DOI: https://doi.org/10.12700/btsz.2026.8.2.15

THE EVOLUTION OF DOMOTICS SYSTEMS AND THEIR FUNCTION IN SMART BUILDINGS

A DOMOTIKA RENDSZEREK FEJLŐDÉSE ÉS SZEREPE AZ INTELLIGENS ÉPÜLETEK MŰKÖDÉSÉBEN

MÁRKOS Szilárd Attila[1] – KOLLÁR Csaba[2]

Abstract

The development of intelligent buildings has undergone significant transformation over the past two decades. In order to achieve comfort, energy-efficiency, and sustainability objectives, the most advanced technologies are increasingly being integrated into building operation systems. This study provides a systematic literature review of the technological development of domotics systems, their role in intelligent buildings, and their operational principles. The study presents the evolution of building automation from electromechanical control devices to systems supported by artificial intelligence. Furthermore, it discusses the role of IoT architectures, communication protocols, ESG/sustainability considerations, digital twin technology, edge computing, and cloud-based data processing. The study also addresses cybersecurity challenges and emphasizes the importance of user acceptance and organizational culture in the effective operation of intelligent buildings.

Keywords

Intelligent buildings, building automation, digital twin, IoT, edge computing

Absztrakt

Az intelligens épületek fejlődése az elmúlt két évtizedben jelentős átalakuláson ment keresztül. A komfort-, az energiahatékonysági és a fenntarthatósági célok elérése érdekében a legmodernebb technológiák épülnek be az épületüzemeltetésbe. A tanulmány a domotika rendszerek technológiai fejlődését, intelligens épületekben betöltött szerepét és működési alapelveit tekinti át szisztematikus irodalmi összefoglalás keretében. A tanulmány bemutatja az épületautomatizálás fejlődését az elektromechanikus vezérlőeszközöktől egészen a mesterséges intelligenciával támogatott rendszerekig, továbbá ismerteti az IoT-architektúrák, a kommunikációs protokollok, az ESG/fenntarthatósági szempontok, a digitális iker technológia, az edge computing és a felhőalapú adatfeldolgozás szerepét. A tanulmány külön kitér a kiberbiztonsági kihívásokra, továbbá hangsúlyozza a felhasználói elfogadás és a szervezeti kultúra szerepét az intelligens épületek hatékony működtetésében.

Kulcsszavak

Intelligens épületek, épületautomatizálás, digitális iker, IoT, edge computing

[1] markos.szilard@bgk.uni-obuda.hu | ORCID: 0009-0007-1044-6099 | university intern, Óbuda University Bánki Donát Faculty of Mechanical and Safety Engineering | egyetemi gyakornok, Óbudai Egyetem Bánki Donát Gépész és Biztonságtechnikai Mérnöki Kar

[2] kollar.csaba@uni-obuda.hu | ORCID: 0000-0002-0981-2385 | senior research fellow and leader, Óbuda University Bánki Donát Faculty of Mechanical and Safety Engineering Artificial Intelligence Workshop | tudományos főmunkatárs és vezető, Óbudai Egyetem Bánki Donát Gépész és Biztonságtechnikai Mérnöki Kar Mesterséges Intelligencia Műhely

BEVEZETÉS

Az épületek vezérlési technológiája az elmúlt két évtizedben gyökeresen megváltozott. Ami korábban statikus infrastruktúra volt, az mára adatvezérelt, hálózatba kapcsolat rendszerré vált. A modern intelligens rendszerek működése egyre inkább arra épül, hogy az épület képes legyen alkalmazkodni a benne élők igényeihez és a környezet folyamatos változásaihoz. Ennek eredményeként a különböző gépészeti megoldások összehangoltabban működhetnek, miközben a rendszer előre reagálhat bizonyos helyzetekre a komfort és a hatékonyság fenntartása érdekében [1], [2].

Az Európai Unió statisztikái szerint a teljes energiafogyasztásának közel 40 százalékáért az épületállomány felel [3]. Ez a volumen önmagában is magyarázatot ad arra miért lett ez a terület stratégiai kérdés. Ez az arány olyan mértékű, amelyre politikai és gazdasági szabályozások épülnek: energiahatékonysági irányelvek, szén-dioxid-kvóták, kötelező felújítási programok. Ebben a kontextusban az intelligens épületüzemeltetés már nem csak a gazdaságos üzemeltetésről és a komfortról szól, hanem központi gazdasági és szabályozási szükségszerűség [4].

A fejlődés üteme figyelemre méltó. Két-három évtized alatt jutott el a terület az egyszerű időkapcsolóktól az önoptimalizáló, AI-vezérelt rendszerekig. Ma egy épületfelügyeleti platform nemcsak vezérel, hanem előre jelez, tanul és dönt [5]. Az IoT, a felhőalapú platformok és a gépi tanulás kombinációja olyan képességeket adott az épületüzemeltetésnek, amelyek korábban csak ipari folyamatirányításban léteztek [6], [7].

A domotika szerepe azon túl, hogy gazdaságosan üzemeltethető egy épület a felhasználói komfort, az üzemeltetési megbízhatóság, a hosszú távú ingatlanérték fenntartásában is kiemelt szerepet kap [2], [8]. Egy jól felépített rendszer átfogó irányítási stratégiát dolgoz ki és valósít meg.

Mindezzel együtt jár a kockázati profil megváltozása. Minél több érzékelő, vezérlő és hálózati eszköz kerül egy épületbe, annál nagyobb a potenciális kibertámadási felület [9], [10]. Egy HVAC-rendszer vagy beléptető infrastruktúra feltörése ma már nem csak adatvédelmi incidens, fizikai következményekkel is járhat. Az intelligens épületek, különösen közintézményi és ipari környezetben, fokozatosan a kritikus infrastruktúrák kategóriájába kerülnek, és ezt a szemléletet az üzemeltetési gyakorlatnak is követnie kell [11].

A tanulmány a domotika rendszerek fejlődését, technológiai alapjait és szerepét tekinti át az intelligens épületek kontextusában. A vizsgálat kiterjed a fejlődéstörténetre, technológiai felépítésre, energetikai és biztonsági vonatkozásokra, valamint a mesterséges intelligencia épületirányításban betöltött szerepére. A tanulmány a terület meghatározó szakirodalmának feldolgozására épül. A cél az, hogy az olvasó átfogó képet kapjon, hogyan jutottunk az analóg időkapcsolóktól az AI-alapú épületirányításig.

A DOMOTIKA FOGALMI ÉS TECHNOLÓGIAI ALAPJAI

A domotika nem egyszerű szinonimája az épületgépészeti vezérlésnek, hanem annál lényegesen tágabb fogalom. A hagyományos épületautomatizálás az épületgépészeti alrendszerek, elsősorban a fűtés, hűtés, szellőzés, világítás, árnyékolás és biztonságtechnika integrált automatizálása [1]. A modern domotika azonban ennél lényegesen több: az infor-

matikai, kommunikációs és fizikai infrastruktúrák összekapcsolt rendszere, amely adatvezérelt, önoptimalizáló működésre képes [1], [2]. Ez az átalakulás az elmúlt két évtized terméke és szorosan összefügg az IoT és a számítógépes fizikai rendszerek megjelenésével.

A szó a latin domus szóból ered, de ez az etimológia mára kissé szűknek bizonyult. A modern domotika rendszerek egy lakás, egy teljes irodaház, kórház vagy ipari létesítmény digitális idegrendszereként működnek: érzékelnek, feldolgoznak, következtetnek és beavatkoznak, valós időben, folyamatosan [1], [2].

Az épületek belső architektúrája is sokat változott. A korai domotika rendszerek erősen centralizáltak voltak. A centralizált vezérlési architektúrának jelentős sérülékenységet hordoztak, ha a központi egység meghibásodott, az egész rendszer leállt [4]. Ezt akkoriban elfogadható kompromisszumnak tartották. Azonban később, a kritikus infrastruktúrák szemléletének terjedésével egyértelművé vált, hogy ez túl nagy kitettséget jelent és ezt a rendszer tervezése során lehetőség szerint el kell kerülni. A mai intelligens épületekben osztott intelligencia működik: az alrendszerek önálló döntéshozatalra képes egységekként viselkednek, amelyek egymástól függetlenül bővíthetők és fejleszthetők.

Egy közepes irodaépületben ma már több száz érzékelő működik párhuzamosan: hőmérséklet, páratartalom, szén-dioxid-szint, mozgás, fényintenzitás, energiafogyasztás [2], [5]. Ezen adatfolyamokat használja fel a vezérlési logika, az előrejelző modellek és a döntéstámogatás segítésének érdekében.

Az aktuátorok végzik el a vezérlési utasítások fizikai végrehajtását: egy fűtési szelepet mozgat, egy lámpa kapcsol, egy árnyékolót mozgat. Itt találkozik a digitális és a fizikai világ.

A kommunikációs protokoll megválasztása az intelligens épület egyik legtartósabb következményű döntése. A KNX elosztott, eseményvezérelt felépítéssel főként lakó- és kiskereskedelmi épületekben terjedt el; a BACnet nyílt protokollként a kereskedelmi szegmens referenciaszabványává vált; a Modbus az ipari és energetikai alrendszereknél maradt releváns [3], [4], [12].(

A vezeték nélküli technológiák, a ZigBee, Z-Wave, Bluetooth Low Energy és a Matter, rugalmasabb telepítést és könnyebb bővíthetőséget kínálnak, de emelt biztonsági kockázattal. Az IoT elterjedésével az intelligens épület ma már nem egyetlen zárt rendszer, hanem heterogén eszközök és platformok összekapcsolt halmaza [2], [5]. Egyszerre jelenti azonban azt is, hogy a rendszer biztonsági szintjét a leggyengébb láncszem határozza meg.

A felhőalapú és az edge computing megközelítés jól kiegészíti egymást, és az egyensúly megtalálása az intelligens épület egyik legfontosabb tervezési kérdése. A felhő alapú erős hosszú távú elemzésnél, nagy adatvolumennél, összesített riportingnál [6]. Az edge computing ott nélkülözhetetlen, ahol a válaszidő valóban számít.

A modern domotika rendszerek tehát kiberfizikai rendszerekké váltak: olyan infrastruktúrává, ahol a fizikai tér és a digitális vezérlés szoros kölcsönhatásban működik [5], [6]. Ez az integráció hatékonyságot és alkalmazkodóképességet ad. Egyúttal azt is jelenti azonban, hogy egy digitális kompromittáció fizikai következményekkel járhat.

A DOMOTIKA RENDSZEREK FEJLŐDÉSTÖRTÉNETE

A korai automatizálási rendszerek

Az épületautomatizálás gyökerei az 1960-as-1970-es évtizedekbe nyúlnak vissza. A korai megoldások az elektromechanikus logikára épültek [1]. Mai szemmel nézve ezek egyszerű

eszközök voltak: időkapcsoló relék, hőfokszabályozók és analóg vezérlőegységek. De a maguk korában komoly lépést jelentettek azáltal, hogy lehetővé tették az épületüzemeltetés részleges automatizálhatóságát, ezzel sikerült az emberi beavatkozást részben kiváltani.

Az 1973-as olajválság indikátorként hatott az épületüzemeltetés fejlődésére. Az energiaárak drasztikus megugrása rávilágított arra, hogy az épületek pazarló üzemeltetése [2]. Ez a gazdasági kényszer valódi keresletet teremtett az automatizált energiafelügyelet iránt, amit addig inkább csak kényelmi szempontból szorgalmaztak. A korszak rendszerei egymástól elszigetelve működtek, melyek nem kommunikáltak egymással és nem voltak képesek alkalmazkodni a változó körülményekhez. Ezen rendszerek rugalmatlansága jelentősen korlátozta a működésük hatékonyságát.

Visszatekintve ezekre a korai rendszerekre, nehéz lenne intelligensnek nevezni, hiányzott belőlük az alkalmazkodóképesség és a hálózati integráció [1]. Kezdetlegességük ellenére kiemelt jelentőséggel bírnak a logikai alapok lefektetésében, ami a modern rendszerek alapját képezik elsősorban a HVAC szabályozás és az energiafelügyelet területén.

Az analóg szabályozók egyik paradoxona a statikus beállíthatóság, ami egyszerre erény és korlátozó tényező is. Megbízhatóak és könnyen üzemeltethetőek voltak, azonban mivel egy előre beállított logika alapján működtek, képtelenek voltak alkalmazkodni a környezeti változásokhoz [3]. Ez a rugalmatlanság olyan igényt teremtett, amelyet az analóg világ nem tudott kielégíteni.

A mikroprocesszoros korszak

Az 1980-as évek elején megjelent mikroprocesszorok valódi fejlődési ugrást jelentettek az épületautomatizálásban. Nemcsak gyorsabb volt az analóg logikánál, hanem programozható is: lehetett benne szabályokat tárolni, feltételeket kezelni, és idővel egyre összetettebb vezérlési logikát futtatni [4]. Az épületautomatizálás ekkor lépett ki az egyszerű időzítők és küszöbértékek szűk keretei közül.

Ebből a mikroprocesszoros alapból nőttek ki az első valódi épületmenedzsment-rendszerek. Ezek már arra is képesek voltak, amit korábban elképzelhetetlennek tartottak: egyetlen kezelőfelületen látni és vezérelni egy egész épület HVAC, világítás és energiamenedzsment rendszerét [5]. Az energetikai megtakarítások mérhetők lettek, a működés átláthatóbbá vált. Az optimalizálás szó azonban még nem volt helyénvaló, mert a rendszer csak azt csinálta, amire betanították.

A korszak egyik fontos eredménye a kommunikációs protokollok első generációjának megjelenése volt. Addig minden gyártó saját, zárt rendszerben gondolkodott. Az első protokollok ezt a falat kezdték lebontani: különböző gyártók eszközei elkezdtek egymással „kommunikálni" [6]. A kompatibilitás azonban korántsem volt teljes, és a különböző szabványok közötti feszültség évtizedeken át tartott.

Hálózatba kapcsolt intelligens rendszerek

A 2000-es évek elején az internet alapú kommunikáció egyszerre hozta el az intelligens épületek egyik legnagyobb lehetőségét és egyik legnagyobb kockázatát. Az internet megjelenése az épületautomatizálásban forradalmasította az integrációt: különböző alrendszerek össze tudtak kapcsolódni, adatot tudtak megosztani, és egy átfogó felügyeleti rendszerbe lehetett őket integrálni [7]. Ugyanakkor az addig fizikailag elszigetelt infrastruktúra nyitottá vált a világ felé és ezáltal kibertámadási kockázatot jelentett. Az épületautomatizálási szektor csak évekkel később kezdett el az ilyen veszélyek elhárításával komolyabban foglalkozni.

A KNX, a BACnet és a LonWorks ebben az időszakban váltak iparági szabvánnyá [8]. Az Ethernet megjelenése az épülethálózatokban növelte az adatátvitel kapacitását és az összekapcsolható eszközök számát. Egy valódi épületintegráció első generációja jött létre: a HVAC, a világítás, a biztonságtechnika és az energiafelügyelet közös adatbuszra kerülhetett.

Az integrált rendszerek egy olyan üzemeltetési modellt tettek lehetővé, amelyet korábban csak elméletben lehetett elképzelni: az épület különböző alrendszerei valós idejű adatokat cseréltek, és ezek alapján összehangoltan vezéreltek [7]. A monitoring és az automatizált szabályozás egymást erősítő elemmé vált. A korábban egymástól elszigetelt alrendszerek összekapcsolhatóvá váltak és egy komplex épület automatizálási rendszer részét képezték.

A hálózati integráció lehetővé tette az adatvezérelt épületmenedzsmentet, de olyan komplexitást is teremtett, amellyel a kor üzemeltetői nehezen boldogultak [8]. Vegyes protokollok, inkompatibilis platformok, integrációs problémák a mai napig problémát okoznak.

A kiberbiztonsági gondolkodás felismerése nem tartott lépést a technológiai fejlődéssel. Az épületüzemeltetők és tervezők fizikai infrastruktúrában gondolkodtak, amelynek biztonságát fizikai védelemmel biztosították. Az internetkapcsolat megjelenése teljesen megváltoztatta a fenyegetési modellt [9] amit a tervezési és üzemeltetési gyakorlat csak évekkel később követett le.

IoT és mesterséges intelligencia alapú korszak

Napjainkban az intelligens épületek fejlődése már egy teljesen új dimenzióba lépett. Az IoT, a felhőalapú adatfeldolgozás, a mesterséges intelligencia és a kiberfizikai rendszerek egymást erősítő konvergenciája olyan képességeket ad az épületüzemeltetési rendszereknek, amelyeknek korábban elképzelhetetlenek voltak [10]. A modern intelligens épület nem vezérel, hanem gondolkodik: mintázatokat ismer fel, döntéseket hoz, és tanul.

A leglátványosabb változás az optimalizálás fogalmában van. A statikus szabályozás végrehajtása helyett ma az optimalizálás az időjárás-előrejelzés, az aktuális energiaárak, a hálózati terhelés és a felhasználói szokások egyidejű figyelembevételét jelenti [13]. A rendszer nem reagál, hanem megelőz. A prediktív karbantartás, az alkalmazkodó vezérlés, az önoptimalizáló üzemeltetés, ma már az épületüzemeltetés szerves részét képezi.

Az IoT-korszak számos előnye mellett a korábbi biztonsági kockázatokat tovább fokozza. Minél több eszköz kapcsolódik a hálózathoz, annál több a potenciális belépési pont egy esetleges támadáshoz [14]. Az IoT-eszközök sokszor korlátozott biztonsági képességekkel érkeznek: gyenge hitelesítés, ritka frissítések, gyártói támogatás idő előtti megszűnése. A modern intelligens épületek, különösen közintézményi és ipari környezetben, ma már a kritikus infrastruktúrák biztonsági logikájával kezelendők [11].

A digitális iker és az edge computing technológiái szorosan kapcsolódnak ehhez a területhez, részletes bemutatásuk azonban az 5. fejezetben történik.

A DOMOTIKA RENDSZEREK SZEREPE AZ INTELLIGENS ÉPÜLETEK MŰKÖDÉSÉBEN

Energiahatékonyság és optimalizálás

Az intelligens épületek legkézzelfoghatóbb hozzáadott értéke az energiafelhasználás csökkentése, ami nem csak környezeti, hanem egyre erősebb gazdasági érdek. Az épületek a teljes energia fogyasztás jelentős részét teszik ki [1]. Egy jól üzemeltetett intelligens

épületautomatizálási rendszer ezt az arányt szignifikánsan csökkenteni tudja. A szén-dioxid-kvóták miatt ez a kérdés már nem csak a végfelhasználókat érinti, hanem egy komoly stratégiai érdek.

A HVAC-rendszerek az épületek energiafelhasználásának tipikusan a legnagyobb tételét teszik ki. Intelligens szabályozással ez lényegesen csökkenthető, az igények pontosabb előrejelzésével, figyeli a helységek foglaltsági mintáit, a külső időjárási tényezők aktuális és várható paramétereit és az aktuális energiaárakat [2]. A rendszer nem a jelenlegi hőmérsékletet kezeli, hanem modellezi, mire lesz szükség egy óra múlva, és már most megteszi a szükséges lépésket. A hőkomfort és az energiatakarékosság, amelyek sokáig egymásnak ellentmondó céloknak tűntek, így egyszerre valósítható meg.

A gépi tanulás megjelenése az energiamenedzsmentben jelentős előrelépést hozott. Az adatvezérelt rendszerek energiafogyasztási mintázatokat azonosítanak, és proaktívan módosítják az épület működését [3]. Az adatvezérelt megközelítés különösen nagy épületeknél hozza a legjelentősebb megtakarítási eredményeket, ahol a mintázatok komplexek és a megtakarítási potenciál nagy.

A világításvezérlés kevésbé látványos tétel, de az összkép szempontjából nem elhanyagolható. Jelenlétérzékelők, természetes fény mérése, automatizált fényerőszabályozás: ezek kombinációja nemcsak az energiafelhasználást csökkenti, hanem a vizuális komfortot is javítja [4], [15]. Irodaépületeknél, ahol a munkavállalói teljesítmény mérhető, ez az összefüggés közvetlenül gazdasági értékké fordítható.

Az árnyékolástechnika az egyik leginkább alulértékelt energetikai eszköz. A napenergia-bevitel megfelelő szabályozása egyszerre csökkenti a nyári hűtési csúcsokat és a téli fűtési igényt [5]. Nagy üvegfelületű épületeknél ez különösen kritikus dimenzió.

A megújuló energiaforrások integrációja az intelligens épületeket teljesen új szerepbe hozza. Az épület aktív energiapiaci szereplővé válik. A napelemes termelés, az akkumulátoros tárolás és az elektromos töltőinfrastruktúra koordinálása olyan feladat, amelyre hagyományos épület nem képes [6]. A smart grid-del összekötött intelligens épület alkalmazkodik a hálózati terheléshez, felesleges termelését visszaadja, és kedvező árakon tárol.

Komfort és felhasználói élmény

A modern rendszerek valóban képesek megtanulni a felhasználói szokásokat, és ehhez igazítani az üzemeltetési paramétereket [7]. Ez az alkalmazkodóképesség azonban nem korlátlan, a technológia nyújtotta lehetőségek és a felhasználói elvárások közötti eltérések olykor feszültséget eredményezhetnek.

A domotika rendszerek komfortfunkciói mára már jóval túlmutatnak az egyszerű hőmérséklet beálltáson, a hőkomfort nem egyenlő a hőmérséklettel. A páratartalom, a légáramlás, a sugárzó felületek és a szemközti fal hőmérséklete mind befolyásolja, hogy valaki melegnek vagy hidegnek érzi a teret [2]. Az intelligens HVAC-rendszerek ezeket a tényezőket egyszerre kezelik, és valós idejű visszajelzés alapján finomhangolnak. A kutatások ezt összefüggésbe hozzák a munkavállalói produktivitás mérhető javulásával is.

A levegőminőség-figyelés az utóbbi években felértékelődött, és ebben a COVID-19 járványnak komoly szerepe volt. A beltéri levegő minősége, a szén-dioxid-szint, az illékony vegyületek, a finom részecskék: ezek egészségügyi következményei korábban keveset szerepeltek az épülettervezési vitákban [8], [16]. A szakirodalom részletesen tárgyalja, hogyan integrálhatók az intelligens szellőztetési stratégiák a domotika rendszerekbe, és milyen

mértékben csökkenthető ezzel a felesleges energiaveszteség [16]. Az igény szerinti szellőztetés egyszerre egészségügyi és energetikai megoldás.

Az emberközpontú világításvezérlés a komforttechnológia egyik legkomplexebb területe. A napszakhoz igazodó, dinamikus fényvezérlés a látást segítésén túl, igazoltan befolyásolja a biológiai ritmust, a koncentrációt és a pszichológiai jóllétet [9]. Az optimalizálás itt nem fizikai paraméterekről szól elsősorban, hanem az emberi szervezet reakcióiról. Ez személyre szabottabb és árnyaltabb megközelítést igényel és jóval összetettebb, mint amit egy egyszerű fényerő-szabályozó biztosíthat

A mesterséges intelligencián alapuló alkalmazkodóképesség ígéretes, de nem problémamentes. Az intelligens rendszerek megtanulják a felhasználói szokásokat, és képesek erre alapozva döntéseket hozni [10]. Azonban a túlzott automatizálás csökkenti a felhasználók kontrollérzését, és elidegenedést kelthet. Az adatvédelmi kérdések, különösen a jelenlétérzékelés és a viselkedési adatok gyűjtése, szintén etikai mérlegelést igényelnek.

Biztonság és védelem

Az intelligens épületek biztonsági infrastruktúrája az elmúlt évtizedben teljesen átalakult. Ami korábban párhuzamos, egymástól független rendszerek halmaza volt, ma egyetlen integrált architektúrában működik: videómegfigyelés, beléptető rendszerek, mozgásérzékelés, tűzjelzés és digitális vezérlőrendszerek egyszerre [13]. Az integráció növeli a hatékonyságot, de a potenciális támadási felületet is.

Az integrált rendszerek egyik legnagyobb előnye valós idejű reagálóképesség. Automatizált vészhelyzeti protokollok, valós idejű riasztás, azonnali beavatkozás: ezek drasztikusan lerövidítik az időt, amely egy incidens azonosítása és kezelése között eltelik [17]. Tűzriasztásnál, jogosulatlan belépési kísérletnél vagy műszaki meghibásodásnál ez a reakcióidő biztonsági és vagyoni szempontból is kiemelt jelentőségű.

A mesterséges intelligencia a biztonsági alkalmazásokban, kiváltképpen az anomáliadetektálásban és a videóelemzésben, meghatározó fejlődést hozott. Az algoritmusok szokatlan eseményeket észlelnek, és figyelmeztetést adnak még azelőtt, hogy az incidens bekövetkezne [18]. Az emberi hibákból eredő kockázatok csökkentése ebben az összefüggésben különösen értékes.

A zero trust és a IoT-eszközök sérülékenysége is szorosan kapcsolódnak ehhez a területhez, részletes bemutatásuk azonban az 6.3 fejezetben történik.

A személyi kockázatok témakör szorosan kapcsolódik ehhez a területhez, részletes bemutatásuk azonban az 6.4 fejezetben történik.

Fenntarthatóság és ESG szempontok

A fenntarthatóság mára az intelligens épületek tervezésének megkerülhetetlen keretelemévé vált. Az ESG-szempontok beépülésével ez épületek energia fogyasztásának, és ezzel együtt a széndioxid lábnyomának csökkentése egyszerre befektetői, szabályozói cél. Az ESG-szempontok ingatlanpiaci hatása ma már mérhetően kimutatható. Egy rosszul minősített épület nehezebben adható bérbe, nehezebben hitelezik meg, és veszít az értékéből [19]. Ez azt jelenti, hogy az intelligens épülettechnológiákba való beruházás megtérülési kalkulációjában ma már nemcsak az energiaszámla szerepel.

A LEED, BREEAM és WELL minősítési rendszerek egyre pontosabban számszerűsítik az intelligens automatizálási megoldások hozzájárulását [20]. A minősítési szem-

pontrendszer az iparági elvárások fejlődését is alakítja, és ösztönzi a fejlesztőket, hogy korszerű domotika megoldásokat alkalmazzanak. A kedvező minősítés megszerzése az egyik leghatékonyabb eszköz, amellyel a szabályozói szándék a beruházói döntésekbe beépül.

Ugyanakkor a fenntarthatósági célok és a megvalósítás valósága között máig komoly szakadék tátong. Magas beruházási költségek, interoperabilitási hiányosságok, technológiai avulás: ezek különösen a meglévő épületállomány esetén valódi akadályok [19]. A fenntarthatóság, mint cél és a megvalósítás közötti feszültség az intelligens épületek fenntarthatósági ambícióinak egyik megoldatlan kihívása.

MESTERSÉGES INTELLIGENCIA ÉS ADATVEZÉRELT ÉPÜLETIRÁNYÍTÁS

A HVAC-rendszerek energiaoptimalizálása az a terület, ahol az AI a legmarkánsabb eredményeket produkálja. A gépi tanulási algoritmusok az aktuális hőmérséklet monitorozása mellett az épület teljes energiafelhasználási profilját is elemzik, a felhasználói szokásokat, az időjárási előrejelzéseket, az energiaárak napi változásait [2]. Ennek alapján mindig egy lépéssel a bekövetkező esemény előtt járnak és meg tudják indítani a megelőző intézkedéseiket. Ez a különbség a hagyományos termosztát és egy valódi intelligens rendszer között.

A prediktív vezérlés lényege a megelőzés, amíg a hagyományos rendszer a már bekövetkezett változásra válaszol, az előrejelző algoritmus a várható változást modellezi, és megelőző lépést tesz [3]. A fogyasztási csúcsok csökkentése és az energiaelosztás optimalizálása nemcsak az épület hatékony működése miatt fontos, hanem a villamosenergia hálózat terhelésének kiegyensúlyozásában is egyre nagyobb szerepet kap, különösen a smart grid rendszerek terjedésével.

A prediktív karbantartás az AI alkalmazások egyik leginkább alulértékelt területe. A szenzorhálózatokból érkező adatfolyamok elemzésével az algoritmusok képesek azonosítani a meghibásodások korai jeleit, sokszor hetekkel azelőtt, hogy a probléma láthatóvá válna [4]. A megelőző karbantartás ezt a kockázatot érdemben csökkenti.

Az anomáliadetektálás az a pont, ahol az energetikai és a kiberbiztonság találkozik. A normál működési mintáktól eltérő energiafogyasztás, szokatlan hálózati forgalom vagy gyanús hozzáférési kísérlet egyaránt utalhat rendellenes működésre [5].

A digitális iker technológia talán a legösszetettebb és egyben a legtöbb potenciállal rendelkező terület. Az épület valós idejű virtuális modellje lehetővé teszi, hogy különböző beavatkozásokat teszteljünk anélkül, hogy az éles rendszerben kísérleteznénk [6]. Energiaoptimalizálási változtatásokat, karbantartási forgatókönyveket, szélsőséges üzemi helyzeteket lehet szimulálni, és a várható hatásokat megvizsgálni egy virtuális térben [18]. Ez az üzemeltetési kockázatkezelés egy teljesen új szintje.

A felhőalapú feldolgozás erős centralizált elemzésnél, de ahol alacsony válaszidő kritikus, például a vészhelyzeti rendszereknél, a helyi adatfeldolgozás nem lehet mással kiváltani [7] [17]. Az edge computing adatvédelmi szempontból is előnyösebb mint a felhő alapú adatfeldolgozás, így az üzemeltetés közben gyűjtött érzékeny adatok nem hagyják el a helyszínt.

Az önoptimalizáló épületek hatékonyságot és kényelmet biztosítanak [8], de az üzemeltetői kompetencia és a beavatkozási képesség megőrzése tudatos tervezési döntést igényel. Amit a rendszer automatikusan kezel, azt az ember fokozatosan elfelejti kezelni. Ez hosszú távon üzemeltetési sebezhetőséget is teremthet.

A gépi tanulási modellek döntéshozatalának átláthatósága, különösen mélyebb neurális hálózatok esetén, nem tekinthető evidensnek [9]. A modellek megbízhatósága változó üzemi körülmények között ingadozhat, és fennáll a veszélye annak, hogy kiberbiztonsági támadás célpontjává váljon.

KIHÍVÁSOK ÉS KORLÁTOK

Interoperabilitási problémák

Az épületautomatizálás korai éveiben gondot okozott, hogy különböző gyártók eszközei egyáltalán nem tudtak egymással kommunikálni [1]. A különböző gyártók eltérő protokolokat és vezérlési logikákat alkalmaztak, ami a mai napig kompatibilitási problémákat okazhatnak. A nagyobb platformok rendkívül szigorú feltételeket szabnak és csak az ennek megfelelő kompatibilis eszközök kapják meg az adott rendszer minősítését. Az iparágak korai szabvány választása a mai napig meghatározzák az egyes területek milyen rendszerre építenek. Ezért egy központi platformon működő rendszer átjáró kapukon keresztül kommunikáló alplatformokat fog össze. Például a világítási rendszerek tradicionálisan Dali szabványra épülnek a HVAC rendszerek modbus rendszerűek, a központi rendszer pedig KNX.

A KNX, a BACnet és a Modbus megjelenése az iparági egységesedés felé tett lépés volt, de a valóság ennél szövevényesebb. A gyártók saját kiterjesztéseket fejlesztenek, zárt platformokat tartanak fenn, és az integrációs munkát végül az üzemeltetőre hárítják [2], [3].

A vendor lock-in jelenség ebből következik és hosszútávon a legnagyobb kockázatot jelenti. Ha egy épület üzemeltetési rendszere egyetlen gyártó ökoszisztémájára épül, az üzemeltető elveszíti a szabad bővítés lehetőségét, és beszorul az adott keretrendszer határai közé [4]. Minden frissítés, minden bővítés, minden javítás ugyanattól a szállítótól érkezik, annak feltételei és árazása alapján. Ez a kötöttség különösen hosszú üzemeltetési ciklussal rendelkező épületek esetén lehet kockázatos.

A felhőalapú és edge architektúrák elterjedése egy újabb dimenzióval bővítette a kompatibilitási problémákat. Az eltérő adatkezelési modellek, programozási interfészek és kommunikációs protokollok az amúgy is heterogén épületmenedzsment-környezetet tovább bonyolítják [5]. Az iparág konszenzusa szerint a nyílt szabványok és az interoperábilis architektúrák felé kell haladni, azonban a megvalósítás üteme mégis messze elmarad az elvárásoktól.

Gazdasági korlátok

A domotika rendszerek szélesebb körű terjedését a kezdeti viszonylag magas beruházás korlátozza. A telepítési költségek, különösen meglévő épületek esetén, valóban számottevők [6]. Egy retrofit épület elektromos hálózata, csőrendszere, épületgépészete sokszor nem kompatibilis azzal, amit egy modern domotika rendszer megkövetel [8]. A megtérülési idő tipikusan meghaladja azt a horizontot, amelyen belül egy egyszeri döntéshozó gondolkodik. Közintézményi és önkormányzati környezetben ez az megtérülési időtáv visszafogott adoptációt okoz.

A megtérülési számítás önmagában is komplex feladat. Az energiaárak változékonysága, a kihasználtsági minták, a karbantartási igény és a rendszer várható élettartama mind befolyásolják a megtérülési időt [7]. Bizonytalan energiaárak alakulása és a hosszú

megtérülési idő mellett a kockázatkerülő szervezetek beruházási hajlandósága kifejezetten alacsony.

A technológiai avulás az a kockázat, amelyet a beruházási kalkulációkban a legtöbbször figyelmen kívül hagynak. Szoftverfrissítési igények, új biztonsági szabványok, hardveres kompatibilitási problémák, ezek folyamatos fenntartási költségeket termelnek [9]. Moduláris, nyílt felépítéssel ez mérsékelhető, de nem szüntethető meg teljesen. Egy épület harminc évig üzemel, de a mögötte lévő technológia öt-tíz évenként generációt vált, amivel érdemes lépést tartani.

Az ESG-elvárások intézményesülése, az energiaárak tartós emelkedése és a fenntarthatósági minősítések ingatlanpiaci hatása együttesen olyan nyomást teremt, amely fokozatosan átírja a kalkuláció megtérülési idejét [10]. Ami ma hosszú megtérülési időnek tűnik, holnap versenyképességi kérdéssé válhat.

Kiberbiztonsági kockázatok

Az intelligens épületek kiberbiztonsági helyzete az internetkapcsolat megjelenésével teljesen megváltozott. Az épületüzemeltetési infrastruktúra korábban fizikailag elszigetelt volt, és ebből adódóan nem volt kitéve külső támadásoknak [13]. A rendszerek elérhetők a hálózatról, és ezzel együtt sebezhetővé is váltak. Ezek a támadások az adatlopás mellett fizikai károkat is okozhatnak a berendezésekben.

A sérülékenységek spektruma széles és jól ismert: nem megfelelő hitelesítés, elavult szoftverek, titkosítatlan kommunikáció, gyártóspecifikus kiskapuk [17]. Az intelligens épületek különösen vonzó célpontok zsarolóvírusos támadásokhoz, mert az üzemfolytonosság kényszere gyors döntést kényszerít ki. Egy kórháznál vagy adatközpontnál ez a nyomás óriási, és a támadók ezt használják ki.

A fizikai és a digitális infrastruktúra integrációjából fakadó kockázat az, ami az intelligens épületek kiberbiztonságát veszélyezteti. Egy HVAC-rendszer manipulációja egészségügyi következményekkel járhat. Egy tűzjelzési rendszer feltörése emberéleteket veszélyeztethet. Egy beléptető rendszer kompromittálása fizikai behatolást tesz lehetővé [18]. Ez nem informatikai probléma, amelyet az IT-részleg kezel: épületbiztonsági probléma, amelynek digitális forrása van. Ez megköveteli, hogy a kiberbiztonság együtt kezelje az informatikai veszélyeket az épületbiztonsági kérdésekkel.

Az IoT-eszközök biztonsági gyengesége legtöbbször az eszközök felépítéséből és a természetéből fakad. Korlátozott számítási kapacitás, hosszú frissítési ciklus, gyártói támogatás idő előtti megszűnése, ezeken szoftverfrissítéssel nem lehet változtatni [14]. Egy épületben évtizedekig működő, vegyes korú és gyártójú eszközpark egységes biztonsági keretbe szervezése elsősorban hálózati architektúra kérdése. Szegmentálás, zero trust megközelítéssel és folyamatos monitorozással lehet a helyzetet a legjobban kezelni. A módszertan jól ismert: titkosítás, többfaktoros azonosítás, hálózati szegmentálás, rendszeres frissítések, anomáliadetektálás [21]. A zero trust architektúra szemlélete megjelent az épületüzemeltetési kontextusban is, amely nem feltételez megbízhatóságot egyetlen hálózati szereplővel szemben sem, és minden hozzáférési kérelmet hitelesít.

A kiberbiztonság tehát nem informatikai kérdés, hanem az intelligens épületek üzemeltetésének legkritikusabb területe [13], [21]. Az épületüzemeltetőknek olyan kompetenciákat kell fejleszteniük, amelyek korábban nem tartoztak a munkájukhoz. A kulturális és

szervezeti változás mindig lassabb, mint a technológiai fejlődés. Ez az eltérés ma az egyik legnagyobb biztonsági rés.

Humán tényezők

Az intelligens épületek biztonsági szintje nem csupán technológiai kérdés, hanem szervezeti kockázatokat is jelent. A gyártóspecifikus zárt platformok, a heterogén IoT-környezetek és az egységes szabványok hiánya olyan komplexitást teremtenek, amellyel a legtöbb üzemeltető nehezen birkózik meg [14], [21]. A biztonsági kultúra és a szervezeti felkészültség sokszor fontosabb, mint az alkalmazott technológia. A legfejlettebb automatizálási rendszer sem működik jól, ha a felhasználó nem tudja kezelni, nem érti a működését és ezáltal bizalmatlan a rendszer megfelelő működésével kapcsolatban és kerüli a használatát. Tehát az elfogadás éppúgy befolyásolja a software ergonómiája, mint a technológia megbízhatósága. A tervezés során az ember-gép interakcióra kiemelt figyelmet kell fordítani [22]

A túlzott komplexitás az intelligens rendszerek egyik leggyakoribb gyengesége. Nehezen áttekinthető felületek, átláthatatlan vezérlési logikák, érthetetlen visszajelzések: ezek nem esztétikai hibák, hanem üzemeltetési kockázatok [19]. Azok a rendszerek, a melyek csak teszik a dolgukat és nem jeleznek vissza a felhasználónak mit miért csinálnak alacsonyabb elfogadottsági mutatókkal rendelkeznek [23].

A digitális kompetenciák hiánya különösen közintézményi és lakossági környezetben okoznak gondot [20]. Az összetett domotika rendszerek kezelése tudást feltételez, ami sokszor nem áll rendelkezésre. A nem megfelelően beállított vagy elhanyagolt rendszer nemcsak rosszul működik, hanem sebezhető is.

Az adatvédelmi kérdéseket nem lehet technikai problémaként kezelni. A jelenlétérzékelés, a viselkedési minták rögzítése, az energiafogyasztási adatok tárolása: ezek GDPR-kérdések és etikai kérdések egyszerre. Az a döntés, hogy egy épületrendszer milyen adatokat gyűjt, túlmutat a mérnök hatáskörén [24].

Az intelligens épületek hosszú távú fenntarthatóságát nem kizárólag a technológiai fejlettség határozza meg, hanem az is, hogy a felhasználók mennyire képesek és hajlandók együttműködni ezekkel a rendszerekkel. A felhasználóbarát kezelőfelületek, a rugalmas működési logika és a megelőzésközpontú adatvédelmi szemlélet mellett ezért kiemelt jelentőségű az emberi elfogadás és a támogató szervezeti kultúra, mivel ezek alapvetően befolyásolják a rendszerek hatékony és fenntartható működését.

KÖVETKEZTETÉSEK

A domotika rendszerek az elmúlt hat évtizedben hatalmas fejlődésen mentek keresztül, az egyszerű elektromechanikus automatizálástól egészen az adatvezérelt, gépi tanuláson alapuló önoptimalizáló mesterséges intelligenciával támogatott rendszerekig. Ez a folyamat jól tükrözi a technológiai lehetőségek folyamatos bővülését és a társadalmi elvárások változását. A technológia alapjaiban íta át az ember-gép interakciót. A domotika rendszerek ma már az intelligens épületek idegrendszerét alkotják.

Az energiahatékonyság, a felhasználói komfort, a fenntarthatóság és a biztonság korábban egymástól független területek voltak, amelyeket külön rendszerek kezeltek. Ma ezek egyetlen, integrált infrastruktúrában találkoznak [1], [2]. Ez az összevonás rengeteg

lehetőséget teremt, de komoly felelősséget is: egy rosszul tervezett vagy elhanyagoltan üzemeltetett intelligens rendszer nemcsak hatékonyságveszteséget okoz, hanem biztonsági kockázatot is jelent.

A mesterséges intelligencia, az IoT, az edge computing és a digitális iker technológiák összefonódása alapvetően átírja, mit értünk optimalizálás alatt [3]. Ahogy a rendszerek egyre önállóbbak lesznek, a felülbírálati és beavatkozási képesség megőrzése egyre fontosabb kérdéssé válik [4]. A felhasználónak ebben a folyamatban nem szabad passzív megfigyelővé válnia.

Az összekapcsoltság megnöveli a kiberbiztonsági fenyegetettséget, azáltal, hogy a rendszer nyitott a külvilág felé, és a sebezhetőség több fronton is megnyílik. Egyetlen kompromittált IoT-eszköz komoly rendszerszintű következményekkel járhat, és mivel a digitális és fizikai rétegek egymásba fonódnak, a támadások fizikailag károkat is képesek tenni a rendszerben [5]. A kiberbiztonsági szemlélet beépítése az épületüzemeltetésbe ezért ma már szükséges alapkövetelmény. Az interoperabilitás, a zero trust elvek következetes alkalmazása és a nyílt szabványok előnyben részesítése együttesen teremtik meg azt az alapot, amelyre megbízható rendszerek építhetők [6].

Az ESG-szempontok térnyerése az intelligens épületek gazdasági megítélését is megváltoztatta. Az energiafelhasználás, a szén-dioxid-kibocsátás és a minősítési pontszámok ma már közvetlenül hatnak az ingatlan értékére és finanszírozhatóságára [7]. A domotika rendszerek tehát egy épület hosszú távú értékét meghatározó infrastrukturális feltétel.

Az intelligens épületek fejlődése nem ér véget. A következő évek valószínűleg tovább mélyítik az autonóm működést, és egyre több döntés kerül az algoritmusok hatókörébe. Hogy ez valóban jobb épületeket jelent-e, az nem csupán technológiai kérdés: függ az üzemeltetési kultúrától, a szabályozási környezettől és attól, hogy a tervezők és fejlesztők mennyire veszik komolyan az emberi tényezőt. A domotika rendszerek önmagukban csak eszközök. Hogy mire használják őket, az rajtunk múlik.

FELHASZNÁLT IRODALOM

[1] A. H. Buckman, M. Mayfield, and S. B. M. Beck, “What is a smart building?,” Smart and Sustainable Built Environment (2014) 3 (2): 92–109. doi:10.1108/SASBE-01-2014-0003

[2] A. I. Dounis and C. Caraiscos, “Advanced control systems engineering for energy and comfort management in a building environment—A review,” Renewable and Sustainable Energy Reviews, vol. 13, no. 6–7, pp. 1246–1261, 2009. doi: 10.1016/j.rser.2008.09.015.

[3] United Nations Environment Programme, 2022 Global Status Report for Buildings and Construction, Nairobi, Kenya, 2022. [Online]. Available: https://globalabc.org/resources/publications/2022-global-status-report-buildings-and-construction (letöltve: 2026.01.02.)

[4] S. Wang, Intelligent Buildings and Building Automation. London, U.K.: Spon Press, 2010.

[5] J. Gubbi, R. Buyya, S. Marusic, and M. Palaniswami, “Internet of Things (IoT): A vision, architectural elements, and future directions,” Future Generation Computer Systems, vol. 29, no. 7, pp. 1645–1660, 2013. doi: 10.1016/j.future.2013.01.010.

[6] W. Shi, J. Cao, Q. Zhang, Y. Li, and L. Xu, "Edge Computing: Vision and Challenges," IEEE Internet of Things Journal, vol. 3, no. 5, pp. 637–646, 2016. doi: 10.1109/JIOT.2016.2579198.
[7] Y. Pan and L. Zhang, "Roles of artificial intelligence in construction engineering and management: A critical review and future trends," Automation in Construction, vol. 122, 2021, Art. no. 103517. doi: 10.1016/j.autcon.2020.103517.
[8] D. Clements-Croome, Intelligent Buildings: Design, Management and Operation. London, U.K.: ICE Publishing, 2013.
[9] A. Humayed, J. Lin, F. Li, and B. Luo, "Cyber-Physical Systems Security—A Survey," IEEE Internet of Things Journal, vol. 4, no. 6, pp. 1802–1831, 2017. doi: 10.1109/JIOT.2017.2703172.
[10] S. Sicari, A. Rizzardi, L. A. Grieco, and A. Coen-Porisini, "Security, privacy and trust in Internet of Things: The road ahead," Computer Networks, vol. 76, pp. 146–164, 2015. doi: 10.1016/j.comnet.2014.11.008.
[11] C. Alcaraz and S. Zeadally, "Critical infrastructure protection: Requirements and challenges for the 21st century," International Journal of Critical Infrastructure Protection, vol. 8, pp. 53–66, 2015. doi: 10.1016/j.ijcip.2014.12.002.
[12] Cs. Kollár, „A biztonság fontosabb fogalmai," Biztonságtudományi Szemle, vol. 7, no. 1, pp. 15–23, 2025. doi: 10.12700/btsz.2025.7.1.15
[13] ISO/IEC 14543-3, Information Technology — Home Electronic System (HES) Architecture — Part 3: Communication Layers — KNX Net/IP, International Organization for Standardization, Geneva, Switzerland.
[14] W. Bolton, Programmable Logic Controllers, 6th ed. Oxford, U.K.: Newnes, 2015.
[15] C. E. Ochoa, M. B. C. Aries, and J. L. M. Hensen, "State of the art in lighting simulation for building science: A literature review," Journal of Building Performance Simulation, vol. 5, no. 4, pp. 209–233, 2012. doi: 10.1080/19401493.2011.558211.
[16] Sz. Márkos, "Intelligens szellőztetési stratégiák a domotika rendszerben," Biztonságtudományi Szemle, vol. 7, no. 4, pp. 41–55, 2025. doi: 10.12700/btsz.2025.7.4.41
[17] ASHRAE Standard 135-2020, BACnet—A Data Communication Protocol for Building Automation and Control Networks. Atlanta, GA, USA: ASHRAE, 2020.
[18] L. Pérez-Lombard, J. Ortiz, and C. Pout, "A review on buildings energy consumption information," Energy and Buildings, vol. 40, no. 3, pp. 394–398, 2008. doi: 10.1016/j.enbuild.2007.03.007.
[19] C. Boje, A. Guerriero, S. Kubicki, and Y. Rezgui, "Towards a semantic Construction Digital Twin: Directions for future research," Automation in Construction, vol. 114, 2020, Art. no. 103179. doi: 10.1016/j.autcon.2020.103179.
[20] A. Pandharipande and D. Caicedo, "Daylight integrated illumination control of LED systems based on enhanced presence sensing," Energy and Buildings, vol. 43, no. 4, pp. 944–950, 2011. doi: 10.1016/j.enbuild.2010.12.018.
[21] S. Rose, O. Borchert, S. Mitchell, and S. Connelly, Zero Trust Architecture, National Institute of Standards and Technology, Gaithersburg, MD, USA: NIST Special Publication 800-207, 2020. doi: 10.6028/NIST.SP.800-207
[22] Cs. Kollár, „A biztonság megjelenése a humán tudományokban (3. rész)," Biztonságtudományi Szemle, vol. 6, no. 4, pp. 1–14, 2024. [Online]. https://biztonsagtudomanyi.szemle.uni-obuda.hu/index.php/home/article/view/524 (letöltve: 2026.02.14.)

[23] Cs. Kollár, „A biztonság megjelenése a humán tudományokban (2. rész)," Biztonságtudományi Szemle, vol. 6, no. 3, pp. 1–12, 2024. [Online]. https://biztonsagtudomanyi.szemle.uni-obuda.hu/index.php/home/article/view/504 (letöltve: 2026.02.14.)
[24] Cs. Kollár, „A biztonság megjelenése a humán tudományokban (1. rész)," Biztonságtudományi Szemle, vol. 6, no. 2, pp. 13–22, 2024. [Online]. https://biztonsagtudomanyi.szemle.uni-obuda.hu/index.php/home/article/view/464 (letöltve: 2026.02.14.)