 (elérhető online 2022.06.27.)
[89] Butcher, N., Stewart, A., Biaz, S.: Securing the MAVLink Communication Protocol for Unmanned Aircraft Systems. Technical Report #CSSE14-02, https://pdfs.semanticscholar.org/4ce0/68b40089549f3d445d30e45fe8b53a141c88.pdf (elérhető online 2022.06.27.)
[90] Open Drone ID: Welcome to opendroneid.org - Open Drone ID, url: https://www.opendroneid.org/ (elérhető online 2022.06.27.)
[91] Krick, K.: Ericsson CM-HA. In: IEEE CQR – ERT, Bologna, Olaszország, 2017.07.03., url: http://cqr.committees.comsoc.org/files/2017/03/04-Kelly_Krick.pdf (elérhető online 2022.06.27.)
[92] Blazsovszky György: NetBriefing és MyDroneSpace. VFR Repülésbiztonsági Fórum, url: 2019, https://www.youtube.com/watch?v=RD0gq0Ahngc (elérhető online 2022.06.27.)
[93] Ericsson: Overview – Device & Data Management. url: https://docs.ddm.iot-accelerator.ericsson.net/?page_id=7391 (elérhető online 15.11.2019.)
[94] International Software Testing Qualifications Board: Tesztinfrastruktúra | ISTQB Glossary, url: https://istqb-glossary.page/hu/tesztinfrastruktura/ (elérhető online 2022.06.27.)
[95] Ardupilot: GCS Failsafe. url: https://ardupilot.org/copter/docs/gcs-failsafe.html (elérhető online 2022.06.27.)
[96] Bottyán Zs.: UAS_ENVIRON KKT eredményei, VOLARE zárórendezvény, NKE, Szolnok, url: http://ginop.szrf.hu/galeria/2021.03.11_Volare_live_event.mp4 (elérhető online 2022.06.27.)
[97] Cím nélküli riport, url: http://ginop.szrf.hu/galeria/2021.03.19_VOLARE_3.mp4 (elérhető online 2022.06.27.)
[98] Pavlock, K. M.: Aerospace Engineering Handbook Chapter 2(v): Flight Test Engineering. National Aeronautics and Space Administration Dryden Flight Research Center, Edwards, California, USA, 2014. url: https://ntrs.nasa.gov/api/citations/20140010192/downloads/20140010192.pdf (elérhető online 2022.06.27.)
[99] Ardupilot: Copter Home – Copter documentation, url: https://ardupilot.org/copter/index.html (elérhető online 2022.06.27.)
[100] Ardupilot: Archived: APM 2.5 and 2.6 Overview, https://ardupilot.org/copter/docs/common-apm25-and-26-overview.html (elérhető online 2022.06.27.)
[101] Jsumo.com: Dean's T Plug Pair (Female - Male), url: https://www.jsumo.com/deans-t-plug-female-male (elérhető online 2022.06.27.)
[102] Wikipedia: Tamiya connector, url: https://en.wikipedia.org/wiki/Tamiya_connector (elérhető online 2022.06.27.)
[103] National Center for Atmospheric Research - University Corporation for Atmospheric Research: WEATHER RESEARCH AND FORECASTING MODEL, url: https://www.mmm.ucar.edu/weather-research-and-forecasting-model (elérhető online 2022.06.27.)

[104] Mouat, A.: Using Docker: Developing and Deploying Software with Containers. ISBN-13: 978-1491915769, Sebastopol, Kalifornia, USA, O'Reilly Media, 2016.
[105] conus12km_data_v3, url: http://www2.mmm.ucar.edu/WG2bench/conus12km_data_v3 (elérhető online2017.03.22.)
[106] WRF V3 Parallel Benchmark Page, url: http://www2.mmm.ucar.edu/wrf/WG2/benchv3/ (elérhető online 2017.03.22.)
[107] WRF 12 Kilometer CONUS Benchmarks, url: http://www2.mmm.ucar.edu/wrf/WG2/benchv3/12KM_Results_20100414percore.htm (elérhető online 2017.03.22.)
[108] Elston, J. S.: Overview of Small Fixed-Wing Unmanned Aircraft for Meteorological Sampling, Journal of Atmospheric and Oceanic Technology. 32. 97-115. 10.1175/JTECH-D-13-00236.1. url: https://www.researchgate.net/publication/271200483_Overview_of_Small_Fixed-Wing_Unmanned_Aircraft_for_Meteorological_Sampling (elérhető online 2022.06.27.)
[109] Bottyán Zs.: A közfeladatot ellátó repülések meteorológiai biztosításának kérdései. Repüléstudományi Szemelvények, ISBN 978-615-5845-26-0, Nemzeti Közszolgálati Egyetem Katonai Repülő Intézet, Szolnok, 2017, url: http://www.repulestudomany.hu/kiadvanyok/RepSzem_Bottyan_Zs.pdf (elérhető online 2022.06.27.)
[110] Weidinger T. et al: A pilótanélküli repülőeszközök szerepe a határréteg kutatásban – nemzetközi mérési expedíció Szegeden, url: http://www.repulestudomany.hu/UAV/UAV_Workshop_2014/WS_WT.pdf (elérhető online 2022.06.27.)
[111] MAVLink Developer Guide: Arm Authorization, url: https://mavlink.io/en/services/arm_authorization.html (elérhető online 2022.06.27.)
[112] Berek T.: ABV (CBRN) analitikai laboratórium, mint művelettámogató speciális vegyivédelmi képesség, 2011. pp. 137. Hadmérnök VI. Évfolyam 1. szám - 2011. január ISSN1788-1919 url: http://www.hadmernok.hu/2011_1_berek.pdf (elérhető online 2022.06.27.)
[113] K. Hartmann, K. Giles: UAV Exploitation: A New Domain for Cyber Power. In: 2016 8th International Conference on Cyber Conflict, Cyber Power, N.Pissanidis, H.Rõigas, M.Veenendaal (Eds.), NATO CCD COE Publications, Tallinn, 2016
[114] PrimeKey: Drone safety via security – PKI in action, url: https://www.primekey.com/blog/2019/05/23/drone-safety-via-security-pki-in-action/ (elérhető online 2022.06.27.)
[115] DigiCert: AirMap, DigiCert Introduce First-Ever Digital Identity Certificate for Drones. url: https://www.digicert.com/news/2016-12-13-digicert-partners-with-airmap-for-drone-id/ (elérhető online 2022.06.27.)
[116] Fongen A., Mancini F.: Integrity Attestation in Military IoT. In: IEEE 2nd World Forum on Internet of Things (WF-IoT), Milánó, Olaszország, 2015, DOI: 10.1109/WF-IoT.2015.7389102
[117] Rutkowski A.: ITU-T Takes Lead on Drone IoT Identification in 2019. url: http://www.circleid.com/posts/20190103_itu_t_takes_lead_on_drone_iot_identification_in_2019/ (elérhető online 2022.06.27.)
[118] International Telecommunication Union – Telecommunication Standardization Sector: Identification mechanism for unmanned aerial vehicles using object identifiers. ITU-T X.677 (ex X.uav-oid) work item, Genf, Svájc, 2019.

[119] American National Standards Institute: Small Unmanned Aerial Systems Serial Numbers. CTA 2063-2017 (ANSI standard), Washington, Egyesült Államok, 2017.
[120] European Union Aviation Safety Agency: Drones (UAS) | EASA, url: https://www.easa.europa.eu/the-agency/faqs/drones-uas#category-regulations-on-uas-drone-explained (elérhető online 2022.06.27.)
[121] American Society for Testing and Materials: Standard Specification for Remote ID and Tracking, ASTM F3411-19, url: https://www.astm.org/f3411-19.html (elérhető online 2022.06.27.)
[122] Federal Aviation Administration: Remote Identification of Unmanned Aircraft, FA-A-2019-1100-53264, Washington DC, Egyesült Államok, 2021. url: https://www.regulations.gov/document/FAA-2019-1100-53264 (elérhető online 2022.06.27.)
[123] AeroSpace and Defence Industries Association of Europe – Standardization: Aerospace series - Unmanned Aircraft Systems - Part 002: Direct Remote Identification; English version prEN 4709-002:2020, url: https://asd-stan.org/downloads/din-en-4709-0022021-02/ (elérhető online 2022.06.27.)
[124] Robertson J., Riley M.: The Big Hack: How China Used a Tiny Chip to Infiltrate U.S. Companies, url: https://www.bloomberg.com/news/features/2018-10-04/the-big-hack-how-china-used-a-tiny-chip-to-infiltrate-america-s-top-companies (elérhető online 2022.06.27.)
[125] Európai Parlament, Európai Unió Tanácsa: Az Európai Parlament és a Tanács (EU) 2016/679 Rendelete a természetes személyeknek a személyes adatok kezelése tekintetében történő védelméről és az ilyen adatok szabad áramlásáról, valamint a 95/46/EK rendelet hatályon kívül helyezéséről (általános adatvédelmi rendelet), (2016. április 27.) url: https://eur-lex.europa.eu/legal-content/HU/TXT/HTML/?uri=CELEX:32016R0679 (elérhető online 2022.06.27.)
[126] Sándor Zs.: A pilóta nélküli légijármű rendszerek forgalmi menedzsmentjét biztosító megoldások információrendszerének modellje, Repüléstudományi Közlemények XXIX. évfolyam, 2017/3, pp 167-178. url: http://real.mtak.hu/74184/1/2017_3_13_0417_Sandor_Zsolt_u.pdf (elérhető online 2022.06.27.)
[127] Ijaz, I., Aslam, A., Bukhari, B., Javed, R., Anees, S.: Securing cloud infrastructure through PKI. In: 5th International Conference on Computing, Communication and Networking Technologies (ICCCNT), 2014. 1-6. 10.1109/ICCCNT.2014.6963055.
[128] Szabó V.: Lime elektromos roller használata, url: https://blog.szaboviktor.com/lime-elektromos-roller/ (elérhető online 2022.06.27.)
[129] Gyöngyösi A. Z.: Wind measurement using small drones, In: I. MyDroneMet konferencia, Zalaegerszeg, 2021.12.19. url: https://mouldtechsystems.hu/wp-content/uploads/2022/01/mydronemet_aviation_meteorology_conference_-_gyongyosi_zeno.pdf (elérhető online 2022.06.27.)
[130] Jain L., Vyas J.: Security Analysis of Remote Attestation, CS259 Project Report, url: https://seclab.stanford.edu/pcl/cs259/projects/cs259_final_lavina_jayesh/CS259_report_lavina_jayesh.pdf (elérhető online 2022.06.27.)
[131] MAVLink: Open Drone ID (WIP), url: https://mavlink.io/en/services/opendroneid.html (elérhető online 2022.06.27.)
[132] Kerti A.: Átviteli út biztonság. HADMÉRNÖK II:(4) 2007, pp. 60–65. url: http://www.hadmernok.hu/archivum/2007/4/2007_4_kerti.html (elérhető online 2022.06.27.)
[133] GliderNet: OGN DDB - registered devices, url: http://wiki.glidernet.org/ddb-list (elérhető online 2022.06.27.)

[134] Bottyán Zs., Wantuch F., Gyöngyösi Z., Tuba Z., Hadobács K., Kardos P., Kurunczi R.: Development of a Complex Meteorological Support System for UAVs. WORLD ACADEMY OF SCIENCE ENGINEERING AND TECHNOLOGY 7:(4) pp. 646-651. 2013.
[135] Bottyán Zs. et al: Measuring and Modeling of Hazardous Weather Phenomena to Aviation Using the Hungarian Unmanned Meteorological Aircraft System (HUMAS). IDŐJÁRÁS / QUARTERLY JOURNAL OF THE HUNGARIAN METEOROLOGICAL SERVICE 119:(3) pp. 307-335. (2015).
[136] Gyongyosi A. Z., Kardos P., Kurunczi R., Bottyan Zs.: Development of a complex dynamical modeling system for the meteorological support of unmanned aerial operation in Hungary. In: Kimon P Valavanis, Pascual Campoy (szerk.) 2013. International Conference on Unmanned Aircraft Systems (ICUAS): Conference Proceedings. 1172 p. Konferencia helye, ideje: Atlanta (GA), Amerikai Egyesült Államok, 2013.05.28-2013.05.31. Atlanta (GA): IEEE, 2013. pp. 8-16. (ISBN:978-1-4799-0815-8)
[137] Makkay I.: Ütközések elkerülése a kisgépes és a pilóta nélküli repülésben. REPÜLÉSTUDOMÁNYI KÖZLEMÉNYEK (1997-TŐL) XXIX:(1), 2017, pp. 59–66. url: http://www.repulestudomany.hu/folyoirat/2017_1/2017-1-04-0378_Makkay_Imre.pdf (elérhető online 2022.06.27.)
[138] Open Glider Network: OGN architecture, url: http://ognproject.wdfiles.com/local--files/start/OGN_Arch.png (elérhető online 2022.06.27.)
[139] Github: OGN flavoured APRS, url: https://github.com/svoop/ogn_client-ruby/wiki/OGN-flavoured-APRS (elérhető online 2022.06.27.)
[140] Github: magicbug/PHP-APRS-Passcode, url: https://github.com/magicbug/PHP-APRS-Passcode/blob/master/aprs_func.php (elérhető online 2022.06.27.)
[141] Haig Zs.: In. Kovács László (szerk.) Információ - társadalom – biztonság. NKE Szolgáltató Kft., Budapest, 2015. (ISBN:978-615-5527-08-1)
[142] GliderNet: List of OGN Receivers, url: http://wiki.glidernet.org/list-of-receivers (elérhető online 2022.06.27.)
[143] GliderTracker: Welcome, url: http://glidertracker.org (elérhető online 2022.06.27.)
[144] APRS Passcode Generator: Techical Example of Passcode Generation using PHP, url: https://apps.magicbug.co.uk/passcode/index.php (elérhető online 2022.06.27.)
[145] OpenDroneID: Open Drone ID Core C Library, url: https://github.com/opendroneid/opendroneid-core-c (elérhető online 2022.06.27.)
[146] OpenDroneID: Example Android receiver application for unmanned aircraft Remote ID, url: https://github.com/opendroneid/receiver-android (elérhető online 2022.06.27.)
[147] OpenDroneID: Conceptual overview, url: https://mavlink.io/assets/opendroneid/conceptual_overview.png (elérhető online 2022.06.27.)
[148] MAVLink: MAVLINK Common Message Set, MAV_COMPONENT, url: https://mavlink.io/en/messages/common.html#MAV_COMP_ID_ALL (elérhető online 2022.06.27.)
[149] Weisstein, E. W.: Birthday Problem. url: https://mathworld.wolfram.com/BirthdayProblem.html (elérhető online 2022.06.27.)
[150] Weisstein, E. W.: Birthday Attack. url: https://mathworld.wolfram.com/BirthdayAttack.html (elérhető online 2022.06.27.)
[151] Spala F.: Bluetooth eszközök biztonsági kérdései, diplomamunka, Eötvös Loránd Tudományegyetem, Budapest, 2008. url: http://krasznay.hu/presentation/diploma_spala.pdf (elérhető online 2022.06.27.)

[152] Debreczeni Á.: My bike ride in AR. (Unity + ARKit + Mapbox + Strava), url: https://twitter.com/heyadam/status/872278723700994048 (elérhető online 2022.06.27.)

FÜGGELÉK/MELLÉKLETEK

Definíciók jegyzéke

Képletek jegyzéke

Táblázatok jegyzéke

Ábrák jegyzéke

Az értekezés ábráinak elkészítéséhez (nem kereskedelmi céllal) felhasznált képek elérhetőségei:

- https://www.pngegg.com/en/png-xtydl
- https://www.pngegg.com/en/png-zbjqv
- https://www.pngegg.com/en/png-yiofo
- https://www.seekpng.com/ima/u2a9o0o0q8w7a9q8/
- https://www.pngkey.com/maxpic/u2w7i1u2o0o0o0r5/
- https://www.pngkey.com/maxpic/u2w7r5t4a9q8t4i1/
- https://www.pngkey.com/maxpic/u2a9o0o0a9e6t4i1/
- https://www.pngkey.com/maxpic/u2y3w7w7q8r5a9t4/
- https://www.pngkey.com/maxpic/u2t4e6i1i1t4o0t4/
- https://www.pngkey.com/maxpic/u2q8a9y3t4e6w7y3/
- https://www.pngkey.com/maxpic/u2w7o0e6i1o0y3o0/
- https://www.pngkey.com/maxpic/u2q8q8o0t4u2y3q8/
- https://www.pngkey.com/maxpic/u2q8a9q8i1t4u2q8/
- https://www.pngkey.com/maxpic/u2w7a9q8i1e6t4u2/
- https://www.pngkey.com/maxpic/u2e6a9e6w7i1y3a9/
- https://www.pngkey.com/maxpic/u2q8r5a9t4o0i1a9/
- https://www.pngkey.com/maxpic/u2e6u2a9t4t4u2i1/

FOGALMAK ÉS RÖVIDÍTÉSEK JEGYZÉKE

Rövidítés	Angol megfelelő	Magyar fordítás
4G	4th Generation	4. generációs (mobilhálózat)
5G	5th Generation	5. generációs (mobilhálózat)
ABV		atom, biológiai, vegyi
AIS	Aeronautical Information Service	Repüléstájékoztató szolgáltatás
ANSI	American National Standards Institute	Amerikai Nemzeti Szabványügyi Intézet
API	Application Programming Interface	alkalmazásprogramozási felületet
APM	ArduPilot Mega	
APRS	Automatic Packet Reporting System	automata csomagjelentő rendszer
AR	Augmented Reality	kiterjesztett valóság
ARP	Address Resolution Protocol	cím feloldási protokoll
ASCII	American Standard Code for Information Interchange	amerikai szabványos kódolás információátadásra
ASD-STAN	AeroSpace and Defence Industries Association of Europe - Standardization	Légiközlekedési és Védelmi Ipari Szereplők Szervezete – Szabványügy
ASTM	American Society for Testing and Materials	Tesztelés és Anyagok Amerikai Társasága
C2	Command and Control	vezetés-irányítás
C3	Consultation, Command and Control	konzultáció, vezetés-irányítás
C4ISR	Command, Control, Communications, Computers, Intelligence, Surveillance and Reconnaissance	a vezetés, irányítás, kommunikáció, számítógép, hírszerzés, megfigyelés és felderítés
CA	Certificate Authority	tanúsító hatóság
CAA	Civil Aviation Authority	Polgári Légügyi Hatóság
CAN	Controller Area Network	vezérlőközeli hálózat
CONUS	Continental United States	Kontinentális Egyesült Államok
CRC	Cyclic Redundancy Check	ciklikus redundancia vizsgálat
CRL	Certificate Revocation List	visszavont tanúsítványok listája
CSR	Certificate Signing Request	tanúsítvány aláírási kérelemnek

Rövidítés	Angol megfelelő	Magyar fordítás
DaaS	Data as a Service	szolgáltatásként kínált adat
DNS	Domain Name System	tartománynév rendszer
DoD	Department of Defense	(Amerikai) Védelmi Minisztérium
DOE		Drónpilóták Országos Egyesülete
EASA	European Union Aviation Safety Agency	Európai Repülésbiztonsági Ügynökség
ENISA	The European Union Agency for Cybersecurity	Európai Unió Hálózati és Információbiztonságért felelős Ügynöksége
ETSI	European Telecommunications Standards Institute	Európai Távközlési Szabványügyi Intézet
Flarm	Flight Alarm	„légi riasztó”
GDPR	General Data Protection Regulation	Általános adatvédelmi rendelet
GPS	Global Positioning System	globális helymeghatározó rendszer
HA	High Availability	magas fokú rendelkezésre állás
HALE	High Altitude Long Endurance	nagy magasságú, nagy hatótávolságú (UAV)
HAPS	High-Altitude Pseudo-Satellite	nagy magasságú pszeudoműhold
IaaS	Infrastructure as a Service	szolgáltatásként kínált infrastruktúra
ICAO	International Civil Aviation Organization	Nemzetközi Polgári Repülési Szervezet
ICMP	Internet Control Message Protocol	internet vezérlőüzenet protokoll
IMU	Inertial Measurement Unit	inerciális mérőegység
IEC	International Electrotechnical Commission	Nemzetközi Elektrotechnikai Bizottság
IP	Internet Protocol	Internet Protokoll
ISO	International Organization for Standardization	Nemzetközi Szabványügyi Szervezet
ISTQB	International Software Testing Qualifications Board	Nemzetközi Szoftvertesztelési Minősítő Testület
LB	Load Balancing	terheléselosztás
MaaS	Mission as a Service	szolgáltatásként kínált küldetés
MAC	Media Access Control	média hozzáférés vezérlő

Rövidítés	Angol megfelelő	Magyar fordítás
MAV	Micro Air Vehicle	kis méretű légijármű
NAIH		Nemzeti Adatvédelmi és Információszabadság Hatóság
NaN	Neighbor-aware Network	(wifi) szomszédtudatos hálózat
NATO	North Atlantic Treaty Organisation	Észak-atlanti Szerződés Szervezete
NDZ	No Drone Zone	drón repülés elől elzárt légtér
NFC	Near Field Communication	rövid hatótávú kommunikációs
NFM		Nemzeti Fejlesztési Minisztérium
NIST	National Institute of Standards and Technology	Nemzeti Szabványügyi és Technológiai Intézet
OCSP	Online Certificate Status Protocol	online tanúsítvány státusz protokoll
OGN	Open Glider Network	nyílt vitorlázórepülő hálózat
OID	Object Identifier	objektumazonosító
OTG	On-The-Go	(USB) irányított töltő- és adatkábel
PaaS	Platform as a Service	szolgáltatásként kínált platform
PKCS	Public Key Cryptography Standards	nyilvános kulcsú kriptográfiai szabványok
PKI	Public Key Infrastructure	publikus kulcsú infrastruktúra
PSK	Pre-Shared Key	előre kiosztott titkos kulcs
PWM	Pulse Width Modulation	impulzusszélesség-moduláció
Pymavlink	Python MAVLink	
RA	Registration Authority	nyilvántartó hatóság
RFID	Radio Frequency IDentification	rádiófrekvenciás azonosító
RPAS	Remotely Piloted Aircraft System	távolról repültetett légijármű rendszer
RPV	Remotely Piloted Vehicle	távolról repültetett jármű
SaaS	Software as a Service	szolgáltatásként kínált szoftver
SD	Secure Digital	biztonságos digitális (kártya)
SQL	Structured Query Language	strukturált lekérdezőnyelv
SSID	Service Set IDentifier	(wifi) szolgáltatáskészlet-azonosító
SSL	Secure Sockets Layer	biztonságos socket réteg
STaaS	STorage as a Service	szolgáltatásként kínált tárhely
TCO	Total Cost of Ownership	teljes tulajdonlási költség

Rövidítés	Angol megfelelő	Magyar fordítás
TCP	Transmission Control Protocol	átvitelvezérlési protokoll
TCP/IP	Transmission Control Protocol/Internet Protocol	átviteli vezérlő protokoll/internetprotokoll
TLS	Transport Layer Security	átviteli szint biztonság
TPM	Trusted Platform Module	megbízható platform modul
TRANSEC	Transport Security	átviteli biztonság
TTCN-3	Test and Test Control Notation version 3	3-as verziójú teszt- és tesztvezérlés leíró
UART	Universal Asynchronous Receiver-Transmitter	univerzális aszinkron adóvevő
UAS	Unmanned Aircraft System	személyzet nélküli légijármű-rendszer
UAV	Unmanned Aerial Vehicle	személyzet nélküli légijármű
UDP	User Datagram Protocol	felhasználói datagram protokoll
UML	Unified Modeling Language	Egységesített Modellező Nyelv
URL	Uniform Resource Locator	egységes erőforrás-helymeghatározó
USA	United States of America	Amerikai Egyesült Államok
USB	Universal Serial Bus	univerzális soros busz
UTM	Unmanned Aircraft Systems Traffic Management	pilóta nélküli légijármű-rendszerek forgalmi menedzsmentje
UUID	Universally Unique IDentifier	univerzális egyedi azonosító
VIO	Visual Inertial Odometry	Vizuális inerciális odometria
VM	Virtual Machine	virtuális számítógép
VPS	Virtual Private Server	virtuális magán szolgáltató
VR	Virtual Reality	virtuális valóság
WRF	Weather Research and Forecasting	időjárás kutatási és előrejelzési (modell)

MELLÉKLETEK

Bájt index	Tartalom	Érték	Leírás
0	Csomag kezdete jelzés	0xFE	Protokoll specifikus jelzés. MAVLink rendszerek, melyek nem ismerik ezt a verziót, eldobják a csomagot.
1	Hordozott adat hossza	0 - 255	A hordozott adat hosszát (n) jelöli.
2	Csomag sorszám	0 - 255	Az elveszett csomagok detektálását segíti
3	Rendszer azonosító	1 - 255	A küldő rendszer azonosítója a csatornán. A csatornán kommunikáló egyedi rendszerek megkülönböztetésére szolgál.
4	Komponens azonosító	0 - 255	A küldő komponens azonosítója a rendszeren. A rendszeren belüli komponensek megkülönböztetésére szolgál (például robotpilóta, kamera). Részleteket lásd a 7.2.4 fejezetben.
5	Üzenet típus	0 - 255	Az üzenet típus azonosítója. A hordozott adatstruktúra deszerializálását segíti.
6-tól (n+6)-ig	Hordozott adat		Az üzenet típus által meghatározott adatstruktúra.
(n+7)-től (n+8)-ig	Ellenőrző összeg		Az üzenetre vonatkozó X.25 ciklikus redundancia vizsgálat (CRC[92]) által megállapított érték (a csomag kezdete jelzést kivéve). CRC extra bájtot tartalmaz.

1. melléklet: A MAVLink 1.0 csomagszerkezete.
(A táblázatot fordította és szerkesztette a szerző. Forrás: [86])

[92] Cyclic Redundancy Check

Bájt index	Tartalom	Érték	Leírás
0	Csomag kezdete jelzés	0xFD	Protokoll specifikus jelzés. MAVLink rendszerek, melyek nem ismerik ezt a verziót, eldobják a csomagot.
1	Hordozott adat hossza	0 - 255	A hordozott adat hosszát (n) jelöli.
2	Inkompatibilitás jelzők		Funkcionalitás jelzők, amiket a fogadó komponensnek kötelezően képesnek kell lennie értelmezni. A csomag eldobásra kerül, ha a rendszer nem felel meg a feltételeknek.
3	Kompatibilitás jelzők		Funkcionalitás jelzők, amiket a fogadó komponens opcionálisan képes lehet értelmezni. A csomag feldolgozásra kerülhet akkor is, ha a rendszer nem képes teljes mértékben értelmezni.
4	Csomag sorszám	0 - 255	Az elveszett csomagok detektálását segíti
5	Rendszer azonosító	1 - 255	A küldő rendszer azonosítója a csatornán. A csatornán kommunikáló egyedi rendszerek megkülönböztetésére szolgál.
6	Komponens azonosító	0 - 255	A küldő komponens azonosítója a rendszeren. A rendszeren belüli komponensek megkülönböztetésére szolgál (például robotpilóta, kamera). Részleteket lásd a 7.2.4 fejezetben.
7-től 9-ig	Üzenet típus azonosító	0 - 16777215	Az üzenet típus azonosítója. A hordozott adatstruktúra deszerializálását segíti.
10-től (n+10)-ig	Hordozott adat		Az üzenet típus által meghatározott adatstruktúra.
(n+11)-től (n+12)-ig	Ellenőrző összeg		Az üzenetre vonatkozó X.25 CRC (a csomag kezdete jelzést kivéve). CRC extra bájtot tartalmaz.
(n+12)-től (n+26)-ig	Aláírás		(Opcionális) A csomag átvitel közbeni módosításának megelőzésére szolgál.

2. melléklet: A MAVLink 2.0 csomagszerkezete.
(A táblázatot fordította és szerkesztette a szerző. Forrás: [86])

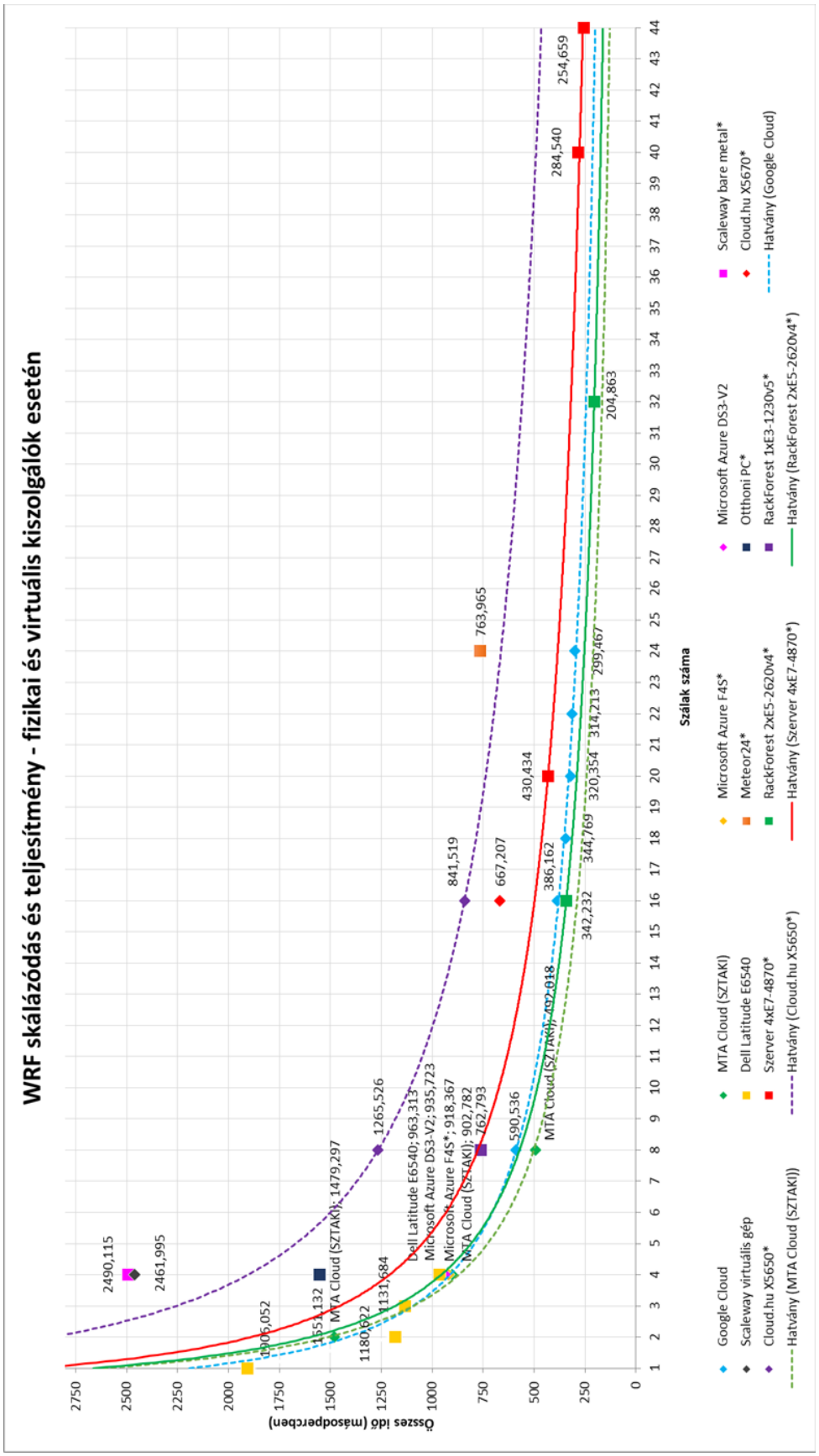
Name of system	OS and version	Processor	Cores	Main memory	Other relevant information	Price in EUR/hr
Google Cloud	CentOs 7.3	vCPU (VM instance)	8*, 16, 18*, 20*, 22*, 24* cores	32 GB	5 measurements and pricing on 16 CPU, only 1 on 8, 18, 20, 22, 24	0,472
MTA Cloud (SZTAKI & Wigner)		vCPU / Intel(R) Xeon(R) CPU E5-2640 v3 @ 2.60GHz	2, 4, 8 cores	8 GB	m1.xlarge, KVM, currently free, pricing to be determined	0
Microsoft Azure F4S*	CentOs 7.3	vCPU (VM instance)	4 cores	2 GB/core	F4S type VM, local SSD	0,21
Microsoft Azure DS3-V2	CentOs 7.3	vCPU (VM instance)	4 cores	3.5 GB/core	DS3_V2 type VM, local SSD	0,31
Scaleway bare metal*		Intel(R) Atom(TM) CPU C2550 @ 2.40GHz	4 cores (dedicated)	2 GB/core	C2S (only one measurement, no significant difference from VM)	0,024
Scaleway virtual machine		vCPU / Intel(R) Atom(TM) CPU C2750 @ 2.40GHz	4 cores	1 GB/core	VC1M type VM	0,012
Dell Latitude E6540	Ubuntu 14.04.5	Intel(R) Core(TM) i7-4600M CPU @ 2.90GHz, 4096 KB L3 cache, HT	2 core/1 socket (4 core with HT)	4 GB/core DDR3	2000 EUR price with 3 years factory warranty as expected lifetime => 0,076103501 EUR/hrs; 0,14362 kWh adapter consumption, ~40 HUF/kWh = 0.1296 EUR/kWh => 0,018613152 EUR/hrs power; server room, networking, maintenance not included, it is an off-the-shelf laptop	0,09471665
Meteor24*		Intel Xeon E5645 (HT enabled) @ 2.40GHz	6 core/2 socket (12 core with HT/socket = 24 core)			No estimate

Name of system	OS and version	Processor	Cores	Main memory	Other relevant information	Price in EUR/hr
Home PC*		Intel i7-4500U (HT enabled) @ 1.80Ghz	2 core/1 socket (4 core with HT)			No estimate
Cloud.hu X5670*		Intel Xeon E5670 @ 2.93GHz	16 cores		52 HUF/hrs	0,1683
Cloud.hu X5650*		Intel Xeon E5650 @ 2.67GHz	8, 16 cores		35 HUF/hrs, 52 HUF/hrs	0,1683
Server with 4xE7-4870*		Intel Xeon E7-4870 @ 2.4Ghz (HT enabled)	10 cores/4 socket (80 cores with HT) max; 20, 40, 44 tested			No estimate
RackForest 2xE5-2620v4*		Intel Xeon E5-2620v4 @ 2.1Ghz (HT enabled)	8, 16 cores (16, 32 cores with HT)	16 GB	61 595 HUF/mon, 730hrs/mon, 309 HUF=1 EUR	0,27306379
RackForest 1xE3-1230v5*		Intel Xeon E3-1230v5 @ 3.40GHz (HT enabled)	4 cores (8 cores with HT)	8 GB	33 655 HUF/mon, 730hrs/mon, 309 HUF=1 EUR	0,1491998

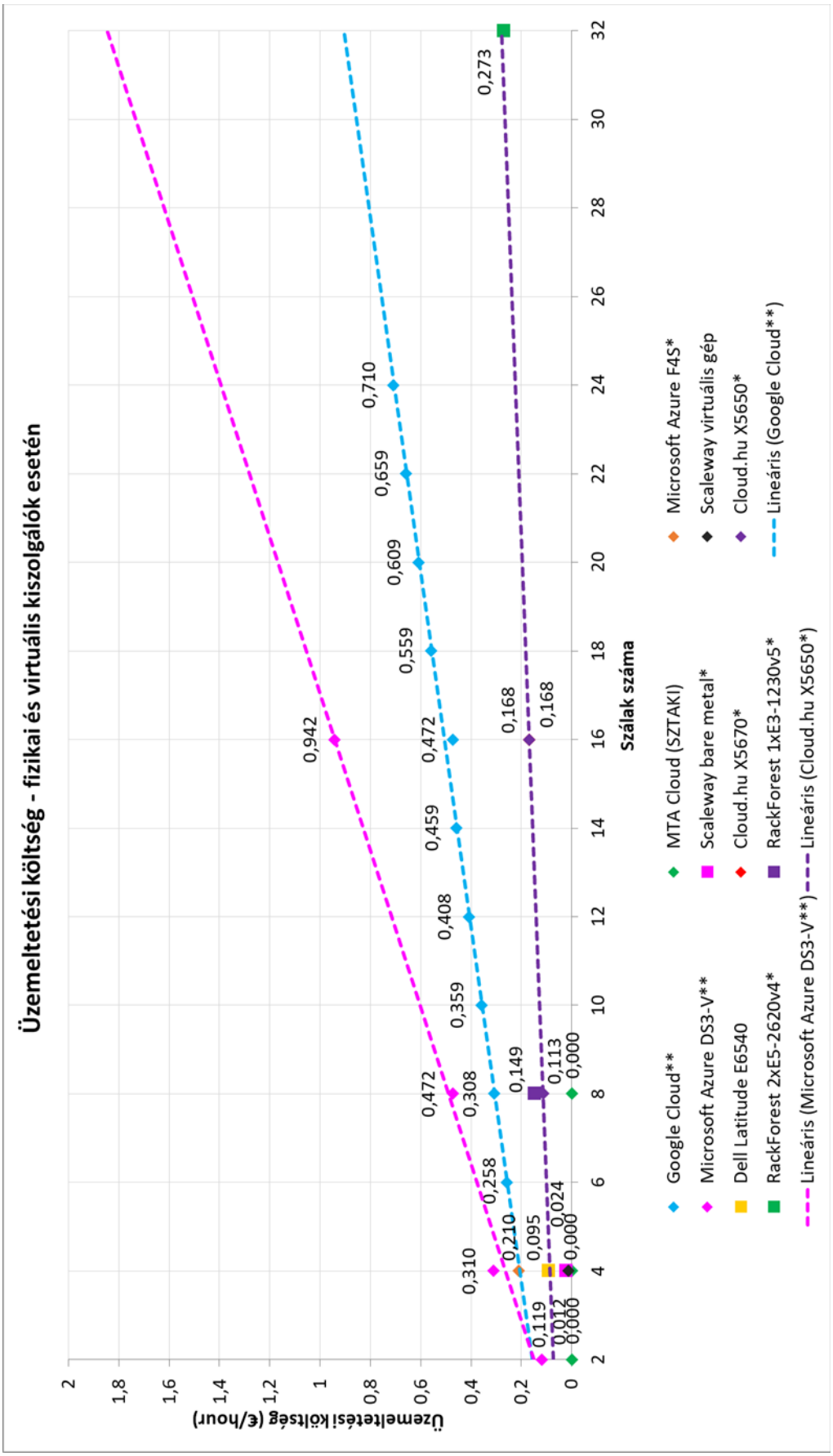
3. melléklet: A mért számítógépes platformok paraméterei és költsége.

Platform	max	min	sum	mean	mean/max
Google Cloud* (24 vCPU)	37,18933	1,66924	299,46712	2,009846	0,054044
Google Cloud* (22 vCPU)	36,12584	1,73918	314,21317	2,108813	0,058374
Google Cloud* (20 vCPU)	34,49511	1,80248	320,35418	2,150028	0,062328
Google Cloud* (18 vCPU)	32,55316	1,96589	344,76927	2,313888	0,07108
Google Cloud (16 vCPU)	37,246576	2,125868	386,16173	2,5916894	0,0697048
Google Cloud* (8 vCPU)	40,47653	3,35293	590,5361	3,96333	0,097917
Meteor24* (24 CPU)	7,47408	4,89977	763,96539	5,127284	0,686009
MTA Sztaki (8 vCPU)	27.63295	2.870226667	492.0180633	3.302134667	0.11959733
MTA Sztaki (4 vCPU)	34,6256067	5,02694667	902,78249	6,058943	0,17501467
MTA Sztaki (2 vCPU)	38,67514667	8,79911	1479,296663	9,928165667	0,25693467
MS Azure DS3-V2 (4 vCPU)	53,1951167	5,52487	935,723123	6,280021	0,11805633
MS Azure F4S* (4 vCPU)	52,32974	5,45215	918,36701	6,163537	0,117783
Dell Latitude E6540 4 CPU	54,29862	5,74593333	963,312567	6,465185	0,119211
Dell Latitude E6540 3 CPU	56,4589633	6,53817333	1131,68386	7,59519367	0,13461767
Dell Latitude E6540 2 CPU	59,8001067	7,09618	1180,62247	7,92364067	0,132617
Dell Latitude E6540 1 CPU	50,9827133	11,7637033	1906,052	12,792295	0,25136767
Home PC* (4 CPU)	37,67339	9,00919	1551,13173	10,41028	0,27633
Scaleway* (4 CPU)	67,3522	15,24812	2490,11511	16,712182	0,248131
Scaleway (4 vCPU)	66,26103	15,02479	2461,99481	16,5234553	0,24941167
Cloud.hu X5670* (16 vCPU)	16,98585	3,66406	667,20701	4,477899	0,263625
Cloud.hu X5650* (16 vCPU)	38,47575	4,9053	841,5186	5,647776	0,146788
Cloud.hu X5650* (8 vCPU)	33,48545	7,42649	1265,52617	8,493464	0,253646
Server with 4xE7-4870* (44 core)	2,92551	1,55003	254,65935	1,709123	0,584214
Server with 4xE7-4870* (40 core)	24,35828	1,61425	284,53965	1,909662	0,078399
Server with 4xE7-4870* (20 core)	22,75208	2,54465	430,43406	2,888819	0,126969
RackForest with 2xE5-2620v4* (32 core)	20,33786	1,16616	204,86324	1,374921	0,067604
RackForest with 2xE5-2620v4* (16 core)	15,9864	2,03613	342,23198	2,296859	0,143676
RackForest with 1xE3-1230v5* (8 core)	24,41109	4,81531	762,7926	5,119413	0,209717

4. melléklet: WRF teljesítmény adatok.



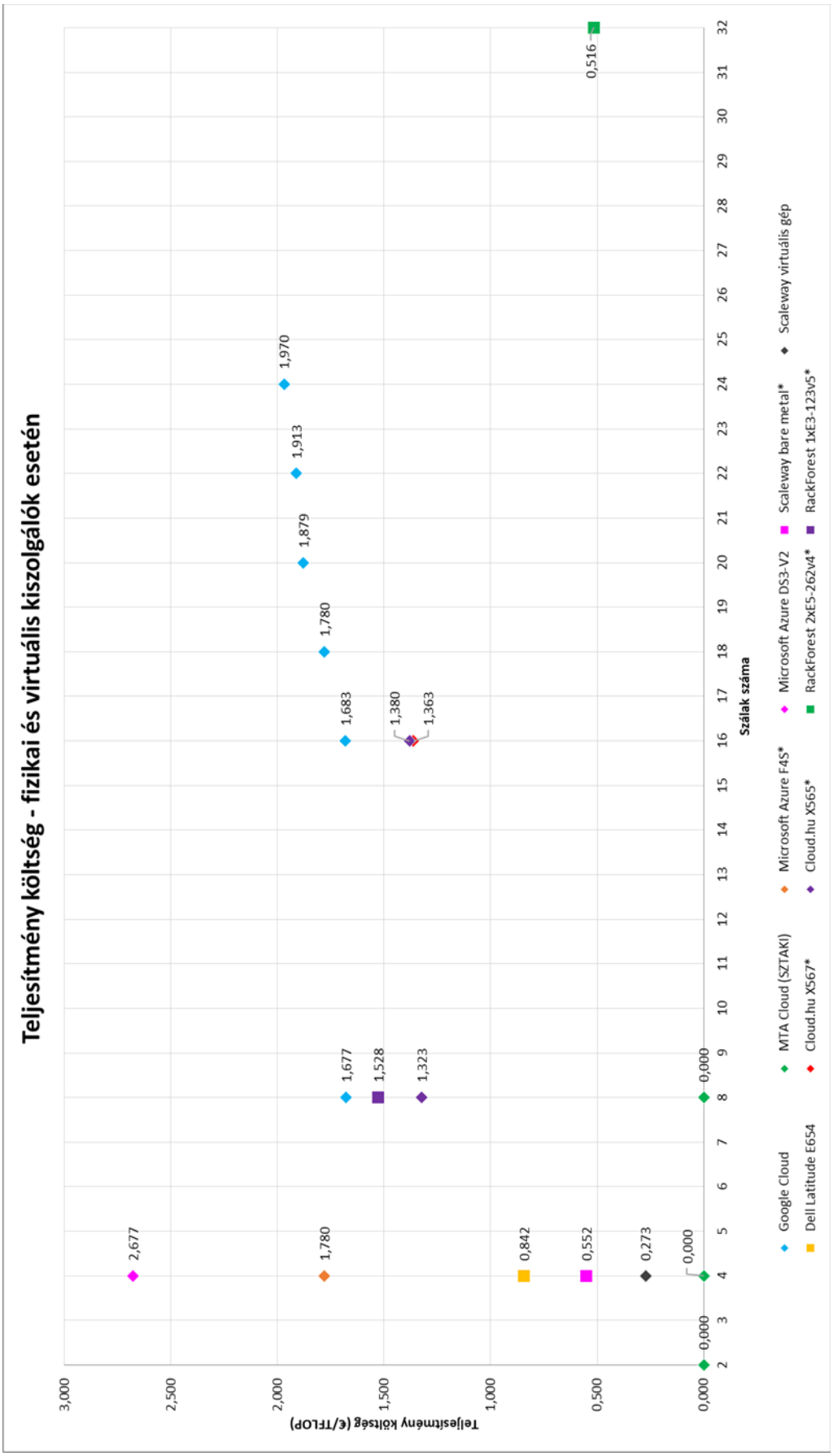
5. melléklet: WRF skálázódás és teljesítmény – fizikai és virtuális kiszolgálók esetén.



6. melléklet: Üzemeltetési költség – fizikai és virtuális kiszolgálók esetén.

Platform / szálak száma	2	4	8	16	18	20	22	24	32
Google Cloud			1,68	1,68	1,78	1,88	1,91	1,97	
MTA Cloud (SZTAKI)	0,00	0,00	0,00						
Microsoft Azure F4S*		1,78							
Microsoft Azure DS3-V2		2,68							
Scaleway bare metal*		0,55							
Scaleway virtuális gép		0,27							
Dell Latitude E654		0,84							
Cloud.hu X567*				1,36					
Cloud.hu X565*			1,32	1,38					
RackForest 2xE5-262v4*									0,52
RackForest 1xE3-123v5*			1,53						

7. melléklet: Teljesítmény és költség, €/TFLOP.



8. melléklet: Teljesítmény költség – fizikai és virtuális kiszolgálók esetén.

UA	Sensor placement	Wind	Humidity	Temperature	Pressure	Other
Cruiser	inside fuselage	GP/IMU/dynamic pressure	Varies	Varies	Varies	meteo + radiation, aerosol, athmosphere dynamics
UMARS 2	modular bay + boom	Five-hole hemisphere	Thermo couple	Meteolabor AG ‘‘Snow White’’ dewpoint hygrometer	Measured around five-hole hemisphere	hygrometer, IMU
Manta	inside and around fuselage	Nine-hole probe	Vaisala HMP45C	Vaisala HMP45C	All sensors barometric sensor	fast response turbulence, hygrometer, temperature | short- and longwave radiometer
ScanEagle	inside and under fuselage	Nine-hole probe	Vaisala HMP45C	Vaisala HMP45C	All sensors barometric sensor	(fast response turbulence, hygrometer, temperature | short- and longwave radiometer) + visible and infrared imagery, laser altimetry
BXAP15 (previously)	temporary mounting points in and on fuselage and wing	Five-hole Pitot-tube	Vaisala HMP45 + proprietary	Vaisala HMP45 + proprietary	Proprietary	Vaisala radiosonde
BXAP15	proprietary internal duct design	Proprietary (future)	Sparvio SKS2	Sparvio SKS2 (fast response)	Sparvio SKH1	Sparvio SKS4 (O3), Sparvio SKS6 (CO2), Sparvio SKH1 (GPS), Peviktera TRB82B OGN tracker
Aerosonde	varies (boom, above or under fuselage)	Proprietary algorithm	Vaisala RS90	Vaisala RS90	Vaisala RS90	
RPMSS	[no information]	GPS/INS	Humidity	Thermal resistor	MEMS	

UA	Sensor placement	Wind	Humidity	Temperature	Pressure	Other
			sensitive capacitor			
Tempest	under the wing	Aeroprobe five-hole probe	Vaisala RS92	Vaisala RS92	Proprietary autopilot sensor	
M2AV	on nose	Five-hole probe	Vaisala HMP50	Vaisala HMP50 and thermocouple	Sensortechnics 144SC0811 Baro	
CU NexSTAR	in each wingtip	Proprietary algorithm	2× Vaisala RS92	2× Vaisala RS92	Proprietary autopilot sensor	
MASC	on nose	Five-hole probe	Custom (Wildmann et al. 2013)	Thin wire and thermocouple (Wildmann et al. 2013)	Sensortechnics 144SC0811 Baro	
Aerolemma-3	shrouded boom upstream of propeller	None	CSI HMP50	CSI HMP50	CSI CS100	
SMARTSonde	inside fuselage	GPS/infrared	Sensiron SHT75	Sensiron SHT75/VTI SCP1000	VTI SCP1000	Aeroqual SM50 sensor, GPS
Powersonde	inside fuselage (varies)	None	NSSL Radiosonde	NSSL Radiosonde	NSSL Radiosonde	
Kali	above fuselage	None	Honeywell HIH-3605-B	National Semiconductor LM50 C	Motorola MPX 2100	
DataHawk	inside and above fuselage	GPS/infrared	Honeywell capacitive polymer	TI ADS1118	MS5611–01BA03	100-Hz cold-wire probe, GPS
SUMO	boom above nose	GPS/IMU	Sensiron SHT75	Sensiron SHT75 / PT1000	VTI SCP1000	IMU

9. melléklet: Merevszárnyú UAS-k szenzorálási lehetőségei.