



ÓBUDAI EGYETEM
ÓBUDA UNIVERSITY

DOKTORI (PHD) ÉRTEKEZÉS
TÉZISFÜZETE

BORSOS DÖNÍZ

IoT technológiák
alkalmazásának lehetőségei a
személy- és vagyonvédelem
területén

Témavezető: Prof. Em. Dr. Berek Lajos

BIZTONSÁGTUDOMÁNYI
DOKTORI ISKOLA

Budapest, 2026. május 12.

Tartalomjegyzék

1	Summary	3
2	A kutatás előzményei	4
3	Célkitűzések	6
4	Vizsgálati módszerek	8
5	Új tudományos eredmények.....	10
6	Az eredmények hasznosítási lehetősége	12
7	Irodalmi hivatkozások listája/ Irodalomjegyzék	14
8	A tézispontokhoz kapcsolódó tudományos közlemények	29
9	További tudományos közlemények (opcionális)	31

1 Summary

The dissertation and research focused on the applicability of IoT-based solutions, particularly LoRaWAN, in personal and property security systems. The relevance of this topic is demonstrated by the rapid development and widespread adoption of IoT technologies, as well as the growing use of security systems based on IoT sensor networks and wireless communication solutions. IoT-based systems offer numerous advantages, such as large-scale facility monitoring, remote monitoring solutions, and automated operation; however, their operational characteristics and limitations raise new research questions regarding security.

I began my research by reviewing international and domestic literature on the topic, which was present throughout the process, with a particular focus on the operational characteristics of IoT and LPWAN and their known application limitations. In the second step, I conducted large-scale empirical studies twice among certified LoRaWAN end-nodes. As a result of the analysis, I identified the patterns that influence the applicability of technology and developed a functional classification of LoRaWAN end-nodes. During my research, I developed a conceptual framework for an IoT-based security system and a multidimensional model of the security reliability of IoT nodes. The reliability model and the risk classification derived from it can be used to evaluate and compare the applicability of end-nodes. I validated the model's practical validity and the relationships between dimensions through measurements and experiments. An important result of the final part of my research was the general IoT lifecycle closure model developed from the examination of IoT nodes lifecycle management, as well as the decommissioning procedure adapted for LoRaWAN end-nodes.

The dissertation presents the results of my research in a logical structure: first, it describes the theoretical and technological foundations (Chapter 1), followed by an empirical examination of certified LoRaWAN end-nodes (Chapter 2). This is followed by a presentation of the conceptual and modeling framework developed during the research (Chapter 3), and then the „practical validity of the model based on measurement and experimental results (Chapter 4). The final chapter of the dissertation discusses lifecycle management issues for IoT endpoints and describes the developed exit-procedure model (Chapter 5).

2 A kutatás előzményei

Az elmúlt évtizedben a dolgok internete alapú (Internet of Things, továbbiakban: IoT) megoldások rohamos fejlődése [1][2][3] számottevően átalakította a műszaki infrastruktúrák működését [4] és a különböző szolgáltatások technológiai hátterét [5], beleértve a biztonságtechnikai megoldásokat is. A megjelent új rendszerarchitektúrák lehetővé tették a fizikai környezet állandó monitorozását, az érzékelőinformációk valós idejű továbbítását, valamint a folyamatos távfelügyeletet és a teljesen automatizált működést. [6] A nagy kiterjedésű hálózatok megvalósítását szolgáló technológiák új dimenziót nyitottak meg [7] a vezeték nélküli infrastruktúrák kialakításában és a vezetékes megoldások kiváltásában.

Ez a fejlődési irány a személy- és vagyonvédelemben is jelentős változásokat hozott. A különböző detektáló- és jelzőrendszerek, valamint a távfelügyeleti rendszerek egyre gyakrabban támaszkodnak valamilyen IoT-kommunikációra. [8] Alkalmazásuk előnyös lehet kiterjedt objektumok és elszigetelt területek felügyeletekor [9] vagy utólagos telepítés esetén. Ezzel párhuzamosan, ahogy bővültek a technológiai lehetőségek, új típusú kérdések és kockázatok [10] jelentek meg.

A korábbi, jellemzően zárt, dedikált kommunikációra épülő személy- és vagyonvédelmi rendszerek helyére egyre több, nyílt szabványra épülő, vezeték nélküli infrastruktúra kerül. A rugalmasságot és az egyszerű integrálhatóságot biztosító megoldások a rendszerek komplexitásnövekedésével járnak és a kockázati tényezők számát is növelik. Ez azt eredményezi, hogy az új rendszerek a korábbinál átfogóbb megközelítéseket igényelnek. Személy- és vagyonvédelmi rendszerekben az adatátvitel nem egyszerűen statisztikai célú, mint például egy fogyasztásmérés esetén, hanem közvetlenül hatással van a rendszerszintű kiértékelésre és döntéshozatalra [11], például egy behatolásdetektálás esetén.

Közel tíz éve foglalkozom IoT-alapú kommunikációs rendszerek tervezésével, fejlesztésével és elemzésével, ezen belül kiemelten a LoRaWAN technológiával, de munkásságom kiterjed az ipari kommunikációs megoldásokra, az Ipar 4.0 koncepcióhoz kapcsolódó infrastruktúrákra, kritikus infrastruktúrák vizsgálatára és az okos város koncepció kapcsolataira. A korábbi kutatási és fejlesztési tevékenységeim tapasztalatai rámutattak arra, hogy a kommunikációs működőképesség, a specifikációs megfelelés és a rendszer tényleges megbízhatósága nem minden esetben esik egybe.

Tudományos probléma megfogalmazása

Az IoT-alapú rendszerek nem csak ipari területen vagy a mindennapi élet részeként jelentek meg, hanem a személy- és vagyonvédelem területén is meghatározó számban jelen vannak. Ezek, a főleg érzékelőalapú megoldások lehetővé teszik a decentralizált adatgyűjtést és a nagy kiterjedésű objektumok rugalmas felügyeletét. Az eltérő alacsony energiafogyasztású, nagy kiterjedésű hálózati (Low Power Wide Area Network, továbbiakban: LPWAN) technológiák, műszaki szempontból alkalmasak kis adatok, állapot vagy riasztási funkciók továbbítására, így megjelentek személy- és vagyonvédelmi rendszerekben is.

Az IoT elterjedése azonban megelőzte annak biztonságtechnikai tudományi aspektusú rendszerszintű vizsgálatát. Tehát az igény megjelent, amit a piac ki is szolgáltat, de a szakirodalom jelentős része kommunikációs paraméterekre, energiafogyasztás optimalizálására, protokollszerű leírásokra és vizsgálatokra, valamint hálózati felépítésre, esetlegesen információbiztonsági kérdésekre összpontosít. Ezzel szemben, elmarad az IoT végpontok megbízhatósági és kockázati elemzése személy- és vagyonvédelmi alkalmazások kontextusában. Nem vizsgált az IoT sajátosságokból adódó korlátok tényleges védelmi érintettsége és hatása.

A tudományos probléma másik vetülete az IoT végpontok életciklusának teljeskörű kezelése. Az elérhető tudományos publikációk és műszaki dokumentációk jellemzően a telepítésre és üzemeltetésre koncentrálnak, eközben az eszközök életciklus-lezárásának fizikai és logikai kezelése nem jelenik meg egységesített, kidolgozott formában. A szakirodalomban találhatók utalások a kivonási eljárás fontosságára, mint kockázattal járó hiányosságra, de ezek megmaradnak az említés szintjén, és nem épülnek be átfogó modellbe vagy értelmezési keretbe.

A tudományos probléma tehát úgy foglалható össze, hogy hiányzik egy olyan átfogó fogalmi és empirikusan megalapozott keretrendszer, amely az IoT-alapú (különösen LoRaWAN-kommunikációra épülő) személy- és vagyonvédelmi rendszerek, végberendezések megbízhatóságát nem csak kommunikációtechnikai, de biztonságtechnikai szempontból is értelmezi, figyelembe véve a teljes életciklus-menedzsmentet, beleértve annak lezárási szakaszát is. Mindezek hiányában az IoT alkalmazhatóságának értékelése személy- és vagyonvédelem szempontjából hiányos, és nem tükrözi a rendszerállapot és a kockázati vonulat teljes összefüggésrendszerét.

3 Célkitűzések

Az értekezés összetett célja a LoRaWAN-alapú IoT kommunikációs megoldások személy- és vagyonvédelmi alkalmazhatóságának rendszerszintű vizsgálata, a technológiai sajátosságok, a működési megbízhatóság és a biztonságtechnikai értelmezés összefüggéseinek aspektusában. A kutatás célja továbbá egy olyan mérésekkel alátámasztott keretrendszer kialakítása, amely megalapozza a LoRaWAN-alapú védelmi rendszerek alkalmazhatóságának, kockázatainak és életciklus-kezelésének tudományos igényű értékelését.

Ennek megfelelően a kutatás részletes célkitűzései az alábbiak:

- Áttekinteni a hazai- és nemzetközi szakirodalmat az IoT-alapú, személy- és vagyonvédelmi alkalmazásokhoz kapcsolódó kommunikációs technológiák vonatkozásában.
- Elemezni az IoT rendszerek sajátosságait rendszerszinten, különös tekintettel az érzékelőalapú, eseményvezérelt kommunikáció dominanciájára.
- Összehasonlító módon elemezni az LPWAN megoldásait, hangsúlyt helyezve a LoRaWAN, valamint a hasonló célú Sigfox és NB-IoT kommunikációkra.
- Megvizsgálni és azonosítani a LoRaWAN technológia korlátait, specifikációs hiányosságait és működési sajátosságait, kiemelt figyelemmel azok személy- és vagyonvédelmi jelentőségére.
- Behatárolni és értékelni a személy- és vagyonvédelmi alkalmazási területek releváns alrészeit, valamint meghatározni, hogy mely funkcionális környezetben tekinthető a LoRaWAN technológia reális alternatívának.
- Feltárni azokat a szakirodalmi és műszaki értelmezési hiányosságokat, amelyek indokolttá teszik a LoRaWAN technológia biztonságtechnikatudományi szemléletű vizsgálatát.
- Megvizsgálni és elemezni a tanúsított LoRaWAN végberendezések funkcionális felépítését, alkalmazási területeit, működési osztályait, specifikációs besorolását és frekvenciasáv-használatát, valamint összehasonlító elemzéssel értékelni két eltérő időpontban végzett nagymintás felmérés eredményeit a megjelenő mintázatok azonosításának érdekében.
- Kidolgozni és továbbfejleszteni egy funkcionális taxonómiát a tanúsított eszközök csoportosítására, a releváns kategóriák kijelölésével.

- Értékelni, hogy a tanúsítás megléte önmagában mennyiben tekinthető elegendőnek biztonságtechnikai alkalmassági feltételként.
- Kidolgozni és meghatározni az IoT-alapú elektronikai védelmi eszközök fogalmi- és modellkeretét, valamint elhatárolni a kommunikációs infrastruktúra-szintű és a biztonságtechnikai megbízhatósági értelmezését.
- Azonosítani és többdimenziós modellbe rendezni a megbízhatóságot befolyásoló tényezőket, valamint formalizálni azok értelmezési keretét.
- Kidolgozni egy kockázati osztályozási keretet, amely lehetővé teszi az IoT végpontok és rendszerek funkcionális összehasonlítását.
- Mérésekkel és kísérletekkel igazolni a többdimenziós megbízhatósági modell gyakorlati alkalmazhatóságát, valamint feltárni és értékelni a megbízhatósági dimenziók közötti kapcsolatokat.
- Igazolni, hogy a végpontok életciklus-állapota mérhető módon befolyásolja a rendszer megbízhatóságát és rejtett védelmi kockázatot eredményezhet.
- Rendszerszinten értelmezni az eszköz-életciklus szakaszait, különös tekintettel az életciklus lezárására.
- Kidolgozni és elvi megoldásként javasolni egy olyan életciklus-modellt és keretrendszert, amely biztosítja a következetes, ellenőrizhető és reprodukálható fizikai és logikai lezárást.

4 Vizsgálati módszerek

Az értekezés kutatási módszertana többretegű és integrált megközelítést alkalmaz, ötvözve az empirikus, logikai és (bizonyos mértékig) a matematikai módszereket. [12] Egyaránt alkalmaztam kvantitatív és kvalitatív elemeket is az elméletorientált és a gyakorlati alapú célok megvalósításához. A kutatási téma több ismeretterületet is érint, a biztonságtechnika mellett más tudományterületek vizsgálata is megjelenik. Ezért, a kutatási módszerek megválasztásánál kiemelt szempont volt a rendszerszemléletű, a szükséges mértékű teljességre törekvő megközelítés. Cél volt, hogy ne csak elméleti feldolgozás jelenjen meg az értekezésben, hanem empirikus eredményekkel alátámasztható, validálható következtetések is. Az értekezés a szakirodalmi és dokumentációs háttér feldolgozásából indul ki, de támaszkodik saját adatfeldolgozásra, mérésekre és ezek statisztikai értékelésére is.

A kutatómunka megalapozásához irodalmi feldolgozást végeztem, ahol első lépésben a tématerület feltérképezése és az alapinformációk rendszerezése jelent meg célként. Kezdeti lépés volt az IoT, LoRaWAN technológia és a személy- és vagyonvédelmi alkalmazási környezetek kapcsolódó tématerületeinek összegzése és rendszerezése. Rendszereztem az IoT-hoz kapcsolódó alapfogalmakat, architekturális elemeket és működési mechanizmusokat. Emellett, behatároltam az LPWAN személy- és vagyonvédelem területén való alkalmazásának releváns részterületeit. Ezekhez elérhető hazai és nemzetközi publikációkat, tanulmányokat, valamint specifikációkat, technikai dokumentációkat, ajánlásokat, szabványokat dolgoztam fel. A fogalmak, mechanizmusok és korlátok megismeréséhez analízist alkalmaztam. A technológiai részleteket összehasonlítóval vizsgáltam. Az elemek rendszerszintű értelmezése szintézis alapú volt. Az irodalmi feldolgozás célja a kutatási részek azonosítása, az ismeretanyag összefoglalása, valamint az értekezés 2-5. fejezeteinek előkészítése volt.

A kutatás empirikus kiindulópontját a tanúsított LoRaWAN eszközök nagy elemszámú strukturált feldolgozása jelentette, ahol kvantitatív módszerekkel elemeztem többek között a végberendezések funkcionális dominanciáját, specifikációkövetési heterogenitást, működési osztályok arányát, életciklus-menedzsment megjelenését és kapcsolatot a személy- és vagyonvédelemmel. A módszer célja olyan mintázatok kimutatása volt, amelyek megalapozzák a 3. fejezet fogalmi és dimenzionális modelljét, valamint előkészítik a 4. fejezet validációra vonatkozó méréseit.

Az 1. fejezetben azonosított irodalmi hiányosságokra és a 2. fejezet empirikus vizsgálatának eredményeire építve logikai módszerek alkalmazásával kidolgoztam az IoT végpontok

biztonságtechnikai aspektusban értelmezhető megbízhatóságát és többdimenziós modelljét. Elválasztottam a kommunikációs működőképességet a személy- és vagyonvédelemben értelmezhető megbízhatóságtól, dimenziómodellt és fogalmakat definiáltam, ezekből mérhető következményeket vezettem le és egységes keretrendszerbe illesztést valósítottam meg.

Az elméleti eredmények (fogalmak, dimenziók, keretrendszer) ellenőrzésére mérés és kísérlet alapú validációt végeztem. Vizsgáltam a paramétermanipuláció hatását és azok kompromisszumos jellegét. Méréseket végeztem a környezeti változók és a dimenziók értelmezésére. A mérési és kísérleti eredmények feldolgozásával és statisztikai értékelésével kölcsönhatásokat azonosítottam, kimutattam a dimenziók közötti összefüggéseket.

A kutatás záró szakaszában a végpontok életciklus-menedzsmentjét és életciklusának lezárását, illetve a LoRaWAN specifikációkban nem formalizált kivonási problémát vizsgáltam, amely specifikáció- és követelményelemzésre, logikai állapotmodellezésre, valamint eljárás- és követelményrendszer kidolgozására épült.

5 Új tudományos eredmények

Értekezésem elkészítése során négy összetett hipotézist vizsgáltam, melyekkel kapcsolatosan az alábbi megállapításokat teszem. Az értekezés tézisei:

Tézis 1. [BD7] [BD8] [BD9]

Empirikus vizsgálatok alapján elvégeztem a tanúsított LoRaWAN végberendezések strukturált elemzését és kialakítottam azok funkcionális tipológiáját. Igazoltam, hogy a tanúsított eszközállomány visszatérő mintázatokat mutat – különösen a detektálási/jelzési funkcionális dominancia, az eseményvezérelt kommunikáció korlátozó jellege, a specifikációs és működési heterogenitás, valamint a termékportfólió fluktuációjából adódó életciklus-instabilitás tekintetében –, amelyek rendszerszinten meghatározzák a személy- és vagyonvédelmi alkalmazhatóság korlátait.

Tézis 2. [BD1] [BD2] [BD3] [BD4] [BD5] [BD6] [BD7] [BD8] [BD9] [BD10] [BD11] [BD12] [BD13] [BD14]

Megalkottam az IoT-alapú elektronikai védelmi rendszer többretegű értelmezési keretét, továbbá kidolgoztam az IoT-végpontok biztonságtechnikai megbízhatóságának 4+1 dimenziós (F, T, C, L, S) modelljét, amely a megbízhatóságot a védelmi cél teljesítésére való alkalmasságként értelmezi és azt 0-1 tartományú indexként határoztam meg. A modell alapján kialakítottam a funkcionális végpont-kockázati osztályokat (K1-K4), amelyek lehetővé teszik a heterogén IoT-végpontok összehasonlítását személy- és vagyonvédelmi környezetben.

Tézis 3. [BD1] [BD3] [BD5] [BD10] [BD13] [BD14] [BD15] [BD16]

Mérésekkel és kísérletekkel igazoltam, hogy a többdimenziós megbízhatósági modell dimenziói mérhető hatást gyakorolnak a LoRaWAN-alapú IoT-végpontok személy- és vagyonvédelmi szempontból releváns működésére, valamint hogy azonosíthatók a dimenziók közötti kölcsönhatások. Bizonyítottam, hogy a kontextuális és életciklus-tényezők nemlineáris módon befolyásolják a végpontok működési stabilitását, továbbá azt, hogy a funkcionális dimenzió paraméterezésének optimalizálása bizonyos mértékű kompenzációt tesz lehetővé, ugyanakkor kompromisszumokkal jár.

Tézis 4. [BD4]

T4: Igazoltam, hogy az IoT-végpontok megfelelő életciklus-lezárásának hiányában a fizikai és logikai állapot inkonzisztenciája állhat fenn, amely befolyásolja az IoT-alapú személy- és vagyonvédelmi rendszerek megbízhatóságát, rejtett kockázatokat eredményez és torzítja a rendszerállapot értékelését. Ennek kezelésére kidolgoztam egy általános IoT-életciklus lezárási modellt, valamint ezt adaptáltam LoRaWAN IoT-végpontok kivonására is.

6 Az eredmények hasznosítási lehetősége

Az értekezésben ismertetett kutatási eredményeket gyakorlati szempontból elsősorban az IoT-alapú személy- és vagyonvédelmi rendszerek tervezésében, értékelésében és üzemeltetésében lehet hasznosítani. A vizsgált eszközök, a kidolgozott fogalmi keretek, modellek, osztályozások és eljárások lehetőséget biztosítanak arra, hogy az IoT-végpontok alkalmazhatósága ne kizárólag kommunikációs vagy technológiai paraméterek alapján kerüljön megítélésre, hanem figyelembe vegye a működési körülményeket, a funkcionális sajátosságokat, valamint az eszközök életciklus-állapotát is. Ez a fajta új megközelítés hozzájárulhat a tervezési döntések megalapozásához, valamint a különböző IoT-megoldások biztonságtechnikai szempontú értékeléséhez és összehasonlításához.

A kutatási eredményeim ezek mellett módszertani támogatást biztosítanak a személy- és vagyonvédelmi rendszerek fejlesztésével és üzemeltetésével foglalkozó szakemberek részére is. Az ismertetett modell és a hozzá kapcsolódó kockázati osztályok alkalmazhatók lehetnek IoT-alapú rendszerek értékelése, auditálása, kockázatelemzése, tervezési folyamatai és üzemeltetése során. Az IoT-végpontok életciklus-lezárására vonatkozó megállapítások és a LoRaWAN végpontokra kidolgozott kivonási eljárás pedig hozzájárulhat az ilyen rendszerek hosszú távú megbízhatóságának fenntartásához, valamint a rejtett kockázatok csökkentéséhez, kezeléséhez.

Az értekezés eredményei az alábbi területek szakmai szereplői számára hasznosíthatók a leginkább:

- Biztonságtechnikai rendszerek tervezői és integrátorai számára a megfelelő megoldások kiválasztásához.
- Biztonságtechnikai szolgáltatók és üzemeltetők részére rendszerértékelésre és a kockázatok azonosítására.
- IoT-eszközök és rendszerek fejlesztőinek a megfelelő módszerek implementálásához.
- Auditorok és kockázatelemzéssel foglalkozó szakemberek számára a strukturált rendszerértékeléshez.
- Kritikus infrastruktúrák, ipari IoT és Ipar 4.0 területén dolgozó mérnök és kiberbiztonsági szakemberek számára a rendszerek és megoldások értékeléséhez.
- Szakmai és szabályozási szerveknek irányelvek és ajánlások kidolgozásához.
- Kutatók, oktatók részére további elemzésekhez és tudományos vizsgálatokhoz.

A kutatási eredmények hozzájárulhatnak az IoT-alapú személy- és vagyonvédelmi rendszerek tudatosabb tervezéséhez, értékeléséhez és üzemeltetéséhez, valamint alapot nyújthatnak a technológia alkalmazásainak további fejlesztéséhez.

Az értekezés eredményei alapján több új kutatási irányt is ki lehet emelni. Az értekezés logikai ívéhez szorosan kapcsolódva, a modellek és a vizsgálatok kiterjeszthetők más hálózati architektúrájú rendszerekre. Ezek az új irányok [132] további mélységet eredményeznek és hozzájárulnak az értelmezések további finomításához.

Az alkalmazási terület kiterjesztésének egyik ilyen lehetősége az IoT-alapú kommunikációs rendszerek alkalmazásának és szerepének vizsgálata komplex rendszerekben, kifejezetten okos városok (Smart City) infrastruktúráiban az alrendszerek közötti adattovábbítás tekintetében. A másik lehetséges irány a kritikus infrastruktúrák védelmét támogató és megvalósító IoT megoldások elemzése.

Eltérő, bár nagyon aktuális terület a mesterséges intelligencia és a gépi tanulási módszerek integrálása a rendszerek működésének vizsgálatához. A nagymennyiségű kommunikációra és működésre vonatkozó adatok felhasználhatók olyan modellek kialakítására, mely alkalmas prediktív becslésre, anomáliák korai felismerésére, valamint valós idejű állapotértékelésre.

7 Irodalmi hivatkozások listája/ Irodalomjegyzék

- [1] M. A. Razzaque, M. Milojevic-Jevric, A. Palade, és S. Clarke, „Middleware for Internet of Things: A Survey”, *IEEE Internet Things J.*, köt. 3, sz. 1, o. 70–95, febr. 2016, doi: 10.1109/JIOT.2015.2498900.
- [2] N. Srivastava és P. Pandey, „Internet of things (IoT): Applications, trends, issues and challenges”, *Mater. Today Proc.*, köt. 69, o. 587–591, 2022, doi: 10.1016/j.matpr.2022.09.490.
- [3] H. Park és S. Park, „Emerging Trends and Challenges in IoT Networks”, *Electronics (Basel)*, köt. 13, sz. 3, o. 513, jan. 2024, doi: 10.3390/electronics13030513.
- [4] K. M. Hou, X. Diao, H. Shi, H. Ding, H. Zhou, és C. de Vault, „Trends and Challenges in AIoT/IIoT/IoT Implementation”, *Sensors*, köt. 23, sz. 11, o. 5074, máj. 2023, doi: 10.3390/s23115074.
- [5] L. L. Knud, „IoT 2019 in Review: The 10 Most Relevant IoT Developments of the Year”, IoT Analytics. Elérés: 2024. február 4. [Online]. Elérhető: <https://iot-analytics.com/iot-2019-in-review/>
- [6] I. Cvitić, D. Peraković, M. Periša, A. Jevremović, és A. Shalaginov, „An Overview of Smart Home IoT Trends and related Cybersecurity Challenges”, *Mobile Networks and Applications*, köt. 28, sz. 4, o. 1334–1348, aug. 2023, doi: 10.1007/s11036-022-02055-w.
- [7] M. Centenaro, L. Vangelista, A. Zanella, és M. Zorzi, „Long-range communications in unlicensed bands: the rising stars in the IoT and smart city scenarios”, *IEEE Wirel. Commun.*, köt. 23, sz. 5, o. 60–67, okt. 2016, doi: 10.1109/MWC.2016.7721743.
- [8] N. S. Sayem és mtsai., „IoT-based smart protection system to address agro-farm security challenges in Bangladesh”, *Smart Agricultural Technology*, köt. 6, o. 100358, dec. 2023, doi: 10.1016/j.atech.2023.100358.
- [9] D. Borsos, „A LoRaWAN-technológia szerepe az elektronikai védelem területén, az építőipari beruházások vonatkozásában”, *Hadmérnök*, köt. 16, sz. 3, o. 5–16, nov. 2021, doi: 10.32567/hm.2021.3.1.

- [10] F. Bálint és R. Pető, „Sustainable and Safe Cities through Computer Applications”, *Interdisciplinary Description of Complex Systems*, köt. 23, sz. 3, o. 207–216, 2025, doi: 10.7906/indecs.23.3.2.
- [11] A. Karkouch, H. Mousannif, H. Al Moatassime, és T. Noel, „Data quality in internet of things: A state-of-the-art survey”, *Journal of Network and Computer Applications*, köt. 73, o. 57–81, szept. 2016, doi: 10.1016/j.jnca.2016.08.002.
- [12] L. Berek, L. Berek, és Z. Rajnai, „A tudományos kutatás folyamata és módszerei”, Budapest, Magyarország: Óbudai Egyetem, Bánki Donát Gépész és Biztonságtechnikai Mérnöki Kar, 2018, o. 1–147. Elérés: 2025. december 6. [Online]. Elérhető: https://oda.uni-obuda.hu/bitstream/handle/20.500.14044/25308/Berek_Berek_Rajnai_Tudkut_2022.pdf?sequence=1&isAllowed=y
- [13] L. L. Knud, „Top 10 IoT applications in 2020”, IoT Analytics. Elérés: 2024. május 4. [Online]. Elérhető: <https://iot-analytics.com/top-10-iot-applications-in-2020/>
- [14] M. Asemani, F. Abdollahei, és F. Jabbari, „Understanding IoT Platforms : Towards a comprehensive definition and main characteristic description”, in *2019 5th International Conference on Web Research (ICWR)*, IEEE, ápr. 2019, o. 172–177. doi: 10.1109/ICWR.2019.8765259.
- [15] B. Dorsemayne, J.-P. Gaulier, J.-P. Wary, N. Kheir, és P. Urien, „Internet of Things: A Definition & Taxonomy”, in *2015 9th International Conference on Next Generation Mobile Applications, Services and Technologies*, IEEE, szept. 2015, o. 72–77. doi: 10.1109/NGMAST.2015.71.
- [16] L. Atzori, A. Iera, és G. Morabito, „Understanding the Internet of Things: definition, potentials, and societal role of a fast evolving paradigm”, *Ad Hoc Networks*, köt. 56, o. 122–140, márc. 2017, doi: 10.1016/j.adhoc.2016.12.004.
- [17] K. Sorri, N. Mustafee, és M. Seppänen, „Revisiting IoT definitions: A framework towards comprehensive use”, *Technol. Forecast. Soc. Change*, köt. 179, o. 121623, jún. 2022, doi: 10.1016/j.techfore.2022.121623.
- [18] R. Minerva, A. Biru, és D. Rotondi, „Towards a definition of the Internet of Things (IoT)”, IEEE Internet Initiative, Telecom Italia S.p.A., 2014, o. 1–86. Elérés: 2025. március 4. [Online]. Elérhető:

https://iot.ieee.org/images/files/pdf/IEEE_IoT_Towards_Definition_Internet_of_Things_Revision1_27MAY15.pdf

- [19] L. Da Xu, W. He, és S. Li, „Internet of Things in Industries: A Survey”, *IEEE Trans. Industr. Inform.*, köt. 10, sz. 4, o. 2233–2243, nov. 2014, doi: 10.1109/TII.2014.2300753.
- [20] D. Borsos, „Bevezetés a személy- és vagyonvédelem területén alkalmazható IoT technológiákba – LoRaWAN technológia”, in *XXXV. Jubileumi Kandó Konferencia 2019*, Temesvári Zsolt, Szerk., Budapest, Hungary: Óbudai Egyetem, Kandó Kálmán Villamosmérnöki Kar, 2020, o. 94–102.
- [21] L. L. Knud, „State of the IoT 2020: 12 billion IoT connections, surpassing non-IoT for the first time”, IoT Analytics. Elérés: 2024. március 1. [Online]. Elérhető: <https://iot-analytics.com/state-of-the-iot-2020-12-billion-iot-connections-surpassing-non-iot-for-the-first-time/>
- [22] P. J. Basford, F. M. J. Bulot, M. Apetroaie-Cristea, S. J. Cox, és S. J. Ossont, „LoRaWAN for Smart City IoT Deployments: A Long Term Evaluation”, *Sensors*, köt. 20, sz. 3, o. 648, jan. 2020, doi: 10.3390/s20030648.
- [23] S. Satyajit, „State of IoT 2025: Number of connected IoT devices growing 14% to 21.1 billion globally”, IoT Analytics. Elérés: 2025. december 4. [Online]. Elérhető: <https://iot-analytics.com/number-connected-iot-devices/>
- [24] „Internet Of Things Market Size & Share Analysis - Growth Trends And Forecast (2025 - 2030)”, Mordor Intelligence. Elérés: 2025. november 5. [Online]. Elérhető: <https://www.mordorintelligence.com/industry-reports/internet-of-things-iot-market>
- [25] ISO/IEC 21823:2019, *Internet of things (IoT) — Interoperability for IoT systems*. ISO, 2019.
- [26] ISO/IEC 27400:2022, *Cybersecurity — IoT security and privacy — Guidelines*. ISO, 2022.
- [27] ETSI EN 303 645, „CYBER; Cyber Security for Consumer Internet of Things: Baseline Requirements”, ETSI, 2024, o. 1–40. Elérés: 2024. július 6. [Online]. Elérhető: https://www.etsi.org/deliver/etsi_ts/103600_103699/103645/03.01.01_60/ts_103645v030101p.pdf
- [28] ISO/IEC 30141:2024, *Internet of Things (IoT) — Reference architecture*. ISO, 2024.

- [29] G. Breda, P. J. Varga, és Z. Illesi, „Forensic Functional Profile of IoT Devices-Based on Common Criteria”, in *2018 IEEE 16th International Symposium on Intelligent Systems and Informatics (SISY)*, IEEE, szept. 2018, o. 000261–000264. doi: 10.1109/SISY.2018.8524813.
- [30] B. Sándor, „Okos épületek kiberbiztonsági intézkedéseinek vizsgálata - DOKTORI (PHD) ÉRTEKEZÉS”, Budapest: Óbudai Egyetem, Biztonságtudományi Doktori Iskola, 2014, o. 1–113. Elérés: 2026. március 9. [Online]. Elérhető: <https://bdi.uni-obuda.hu/wp-content/uploads/2024/07/Doktori-PhD-ertekezes-Sandor-Barnabas.pdf>
- [31] J. A. López-Pastor, M. Poveda-García, A. Gil-Martínez, D. Cañete-Rebenaque, és J. L. Gómez-Tornero, „2-D Localization System for Mobile IoT Devices Using a Single Wi-Fi Access Point With a Passive Frequency-Scanned Antenna”, *IEEE Internet Things J.*, köt. 10, sz. 17, o. 14995–15011, szept. 2023, doi: 10.1109/JIOT.2023.3262830.
- [32] G. Koulouras, S. Katsoulis, és F. Zantalis, „Evolution of Bluetooth Technology: BLE in the IoT Ecosystem”, *Sensors*, köt. 25, sz. 4, o. 996, febr. 2025, doi: 10.3390/s25040996.
- [33] A. Zohourian és mtsai., „IoT Zigbee device security: A comprehensive review”, *Internet of Things*, köt. 22, o. 100791, júl. 2023, doi: 10.1016/j.iot.2023.100791.
- [34] G. Qiu, W. Tao, R.-C. Hwang, és C. Xie, „Wide-Area Visual Monitoring System Based on NB-IoT”, *Sensors*, köt. 25, sz. 21, o. 6589, okt. 2025, doi: 10.3390/s25216589.
- [35] N. H. Qasim, A. J. Salman, H. M. Salman, A. A. AbdelRahman, és A. Kondakova, „Evaluating NB-IoT within LTE Networks for Enhanced IoT Connectivity”, in *2024 35th Conference of Open Innovations Association (FRUCT)*, IEEE, ápr. 2024, o. 552–559. doi: 10.23919/FRUCT61870.2024.10516400.
- [36] H. A. K. M. Bahalul, M. Z. Md. Oahiduzzaman, és H. Md. Rifat, „5G and Internet of Things—Integration Trends, Opportunities, and Future Research Avenues”, in *5G and Beyond*, Springer, Singapore: Springer Tracts in Electrical and Electronics Engineering, 2023, o. 217–245. doi: 10.1007/978-981-99-3668-7_11.
- [37] A. Ilyin, A. Matinyan, A. Rolich, és L. Voskov, „Experimental Evaluation of Iridium Performance under Varying Weather Conditions and Elevation Angles”, in *2024 International Seminar on Electron Devices Design and Production (SED)*, IEEE, okt. 2024, o. 1–5. doi: 10.1109/SED63331.2024.10741060.

- [38] A. Andreadis, G. Giambene, és R. Zambon, „Latency Analysis for Satellite IoT in Remote Areas”, in *2025 IEEE 21st International Conference on Factory Communication Systems (WFCS)*, IEEE, jún. 2025, o. 1–8. doi: 10.1109/WFCS63373.2025.11077635.
- [39] G. Boquet, B. Martinez, F. Adelantado, J. Pages, J. A. Ruiz-de-Azua, és X. Vilajosana, „Low-Power Satellite Access Time Estimation for Internet of Things Services Over Nonterrestrial Networks”, *IEEE Internet Things J.*, köt. 11, sz. 2, o. 3206–3216, jan. 2024, doi: 10.1109/JIOT.2023.3298017.
- [40] A. Feijoo-Añazco, D. Garcia-Carrillo, J. Sanchez-Gomez, és R. Marin-Perez, „Innovative security and compression for constrained IoT networks”, *Internet of Things*, köt. 24, o. 100899, dec. 2023, doi: 10.1016/j.iot.2023.100899.
- [41] D. Orlovs, A. Rusins, V. Skrastiņš, és J. Judvaitis, „LPWAN Technologies for IoT: Real-World Deployment Performance and Practical Comparison”, *IoT*, köt. 6, sz. 4, o. 77, dec. 2025, doi: 10.3390/iot6040077.
- [42] P. Ruckebusch, S. Giannoulis, I. Moerman, J. Hoebeke, és E. De Poorter, „Modelling the energy consumption for over-the-air software updates in LPWAN networks: SigFox, LoRa and IEEE 802.15.4g”, *Internet of Things*, köt. 3–4, o. 104–119, okt. 2018, doi: 10.1016/j.iot.2018.09.010.
- [43] S. Satyajit, „Global LPWAN Market Tracker and Forecast 2015-2027 (Q1/2024 Update)”, IoT Analytics. Elérés: 2025. május 5. [Online]. Elérhető: <https://iot-analytics.com/product/global-lpwan-market-tracker-and-forecast-2015-2027-q1-2024-update/>
- [44] R. S. Sinha, Y. Wei, és S.-H. Hwang, „A survey on LPWA technology: LoRa and NB-IoT”, *ICT Express*, köt. 3, sz. 1, o. 14–21, márc. 2017, doi: 10.1016/j.icte.2017.03.004.
- [45] A. Lavric, A. I. Petrariu, és V. Popa, „Long Range SigFox Communication Protocol Scalability Analysis Under Large-Scale, High-Density Conditions”, *IEEE Access*, köt. 7, o. 35816–35825, 2019, doi: 10.1109/ACCESS.2019.2903157.
- [46] A. M. Abbas, K. Y. Youssef, I. I. Mahmoud, és A. Zekry, „NB-IoT optimization for smart meters networks of smart cities: Case study”, *Alexandria Engineering Journal*, köt. 59, sz. 6, o. 4267–4281, dec. 2020, doi: 10.1016/j.aej.2020.07.030.

- [47] B. Miles, E.-B. Bourennane, S. Boucherkha, és S. Chikhi, „A study of LoRaWAN protocol performance for IoT applications in smart agriculture”, *Comput. Commun.*, köt. 164, o. 148–157, dec. 2020, doi: 10.1016/j.comcom.2020.10.009.
- [48] K. Mekki, E. Bajic, F. Chaxel, és F. Meyer, „A comparative study of LPWAN technologies for large-scale IoT deployment”, *ICT Express*, köt. 5, sz. 1, o. 1–7, márc. 2019, doi: 10.1016/j.ict.2017.12.005.
- [49] LoRa Alliance, „LoRaWAN® Specification v1.0”, 2015, o. 1–91. Elérés: 2023. február 5. [Online]. Elérhető: https://lora-alliance.org/sites/default/files/2018-05/2015_-_lorawan_specification_1r0_611_1.pdf
- [50] H. Mroue és mtsai., „LoRa+: An extension of LoRaWAN protocol to reduce infrastructure costs by improving the Quality of Service”, *Internet of Things*, köt. 9, o. 100176, márc. 2020, doi: 10.1016/j.iot.2020.100176.
- [51] A. D. Zayas és P. Merino, „The 3GPP NB-IoT system architecture for the Internet of Things”, in *2017 IEEE International Conference on Communications Workshops (ICC Workshops)*, IEEE, máj. 2017, o. 277–282. doi: 10.1109/ICCW.2017.7962670.
- [52] LoRa Alliance, „About LoRa Alliance®”. Elérés: 2020. január 12. [Online]. Elérhető: <https://lora-alliance.org/about-lora-alliance/>
- [53] D. Hunt, „LoRa Alliance Certification”, *Journal of ICT Standardization*, köt. 9, sz. 1, o. 13–20, ápr. 2021, doi: 10.13052/jicts2245-800X.912.
- [54] LoRa Alliance, „LoRaWAN® Specification v1.0.1”, 2016, o. 1–82. Elérés: 2025. december 5. [Online]. Elérhető: <https://resources.lora-alliance.org/technical-specifications/lorawan-specification-v1-0-1>
- [55] LoRa Alliance, „LoRaWAN® Specification v1.0.2”, 2016, o. 1–70. Elérés: 2026. január 15. [Online]. Elérhető: <https://resources.lora-alliance.org/technical-specifications/lorawan-specification-v1-0-2>
- [56] LoRa Alliance, „LoRaWAN® Specification v1.0.3”, 2018, o. 1–72. Elérés: 2025. április 5. [Online]. Elérhető: <https://resources.lora-alliance.org/technical-specifications/lorawan-specification-v1-0-3>

- [57] LoRa Alliance, „TS001-1.0.4 LoRaWAN® L2 1.0.4 Specification”, 2020, o. 1–90. Elérés: 2026. január 4. [Online]. Elérhető: <https://resources.lora-alliance.org/technical-specifications/ts001-1-0-4-lorawan-l2-1-0-4-specification>
- [58] LoRa Alliance, „LoRaWAN® Specification v1.1”, 2017, o. 1–101. Elérés: 2024. augusztus 4. [Online]. Elérhető: <https://resources.lora-alliance.org/technical-specifications/lorawan-specification-v1-1>
- [59] I. Butun, N. Pereira, és M. Gidlund, „Security Risk Analysis of LoRaWAN and Future Directions”, *Future Internet*, köt. 11, sz. 1, o. 3, dec. 2018, doi: 10.3390/fi11010003.
- [60] S. Loukil, L. C. Fourati, A. Nayyar, és C. So-In, „Investigation on Security Risk of LoRaWAN: Compatibility Scenarios”, *IEEE Access*, köt. 10, o. 101825–101843, 2022, doi: 10.1109/ACCESS.2022.3208171.
- [61] LoRa Alliance, „TS002-1.1.0 LoRaWAN® Backend Interfaces”, 2020, o. 1–85. Elérés: 2024. május 11. [Online]. Elérhető: <https://resources.lora-alliance.org/technical-specifications/ts002-1-1-0-lorawan-backend-interfaces>
- [62] M. Alipio és M. Bures, „Current testing and performance evaluation methodologies of LoRa and LoRaWAN in IoT applications: Classification, issues, and future directives”, *Internet of Things*, köt. 25, o. 101053, ápr. 2024, doi: 10.1016/j.iot.2023.101053.
- [63] R. Carvalho, N. Correia, és F. Al-Tam, „Mobility planning of LoRa gateways for edge storage of IoT data”, *Computer Networks*, köt. 221, o. 109521, febr. 2023, doi: 10.1016/j.comnet.2022.109521.
- [64] J. R. Cotrim és J. H. Kleinschmidt, „An analytical model for multihop LoRaWAN networks”, *Internet of Things*, köt. 22, o. 100807, júl. 2023, doi: 10.1016/j.iot.2023.100807.
- [65] H. Noura, T. Hatoum, O. Salman, J.-P. Yaacoub, és A. Chehab, „LoRaWAN security survey: Issues, threats and possible mitigation techniques”, *Internet of Things*, köt. 12, o. 100303, dec. 2020, doi: 10.1016/j.iot.2020.100303.
- [66] L. Febriarti, A. M. Imammuddin, és D. Suprianto, „Analysis of Coverage Range and Data Transmission Success Rate of LoRaWAN in the Implementation of an Electrical Power Monitoring System”, *JURNAL JARTEL: Jurnal Jaringan Telekomunikasi*, köt. 15, sz. 4, o. 479–484, dec. 2025, doi: 10.33795/jartel.v15i4.8716.

- [67] M. Mehic, M. Duliman, N. Selimovic, és M. Voznak, „LoRaWAN End Nodes: Security and Energy Efficiency Analysis”, *Alexandria Engineering Journal*, köt. 61, sz. 11, o. 8997–9009, nov. 2022, doi: 10.1016/j.aej.2022.02.035.
- [68] Semtech, „AN1200.22 LoRa Modulation Basics”, 2015, o. 1–26. Elérés: 2021. november 10. [Online]. Elérhető: <https://semtech.my.salesforce.com/sfc/p/#E00000000JelG/a/2R00000001OJu/xvKUc5w9yJG1q5Pb2IikpolW54YYqGb.frOZ7HQBcRc>
- [69] LoRa Alliance, „RP002-1.0.4 Regional Parameters”, 2022, o. 1–100. Elérés: 2025. március 2. [Online]. Elérhető: <https://resources.lora-alliance.org/technical-specifications/rp002-1-0-4-regional-parameters>
- [70] P. Maurya, A. Singh, és A. A. Kherani, „A review: spreading factor allocation schemes for LoRaWAN”, *Telecommun. Syst.*, köt. 80, sz. 3, o. 449–468, júl. 2022, doi: 10.1007/s11235-022-00903-4.
- [71] D. Borsos, „Image Transmission with LoRaWAN in Agriculture”, in *Critical Infrastructure Protection in the Light of the Armed Conflicts. HCC 2022. Advanced Sciences and Technologies for Security Applications*, T. A. Kovács, Z. Nyikes, T. Berek, N. Daruka, és L. Tóth, Szerk., Cham: Springer, 2024, o. 235–246. doi: 10.1007/978-3-031-47990-8_21.
- [72] E. F. Silva és mtsai., „Adaptive Parameters for LoRa-Based Networks Physical-Layer”, *Sensors*, köt. 23, sz. 10, o. 4597, máj. 2023, doi: 10.3390/s23104597.
- [73] A. H. Jebril és R. A. Rashid, „A systematic literature review on downlink frames in LoRaWAN”, *Computers and Electrical Engineering*, köt. 101, o. 108006, júl. 2022, doi: 10.1016/j.compeleceng.2022.108006.
- [74] D. Borsos, „Development and Optimisation of Exit Procedures for LoRaWan Nodes”, in *2024 IEEE 22nd Jubilee International Symposium on Intelligent Systems and Informatics (SISY)*, IEEE, szept. 2024, o. 000523–000527. doi: 10.1109/SISY62279.2024.10737616.
- [75] D. Fernandes Carvalho és mtsai., „A test methodology for evaluating architectural delays of LoRaWAN implementations”, *Pervasive Mob. Comput.*, köt. 56, o. 1–17, máj. 2019, doi: 10.1016/j.pmcj.2019.03.002.

- [76] D. Borsos, „APPLICATIONS OF LORAWAN TECHNOLOGY”, *CYBER SECURITY REVIEW online*, o. 1–6, 2020, Elérés: 2024. május 22. [Online]. Elérhető: <https://www.cybersecurity-review.com/wp-content/uploads/2020/09/Doniz-Borsos-article-APPLICATIONS-OF-LORAWAN-TECHNOLOGY-Cyber-Security-Review-Online.pdf>
- [77] L. Berek, „Biztonságtechnika”, Budapest, Magyarország: Nemzeti Közszerológati Egyetem (NKE), 2014, o. 15–36. Elérés: 2020. december 2. [Online]. Elérhető: <https://real.mtak.hu/19709/1/biztonsagtechnika.original.pdf>
- [78] L. Berek, T. Berek, és L. Berek, „Személy- és vagyonsbiztonság”, Budapest, Magyarország: Óbudai Egyetem, Bánki Donát Gépész és Biztonságtechnikai Mérnői Kar, 2016, o. 31–81. Elérés: 2025. március 2. [Online]. Elérhető: <https://oda.uni-obuda.hu/bitstream/handle/20.500.14044/32978/3071%20Szem%C3%A9ly-%20%C3%A9s%20vagyonsbiztons%C3%A1g.pdf?sequence=1>
- [79] R. Pető és D. Tokody, „Building and Operating a Smart City”, *Interdisciplinary Description of Complex Systems*, köt. 17, sz. 3, o. 476–484, 2019, doi: 10.7906/indecs.17.3.6.
- [80] C. Ucar, M. Maloku, O. Yugay, és D. Budimir, „IoT Motion Detection Sensors for Monitoring in a Smart Campus”, in *2024 13th Mediterranean Conference on Embedded Computing (MECO)*, IEEE, jún. 2024, o. 1–4. doi: 10.1109/MECO62516.2024.10577922.
- [81] S. Satpathy, B. Sahoo, és A. K. Turuk, „Sensing and Actuation as a Service Delivery Model in Cloud Edge centric Internet of Things”, *Future Generation Computer Systems*, köt. 86, o. 281–296, szept. 2018, doi: 10.1016/j.future.2018.04.015.
- [82] V. Bonilla, B. Campoverde, és S. G. Yoo, „A Systematic Literature Review of LoRaWAN: Sensors and Applications”, *Sensors*, köt. 23, sz. 20, o. 8440, okt. 2023, doi: 10.3390/s23208440.
- [83] L. Berek, „Óbuda University e-Bulletin”, *ÓBUDA UNIVERSITY E-BULLETIN*, köt. 6, sz. 1, o. 17–20, 2016, Elérés: 2025. szeptember 7. [Online]. Elérhető: https://uni-obuda.hu/e-bulletin/Berek_7.pdf

- [84] GSMA, „The Mobile Economy 2024”, 2024, o. 1–47. Elérés: 2026. január 4. [Online]. Elérhető: <https://www.gsma.com/solutions-and-impact/connectivity-for-good/mobile-economy/wp-content/uploads/2024/02/260224-The-Mobile-Economy-2024.pdf>
- [85] M. Lichtman, R. P. Jover, M. Labib, R. Rao, V. Marojovic, és J. H. Reed, „LTE/LTE-A jamming, spoofing, and sniffing: threat assessment and mitigation”, *IEEE Communications Magazine*, köt. 54, sz. 4, o. 54–61, ápr. 2016, doi: 10.1109/MCOM.2016.7452266.
- [86] D. Borsos, „Additional wireless communication technologies that are used in LoRaWAN products and their importance in the field of personal and property protection”, in *XXXVI. Kandó Konferencia 2020*, Temesvári Zsolt, Szerk., Budapest, Hungary: Óbudai Egyetem, Kandó Kálmán Villamosmérnöki Kar, 2020, o. 121–130.
- [87] H. Boyes, B. Hallaq, J. Cunningham, és T. Watson, „The industrial internet of things (IIoT): An analysis framework”, *Comput. Ind.*, köt. 101, o. 1–12, okt. 2018, doi: 10.1016/j.compind.2018.04.015.
- [88] H. Bhatia, S. N. Panda, és D. Nagpal, „Internet of Things and its Applications in Healthcare-A Survey”, in *2020 8th International Conference on Reliability, Infocom Technologies and Optimization (Trends and Future Directions) (ICRITO)*, IEEE, jún. 2020, o. 305–310. doi: 10.1109/ICRITO48877.2020.9197816.
- [89] M. Szántó és mtsai., „Developing a Health Support System to Promote Care for the Elderly”, *Sensors*, köt. 25, sz. 2, o. 455, 2025, doi: 10.3390/s25020455.
- [90] H. Ali Hashim, S. L. Mohammed, és S. K. Gharghan, „Accurate fall detection for patients with Parkinson’s disease based on a data event algorithm and wireless sensor nodes”, *Measurement*, köt. 156, o. 107573, máj. 2020, doi: 10.1016/j.measurement.2020.107573.
- [91] P. Battistoni, M. Sebillio, és G. Vitiello, „An IoT-Based Mobile System for Safety Monitoring of Lone Workers”, *IoT*, köt. 2, sz. 3, o. 476–497, aug. 2021, doi: 10.3390/iot2030024.
- [92] T. Hadwen, V. Smallbon, Q. Zhang, és M. D’Souza, „Energy efficient LoRa GPS tracker for dementia patients”, in *2017 39th Annual International Conference of the IEEE Engineering in Medicine and Biology Society (EMBC)*, IEEE, júl. 2017, o. 771–774. doi: 10.1109/EMBC.2017.8036938.

- [93] D. Borsos, „LoRaWAN Certified Product Trends with a Special Focus on Smart Cities and Property Protection”, *Interdisciplinary Description of Complex Systems*, köt. 23, sz. 3, o. 230–239, 2025, doi: 10.7906/indecs.23.3.4.
- [94] LoRa Alliance, „LoRaWAN Certified”. Elérés: 2025. február 6. [Online]. Elérhető: <https://lora-alliance.org/lorawan-certification/>
- [95] LoRa Alliance, „LoRaWAN® Marketplace”. Elérés: 2025. december 6. [Online]. Elérhető: https://lora-alliance.org/marketplace/search/?mp_certified=1
- [96] D. Borsos és L. Berek, „Challenges of LoRaWAN technology in smart city solutions”, *Interdisciplinary Description of Complex Systems*, köt. 20, sz. 1, o. 1–10, febr. 2022, doi: 10.7906/indecs.20.1.1.
- [97] H. E. Elbsir, M. Kassab, S. Bhiri, és M. H. Bedoui, „Evaluation of LoRaWAN class B performances and its optimization for better support of actuators”, *Comput. Commun.*, köt. 198, o. 128–139, jan. 2023, doi: 10.1016/j.comcom.2022.11.016.
- [98] D. Borsos és L. Berek, „Jelenlétdetektálás megoldásai és személy- és vagyonvédelmi aspektusai”, in *KVK Habilitációs és PhD Workshop Minikonferencia: Kiadvány kötet*, T. Wühlrl, Szerk., Budapest, Magyarország: Óbudai Egyetem, Kandó Kálmán Villamosmérnöki Kar, 2024, o. 118–124.
- [99] MSZ EN 50131-x-x Szabványsorozat, *Riasztórendszerek. Behatolás- és támadásjelző rendszerek.*
- [100] MSZ EN IEC 62676-x-x Szabványsorozat, *Video-megfigyelőrendszerek biztonsági alkalmazásokhoz.*
- [101] ISO/IEC 27005:2022, *Information security, cybersecurity and privacy protection — Guidance on managing information security risks.* 2022.
- [102] MSZ CLC IEC/TS 62443-x-x Szabványsorozat, *Ipari automatizálási és szabályozási rendszerek biztonsága.*
- [103] D. Borsos, Á. Kohanecz, és D. Kozma, „LoRa and LoRaWAN Tests in the Aspect of Critical Infrastructures”, *TRANSACTIONS of the VŠB – Technical University of Ostrava Safety Engineering Series*, köt. 17, sz. 1, o. 1–11, jún. 2022, doi: 10.35182/tses-2022-0001.

- [104] D. Borsos, „Applications of LoRaWAN technology”, in *ICCECIP 2019 Abstract book*, Z. Nyikes, Szerk., Budapest, Hungary: Óbudai Egyetem, 2019, o. 22.
- [105] D. M. Kozma, Á. Kohanecz, és D. Borsos, „LoRaWAN hálózat stabilitás vizsgálata különböző környezeti viszonyok mellett”, in *XXXVII. Kandó Konferencia*, Temesvári Zsolt, Szerk., Budapest, Hungary: Óbudai Egyetem, Kandó Kálmán Villamosmérnöki Kar, 2021, o. 41–50.
- [106] D. Borsos, „Traffic-Based Anomaly Detection in LoRaWAN Networks under Indoor Environment”, in *2025 IEEE 23rd Jubilee International Symposium on Intelligent Systems and Informatics (SISY)*, IEEE, szept. 2025, o. 000357–000362. doi: 10.1109/SISY67000.2025.11205375.
- [107] D. Borsos, „Lorawan Solutions in the COVID-19 Aspect”, *TRANSACTIONS of the VŠB – Technical University of Ostrava Safety Engineering Series*, köt. 16, sz. 1, o. 7–17, 2021, doi: 10.35182/tses-2021-0002.
- [108] R. Roman, J. Zhou, és J. Lopez, „On the features and challenges of security and privacy in distributed internet of things”, *Computer Networks*, köt. 57, sz. 10, o. 2266–2279, júl. 2013, doi: 10.1016/j.comnet.2012.12.018.
- [109] S. Sicari, A. Rizzardi, L. A. Grieco, és A. Coen-Porisini, „Security, privacy and trust in Internet of Things: The road ahead”, *Computer Networks*, köt. 76, o. 146–164, jan. 2015, doi: 10.1016/j.comnet.2014.11.008.
- [110] M. El-Hosseini, H. ZainEldin, H. Arafat, és M. Badawy, „A fire detection model based on power-aware scheduling for IoT-sensors in smart cities with partial coverage”, *J. Ambient Intell. Humaniz. Comput.*, köt. 12, sz. 2, o. 2629–2648, febr. 2021, doi: 10.1007/s12652-020-02425-w.
- [111] M. Beyrouiti, A. Lounis, B. Lussier, A. Bouabdallah, és A. E. Samhat, „Vulnerability-oriented risk identification framework for IoT risk assessment”, *Internet of Things*, köt. 27, o. 101333, okt. 2024, doi: 10.1016/j.iot.2024.101333.
- [112] D. Borsos, Á. Kohanecz, és D. M. Kozma, „Lorawan networks test aspects of critical infrastructures”, in *ICCECIP 2021 - Poster*, Budapest, Hungary: Óbudai Egyetem, 2021, o. 1.

- [113] Antenna Hungária, „Az Antenna Hungária fejlesztők részére megnyitotta országos IoT hálózatát”. Elérés: 2023. augusztus 6. [Online]. Elérhető: <https://4igtavkozlesiholding.hu/hu/hirek/az-antenna-hungaria-fejlesztok-reszere-megnyitotta-oroszagos-iot-halozatat>
- [114] A. H. Jebril, A. Sali, A. Ismail, és M. F. A. Rasid, „Overcoming Limitations of LoRa Physical Layer in Image Transmission”, *Sensors*, köt. 18, sz. 10, o. 3257, szept. 2018, doi: 10.3390/s18103257.
- [115] D. Borsos, „Lorawan Picture Transmission Solutions in Agriculture”, in *ICCECIP 2022 4th International Conference on Central European Critical Infrastructure Protection: Abstract Book*, Z. Nyikes és T. A. Kovács, Szerk., Budapest, Hungary: Óbudai Egyetem, 2022, o. 38.
- [116] T. Chen, D. Eager, és D. Makaroff, „Efficient Image Transmission Using LoRa Technology In Agricultural Monitoring IoT Systems”, in *2019 International Conference on Internet of Things (iThings) and IEEE Green Computing and Communications (GreenCom) and IEEE Cyber, Physical and Social Computing (CPSCom) and IEEE Smart Data (SmartData)*, IEEE, júl. 2019, o. 937–944. doi: 10.1109/iThings/GreenCom/CPSCom/SmartData.2019.00166.
- [117] J. M. Marais, R. Malekian, és A. M. Abu-Mahfouz, „LoRa and LoRaWAN testbeds: A review”, in *2017 IEEE AFRICON*, IEEE, szept. 2017, o. 1496–1501. doi: 10.1109/AFRCON.2017.8095703.
- [118] ISO/IEC 27002:2022, *Information security, cybersecurity and privacy protection — Information security controls*. 2022.
- [119] F. A. Alaba, M. Othman, I. A. T. Hashem, és F. Alotaibi, „Internet of Things security: A survey”, *Journal of Network and Computer Applications*, köt. 88, o. 10–28, jún. 2017, doi: 10.1016/j.jnca.2017.04.002.
- [120] M. Ammar, G. Russello, és B. Crispo, „Internet of Things: A survey on the security of IoT frameworks”, *Journal of Information Security and Applications*, köt. 38, o. 8–27, febr. 2018, doi: 10.1016/j.jisa.2017.11.002.
- [121] J. Bugeja, A. Jacobsson, és P. Davidsson, „On Privacy and Security Challenges in Smart Connected Homes”, in *2016 European Intelligence and Security Informatics Conference (EISIC)*, IEEE, aug. 2016, o. 172–175. doi: 10.1109/EISIC.2016.044.

- [122] L. Catarinucci és mtsai., „An IoT-Aware Architecture for Smart Healthcare Systems”, *IEEE Internet Things J.*, köt. 2, sz. 6, o. 515–526, dec. 2015, doi: 10.1109/JIOT.2015.2417684.
- [123] J. Zhou, Z. Cao, X. Dong, és A. V. Vasilakos, „Security and Privacy for Cloud-Based IoT: Challenges”, *IEEE Communications Magazine*, köt. 55, sz. 1, o. 26–33, jan. 2017, doi: 10.1109/MCOM.2017.1600363CM.
- [124] Y. Meidan és mtsai., „N-BaIoT—Network-Based Detection of IoT Botnet Attacks Using Deep Autoencoders”, *IEEE Pervasive Comput.*, köt. 17, sz. 3, o. 12–22, júl. 2018, doi: 10.1109/MPRV.2018.03367731.
- [125] E. Dritsas és M. Trigka, „A Survey on Cybersecurity in IoT”, *Future Internet*, köt. 17, sz. 1, o. 30, jan. 2025, doi: 10.3390/fi17010030.
- [126] P. D. More, S. R. Sakhare, és P. Mahalle, „Identity Management in the Internet of Things: A Survey of the State of the Art”, *IEEE Syst. Man Cybern. Mag.*, köt. 9, sz. 4, o. 13–19, okt. 2023, doi: 10.1109/MSMC.2022.3230215.
- [127] IoT Security Foundation, „IoT Cybersecurity for Facilities Professionals in the Smart Built Environment”, 2023, o. 1–53. Elérés: 2024. április 4. [Online]. Elérhető: <https://iotsecurityfoundation.org/wp-content/uploads/2023/03/IoT-Cybersecurity-for-Facilities-Professionals-in-the-Smart-Built-Environment-RELEASE-1-0-FINAL-30-03-2023.pdf>
- [128] IoT Security Foundation, „Secure Design - Best Practice Guides”, 2019, o. 1–20. Elérés: 2024. április 4. [Online]. Elérhető: https://www.iotsecurityfoundation.org/wp-content/uploads/2019/12/Best-Practice-Guides-Release-2_Digitalv3.pdf
- [129] N. Yousefnezhad, A. Malhi, és K. Främling, „Security in product lifecycle of IoT devices: A survey”, *Journal of Network and Computer Applications*, köt. 171, o. 102779, dec. 2020, doi: 10.1016/j.jnca.2020.102779.
- [130] F. Adelantado, X. Vilajosana, P. Tuset-Peiro, B. Martinez, J. Melia-Segui, és T. Watteyne, „Understanding the Limits of LoRaWAN”, *IEEE Communications Magazine*, köt. 55, sz. 9, o. 34–40, 2017, doi: 10.1109/MCOM.2017.1600613.

- [131] J. Haxhibeqiri, E. De Poorter, I. Moerman, és J. Hoebeke, „A Survey of LoRaWAN for IoT: From Technology to Application”, *Sensors*, köt. 18, sz. 11, o. 3995, nov. 2018, doi: 10.3390/s18113995.
- [132] D. Maccarrone, „10 IoT Trends Shaping the Future in 2025”, LORIOT. Elérés: 2026. február 6. [Online]. Elérhető: <https://loriot.io/blog/IoT-trends-2025.html>

8 A tézispontokhoz kapcsolódó tudományos közlemények

- [BD1] D. Borsos, „A LoRaWAN-technológia szerepe az elektronikai védelem területén, az építőipari beruházások vonatkozásában”, *Hadmérnök*, köt. 16, sz. 3, o. 5–16, nov. 2021, doi: 10.32567/hm.2021.3.1.
- [BD2] D. Borsos, „Bevezetés a személy- és vagyonvédelem területén alkalmazható IoT technológiákba – LoRaWAN technológia”, in *XXXV. Jubileumi Kandó Konferencia 2019*, Temesvári Zsolt, Szerk., Budapest, Hungary: Óbudai Egyetem, Kandó Kálmán Villamosmérnöki Kar, 2020, o. 94–102.
- [BD3] D. Borsos, „Image Transmission with LoRaWAN in Agriculture”, in *Critical Infrastructure Protection in the Light of the Armed Conflicts. HCC 2022. Advanced Sciences and Technologies for Security Applications*, T. A. Kovács, Z. Nyikes, T. Berek, N. Daruka, és L. Tóth, Szerk., Cham: Springer, 2024, o. 235–246. doi: 10.1007/978-3-031-47990-8_21.
- [BD4] D. Borsos, „Development and Optimisation of Exit Procedures for LoRaWan Nodes”, in *2024 IEEE 22nd Jubilee International Symposium on Intelligent Systems and Informatics (SISY)*, IEEE, szept. 2024, o. 000523–000527. doi: 10.1109/SISY62279.2024.10737616.
- [BD5] D. Borsos, „APPLICATIONS OF LORAWAN TECHNOLOGY”, *CYBER SECURITY REVIEW online*, o. 1–6, 2020, Elérés: 2024. május 22. [Online]. Elérhető: <https://www.cybersecurity-review.com/wp-content/uploads/2020/09/Doniz-Borsos-article-APPLICATIONS-OF-LORAWAN-TECHNOLOGY-Cyber-Security-Review-Online.pdf>
- [BD6] D. Borsos, „Additional wireless communication technologies that are used in LoRaWAN products and their importance in the field of personal and property protection”, in *XXXVI. Kandó Konferencia 2020*, Temesvári Zsolt, Szerk., Budapest, Hungary: Óbudai Egyetem, Kandó Kálmán Villamosmérnöki Kar, 2020, o. 121–130.
- [BD7] D. Borsos, „LoRaWAN Certified Product Trends with a Special Focus on Smart Cities and Property Protection”, *Interdisciplinary Description of Complex Systems*, köt. 23, sz. 3, o. 230–239, 2025, doi: 10.7906/indec.23.3.4.

- [BD8] D. Borsos és L. Berek, „Challenges of LoRaWAN technology in smart city solutions”, *Interdisciplinary Description of Complex Systems*, köt. 20, sz. 1, o. 1–10, febr. 2022, doi: 10.7906/indec.20.1.1.
- [BD9] D. Borsos és L. Berek, „Jelenlétdetektálás megoldásai és személy- és vagyonvédelmi aspektusai”, in *KVK Habilitációs és PhD Workshop Minikonferencia: Kiadvány kötet*, T. Wühl, Szerk., Budapest, Magyarország: Óbudai Egyetem, Kandó Kálmán Villamosmérnöki Kar, 2024, o. 118–124.
- [BD10] D. Borsos, Á. Kohanecz, és D. Kozma, „LoRa and LoRaWAN Tests in the Aspect of Critical Infrastructures”, *TRANSACTIONS of the VŠB – Technical University of Ostrava Safety Engineering Series*, köt. 17, sz. 1, o. 1–11, jún. 2022, doi: 10.35182/tses-2022-0001.
- [BD11] D. Borsos, „Applications of LoRaWAN technology”, in *ICCECIP 2019 Abstract book*, Z. Nyikes, Szerk., Budapest, Hungary: Óbudai Egyetem, 2019, o. 22.
- [BD12] D. M. Kozma, Á. Kohanecz, és D. Borsos, „LoRaWAN hálózat stabilitás vizsgálata különböző környezeti viszonyok mellett”, in *XXXVII. Kandó Konferencia*, Temesvári Zsolt, Szerk., Budapest, Hungary: Óbudai Egyetem, Kandó Kálmán Villamosmérnöki Kar, 2021, o. 41–50.
- [BD13] D. Borsos, „Traffic-Based Anomaly Detection in LoRaWAN Networks under Indoor Environment”, in *2025 IEEE 23rd Jubilee International Symposium on Intelligent Systems and Informatics (SISY)*, IEEE, szept. 2025, o. 000357–000362. doi: 10.1109/SISY67000.2025.11205375.
- [BD14] D. Borsos, „Lorawan Solutions in the COVID-19 Aspect”, *TRANSACTIONS of the VŠB – Technical University of Ostrava Safety Engineering Series*, köt. 16, sz. 1, o. 7–17, 2021, doi: 10.35182/tses-2021-0002.
- [BD15] D. Borsos, Á. Kohanecz, és D. M. Kozma, „Lorawan networks test aspects of critical infrastructures”, in *ICCECIP 2021 - Poster*, Budapest, Hungary: Óbudai Egyetem, 2021, o. 1.
- [BD16] D. Borsos, „Lorawan Picture Transmission Solutions in Agriculture”, in *ICCECIP 2022 4th International Conference on Central European Critical Infrastructure Protection: Abstract Book*, Z. Nyikes és T. A. Kovács, Szerk., Budapest, Hungary: Óbudai Egyetem, 2022, o. 38.

9 További tudományos közlemények (opcionális)

- [BD17] M. Szántó, D. Borsos, és T. Sándor, „Egészségvédelmi és távfelügyeleti karpánt megvalósítása LoRaWAN technológiával”, in *XXXV. Jubileumi Kandó Konferencia 2019*, Temesvári Zsolt, Szerk., Budapest, Hungary: Óbudai Egyetem, Kandó Kálmán Villamosmérnöki Kar, 2020, o. 195–201.
- [BD18] D. Borsos, J. Fintor, és G. Zsáry, „Teszt- és kényszerfájl generátor FPGA fejlesztéshez és ennek használata, jelentősége az oktatásban”, in *XXXVI. Kandó Konferencia 2020*, Z. Temesvári, Szerk., Budapest, Hungary: Óbudai Egyetem, Kandó Kálmán Villamosmérnöki Kar, 2020, o. 19–32.
- [BD19] D. Borsos és T. Sándor, „IoT alkalmazásának lehetőségei ipari környezetben”, in *XXXV. Jubileumi Kandó Konferencia 2019*, Temesvári Zsolt, Szerk., Budapest, Hungary: Óbudai Egyetem, Kandó Kálmán Villamosmérnöki Kar, 2020, o. 121–129.
- [BD20] D. Borsos és T. Sándor, „Napjaink ipari vezeték nélküli kommunikációnak lehetőségei”, in *XXXV. Jubileumi Kandó Konferencia 2019*, Temesvári Zsolt, Szerk., Budapest, Hungary: Óbudai Egyetem, Kandó Kálmán Villamosmérnöki Kar, 2020, o. 113–120.
- [BD21] D. Borsos és T. Sándor, „Blokk-alapú programozás a mikrokontroller oktatásban”, in *XXXV. Jubileumi Kandó Konferencia 2019*, Temesvári Zsolt, Szerk., Budapest, Hungary: Óbudai Egyetem, Kandó Kálmán Villamosmérnöki Kar, 2020, o. 103–112.
- [BD22] M. Kriston és D. Borsos, „Traffic Sign Detection Using Convolutional Neural Networks”, in *XXXVII. Kandó Konferencia*, Temesvári Zsolt, Szerk., Budapest, Hungary: Óbudai Egyetem, Kandó Kálmán Villamosmérnöki Kar, 2021, o. 131–138.
- [BD23] D. Borsos és T. Sándor, „Környezeti paraméterek figyelésére alapozott mesterséges intelligenciát tartalmazó hajtásvezérlési rendszer problémái”, in *XXXVIII. Kandó Konferencia 2022 - Kiadvány kötet*, Temesvári Zsolt, Wühl Tibor, és Molnár György, Szerk., Budapest, Hungary: Óbudai Egyetem, Kandó Kálmán Villamosmérnöki Kar, 2022, o. 107–114.
- [BD24] D. K. Berkes, M. Sánta, és D. Borsos, „Okosbója mérésadatgyűjtő rendszer”, in *XXXVIII. Kandó Konferencia 2022 - Kiadvány kötet*, Temesvári Zsolt, Wühl Tibor, és Molnár György, Szerk., Budapest, Hungary: Óbudai Egyetem, Kandó Kálmán Villamosmérnöki Kar, 2022, o. 181–190.

- [BD25] J. Kovács, P. Schmidt, T. Sándor, és D. Borsos, „Sakk játék megvalósítása delta robot segítségével”, in *XXXVIII. Kandó Konferencia 2022 - Absztrakt kötet*, Z. Temesvári, T. Wühl, és G. Molnár, Szerk., Budapest, Hungary: Óbudai Egyetem, 2022, o. 78.
- [BD26] D. Borsos, A. Fodor, és T. Sandor, „Challenges in Isokinetic Sampling for Gas and Particle Measurements: Testing Homogeneity and Handling Interruptions in Sampling”, in *INES 2023 - 27th IEEE International Conference on Intelligent Engineering Systems 2023, Proceedings*, Nairobi, Kenya, 2023, o. 229–234. doi: 10.1109/INES59282.2023.10297863.
- [BD27] T. Sándor, G. Molnár, D. Borsos, és Sik Dávid, „Kreatív megoldások, avagy a mérnökké válás első lépései”, in *XXXIX. Kandó Konferencia 2023*, Molnár György, Temesvári Zsolt, és Wühl Tibor, Szerk., Budapest, Magyarország: Óbudai Egyetem, 2023, o. 312–319.
- [BD28] J. Israr és D. Borsos, „Tool Condition Monitoring in High-Speed Machining: Techniques and Trends”, in *2024 IEEE 7th International Conference and Workshop Óbuda on Electrical and Power Engineering (CANDO-EPE)*, Budapest, Hungary, 2024, o. 231–236. doi: 10.1109/CANDO-EPE65072.2024.10772807.
- [BD29] A. Fodor, D. Borsos, és T. Sandor, „Fuzzy-based Gear Shifting Algorithm for Twin-drive in MATLAB Simulink model”, in *2024 IEEE 22nd World Symposium on Applied Machine Intelligence and Informatics, SAMI 2024 - Proceedings*, Stará Lesná, Slovakia, 2024, o. 315–320. doi: 10.1109/SAMI60510.2024.10432838.
- [BD30] D. Sályi és D. Borsos, „Bionic Hand with Phalanx Built-In Servos”, in *Critical Infrastructure Protection in the Light of the Armed Conflicts. HCC 2022. Advanced Sciences and Technologies for Security Applications*, T. A. Kovács, Z. Nyikes, T. Berek, N. Daruka, és L. Tóth, Szerk., Cham: Springer, 2024. doi: 10.1007/978-3-031-47990-8_11.
- [BD31] M. Szántó és mtsai., „Developing a Health Support System to Promote Care for the Elderly”, *Sensors*, köt. 25, sz. 2, o. 455, 2025, doi: 10.3390/s25020455.
- [BD32] A. Kamagara, S. Babirye, és D. Borsos, „Optimized Multi-cloud Service Orchestration in Cloud Computing”, in *The Impact of the Energy Dependency on Critical Infrastructure Protection. ICCECIP 2024. Advanced Sciences and Technologies for Security*

- Applications*, T. A. Kovács, R. G. Stadler, és N. Daruka, Szerk., Cham: Springer, 2025, o. 179–191.
- [BD33] I. Junaid és D. Borsos, „Artificial Intelligence and Machine Learning in Metal Additive Manufacturing: An Overview”, in *XL. Kandó Konferencia Kiadvány*, Wühl Tibor, Szerk., Budapest, Hungary: Óbudai Egyetem, Kandó Kálmán Villamosmérnöki Kar, 2025, o. 60–78.
- [BD34] K. Ben Khaled, D. Borsos, és J. Katona, „Benchmarking Cryptographic Protocols for (IoT) Malware Defence”, in *2025 IEEE 23rd World Symposium on Applied Machine Intelligence and Informatics (SAMI)*, Stará Lesná, Slovakia, 2025, o. 41–46. doi: 10.1109/SAMI63904.2025.10883306.
- [BD35] T. Sándor, I. Bendiák, D. Borsos, és R. Szabolcsi, „Heat Loss Calculation of the Electric Drives”, *Machines*, köt. 13, sz. 11, o. 988, okt. 2025, doi: 10.3390/machines13110988.
- [BD36] K. Ben Khaled, D. Borsos, és J. Katona, „Vulnerability Scanning Techniques in IoT Firmware”, in *2026 IEEE 24th World Symposium on Applied Machine Intelligence and Informatics (SAMI)*, IEEE, jan. 2026, o. 000671–000676. doi: 10.1109/SAMI68106.2026.11420778.