

**NEMZETI KÖZSZOLGÁLATI EGYETEM
KATONAI MŰSZAKI DOKTORI ISKOLA**

Vránics Dávid Ferenc

**A felhő alapú rendszerekből vezérelt
pilóta nélküli légi jármű-rendszerek
biztonsági kérdései**

című doktori (PhD) értekezésének szerzői ismertetője

Témavezető: Dr. Palik Mátyás PhD

BUDAPEST, 2022

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 légitársaság-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 légitársaságok használata. A 2010-es évekre a média hatására a köztudatban is elterjedt e két különálló fogalom, napjainkra pedig már sor került a közös alkal-

mazásukra is – pilóta nélküli légi járműveket 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.

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 (IP¹) alapú hálózaton keresztül. Érdeemes 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 légi jármű-rendszerek esetén kivételesen hasznos tulajdonság lehet.

¹ Internet Protocol

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 kutató-mentő repülések kikerülésére. A veszélyes helyzetek elkerülésén túl a már bajba került pilóta nélküli légi járművek 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 biztosítani kell az adatok sértetlenségét, rendelkezésre állását és hitelességét, esetenként bizalmasságát is, miközben figyelembe veszik a rádiós frekvenciakiosztásra és sáv szélességre, a választott spektrum megengedett telítettségére vonatkozó szabályozásokat.

Különbséget kell tenni felhasználást illetően a védelmi, kereskedelmi és hobbi célú pilóta nélküli légi jármű-rendszerek (UAS²)

² Unmanned Aircraft System

képességei és az elvárt biztonsági szintek között, ennek megfelelően az őket kiszolgáló felhő alapú rendszerrel szemben támasztott követelményeket 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 légi jármű irányításáért felelnek, vagy az európai irányelvek által meghatározott személyes adatokat tartalmaznak. Más adatok viszont közérdeklűek, például a polgári légi jármű pozíciója és azonosítója, vagy egyéb tulajdonságai melyek nyílt csatornán is szórhatók a fedélzeti ütközésselkerülés 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 légi jármű-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 kikapuk elhelyezésével a termékeikben, nem is beszélve a számtalan, napvilágot látott lehallgatási bot-

rányról. 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 légi járművek (UAV³) és a felhő alapú rendszerek jelenlegi lehetőségeit;
- **Elemezem** az elérhető szabványokat és ajánlásokat, valamint jogszabályokat;
- Biztonsági szempontból **megvizsgálom** a pilóta nélküli légi járművek 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 légi jármű-rendszerek tesztelése eredményesen kivitelezhető két irányból: a járművek, illetve az irányítás rendszerrel való helyettesítésével.

³ Unmanned Aerial Vehicle

- 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 működtetését, 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 légi jármű-rendszerek elektronikus biztonsági szempontból megfelelő működtetését.

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.
- 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 vonatkozó következtetések levezetése.

Az elvégzett vizsgálatok összefoglaló leírása és összegzett következtetései

Az értekezés **1. fejezetében** bemutatom a pilóta nélküli légi járműrendszerek különböző aspektusait, történetét, képességeit, felhasználási lehetőségeit. Hasonló szempontok alapján bemutatom a felhő alapú számítástechnika területét és biztonsági, illetve személyes adatokat érintő kérdéseit, illetve a nyilvános kulcsú infrastruktúra (PKI⁴) alapjait is, melyekre a későbbi fejezetek épülnek.

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 a dolgok internete (IoT⁵) rendszerek felépítésével.

⁴ Public Key Infrastructure

⁵ Internet of Things

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 rendszer tervezése során a nyílt forrású és szabad szoftverek alkalmazására törekedtem, a sikeres implementáció rámutatott, hogy a szabályozói feltételek és technikai lehetőségek szabják meg leginkább a hasonló rendszerek tesztelésének korlátait – a szükséges infrastruktúra kialakítása kivitelezhető költséghatékonyan, javarészt ingyenes szoftverrendszer alkalmazásával.

A **4. fejezetben** a végrehajtott repülési teszteseteket mutatom be, melyek rámutattak a rendszer egyes hiányosságaira (pl. az elavult firmware által nem támogatott automatikus fel- és leszállás, koordináta-rendszerek 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.

A kapcsolódó laboratóriumi tesztesetek során 100 drónt szimulálok szoftveresen, miközben demonstrálok 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.

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

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

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

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

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 Unió előírások elektronikus azonosításra vonatkozó követelményeinek. 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.

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

Bemutatom az OpenDroneID rendszer működését és felépítését is, annak korlátait és lehetőségeit. 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, lejáratása, konfigurációja stb.).

Matematikai számításokkal levezetve bemutatom a MAVLink 2.0 aláírás mezőjének egy lehetséges valószínűségszámítás alapú támadását. A protokoll aláírás mezőjét megvizsgálva elmondható, hogy az aláírás mező önmagában nem teszi teljes mértékben ellenállóvá a protokollt eltérítési kísérletekkel szemben, azonban hagyományos, alacsony sávzélességű rádiós adatcsatornák esetén hozzájárul a csomagok sértetlenségének biztosításához.

Végül a robotpilóta irányába a földi irányító állomás szimulálásával végzett laboratóriumi teszteseteket mutatok be. Ezek kimenetele alapján úgy ítélem meg, hogy a választott robotpilóta-rendszer robusztussága elektronikus biztonsági szempontból ténylegesen megfelel a kísérleti repülési tesztek lefolytatásához elvárható szintnek.

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 fedti le a definiált feladatkört.
2. Saját felhő alapú pilóta nélküli légi jármű-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 légi járművek PKI és OpenDroneID alapú, európai uniós irányelveknek megfelelő azonosítására és regisztrációjára, mely folyamatainak példáin keresztül **levezettem**, hogy a modell alkalmazása hozzájárulna a pilóta nélküli légi jármű-rendszereket érintő személyi és adminisztratív folyamatok biztonságos kialakításához.

4. **Megállapítottam**, hogy pilóta nélküli légi jármű-rendszer forgalmi menedzsment (UTM⁶) 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 mesterképzéseiben.
- A felvázolt rendszer általánosítható felhő helyett szoftverkonténer technológián alapuló rendszerek megterve-

⁶ Unmanned Traffic Management

zéséhez 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.

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 légi jármű rendszerek szakirodalmának kutatása, *Hadmérnök XII.*: (1. különszám) pp. 217-233.
- S3** Vránics Dávid Ferenc: Egy felhőalapú, pilóta nélküli légi jármű-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

Doktorjelölt szakmai-tudományos életrajza

Személyi adatok:

Név: Vránics Dávid Ferenc
Születési idő: 1990. július 11.
E-mail cím: vranicsd@gmail.com



Munkahely/beosztások:

- 2020- **Kutató-fejlesztő munkatárs – Mould Tech Systems Kft, MyDroneMet**
- 2011- **Szoftverfejlesztő – Ericsson Magyarország Kft, Titan-Sim, Cloud Execution Environment**
- 2016-2021 **Informatikai szakértő – Nemzeti Közzolgálati Egyetem, GINOP 2.3.2-15-2016-00007 „A légiközlekedés-biztonsághoz kapcsolódó interdiszciplináris tudományos potenciál növelése és integrálása a nemzetközi kutatás-fejlesztési hálózatba a Nemzeti Közzolgálati Egyetemen - VOLARE”**

Tanulmányok:

- 2016-2018 **Nemzeti Közzolgálati Egyetem, Hadtudományi és Honvédtisztképző Kar, Katonai Műszaki Doktori Iskola**
- 2013-2015 **Nemzeti Közzolgálati Egyetem, Hadtudományi és Honvédtisztképző Kar, védelmi vezetéstechnikai rendszertervező MSc szak**
- 2008-2012 **Eötvös Loránd Tudományegyetem, Informatikai Kar, programtervező informatikus BSc szak**

Tagságok:

- 2019- Drónpilóták Országos Egyesülete
- 2019- International Society for Atmospheric Research using Remotely piloted Aircraft

Szakmai tanfolyamok:

ISTQB:

Advanced Level Test Analyst

Advanced Level Specialist - Security Tester

EC-Council:

Certified Ethical Hacker v10

Nyelvismeret:

Angol C1, olasz B1

Egyéb:

B kategóriás személygépkocsi jogosítvány

A1/A3 Open kategóriás drón távpilóta vizsga