HADMÉRNÖK
VÉDELEMINFORMATIKA

20. évfolyam (2025) 1. szám 73–85.
DOI: 10.32567/hm.2025.1.4

Farkas Gábor,[1] Fazekas Gábor[2]

Ipari vezérlőrendszerek sebezhetősége

A Modbus protokollon keresztül történő támadások elleni védekezés lehetőségei

Vulnerability of Industrial Control Systems

Defence Possibilities Against Attacks over Modbus Protocol

Absztrakt

A PLC-k és a SCADA-rendszerek már évtizedek óta növelik az ipari rendszerek hatékonyságát azáltal, hogy vezérlésüket könnyen programozható és felügyelhető módon valósítják meg. Napjainkban ezek az eszközök nélkülözhetetlenek, és jelen vannak minden ipari létesítményben, legyen az termelőüzem, energiatermelő egység vagy forgalomirányító rendszer. A technológia fejlődésével lehetőség nyílt ezen rendszerek hálózatba szervezésére, ami tovább fokozta hatékonyságukat, ugyanakkor növelte a kibertámadásoknak való kitettségüket is. Tekintettel arra, hogy a kritikus infrastruktúra számos elemében működtetnek ilyen eszközöket, fontos hangsúlyt fektetni azok támadással szembeni ellenálló képességére. Tanulmányunkban górcső alá vesszük a jellemző támadási pontokat és az azok védelmére tett kísérleteket. Célunk átfogó képet adni a sérülékenység okairól és a lehetséges védelmi megoldásokról, továbbá bemutatni egy általunk megvalósított, AI-alapú védelmi lehetőséget, ami hozzájárulhat az ipari rendszerek védelméhez és prediktív karbantartásához.

Kulcsszavak: PLC, SCADA, kibertámadás, kritikus infrastruktúra, AI

[1] Doktori hallgató, Nemzeti Közszolgálati Egyetem Katonai Műszaki Doktori Iskola, e-mail: farkas.gabor.csp@gmail.com
[2] Doktori hallgató, Nemzeti Közszolgálati Egyetem Katonai Műszaki Doktori Iskola, e-mail: fazekg@gmail.com

Abstract

For decades, PLCs and SCADA systems have been enhancing the efficiency of industrial systems by enabling their control in a way that is easily programmable and monitorable. Today, these tools are indispensable and present in every industrial facility, whether it be a manufacturing plant, power generation unit or traffic control system. With technological advancements the networking of these systems has become possible, further increasing their efficiency. However, this has also heightened their exposure to cyberattacks. Given that many elements of critical infrastructure rely on these devices, it is crucial to emphasize their resilience against attacks. In our study, we examine the typical attack points and efforts to protect against them. Our goal is to provide a comprehensive overview of the causes of vulnerabilities and potential defense solutions. Furthermore, we aim to present our AI-based defensive solution that we implemented and can provide the opportunity for the protection and predeictive maintenance of industrial systems.

Keywords: PLC, SCADA, cyber-attack, critical infrastructure, AI

Bevezetés

Az ipari vezérlőrendszerek (*industrial control systems,* ICS) fejlődése nagyban hozzájárult az ipari automatizálás elterjedéséhez és hatékonyságának növekedéséhez. Ezek a rendszerek, különösen a PLC-k (*programmable logic controllers* – programozható logikai vezérlő) és a SCADA (*supervisory control and data acquisition* – felügyeleti ellenőrző és adatgyűjtő) rendszerek, központi szerepet játszanak a termelési folyamatok irányításában és felügyeletében. A PLC-k a különböző ipari berendezések vezérléséért felelnek, míg a SCADA-rendszerek távoli hozzáférést és felügyeleti képességeket biztosítanak, lehetővé téve a rendszerek valós idejű monitorozását és irányítását. A technológiai fejlődésnek köszönhetően ezek a rendszerek egyre inkább hálózatba szerveződnek, ami lehetővé teszi a távoli hozzáférést és irányítást, egyúttal növeli a kibertámadások kockázatát is. A SCADA-rendszerek rendkívül lényegesek a kritikus infrastruktúrák szempontjából, azok kibervédelme kulcsfontosságú, hiszen a működésükben fellépő zavarok súlyos gazdasági és biztonsági következményekkel járhatnak.[3] A kiberbiztonsági kihívások nehézségét tovább fokozza az Ipar 4.0 keretében megvalósuló, a rendszerelemek teljes mértékű hálózatba kapcsolása, többek között az Internet of Things (IoT) elterjedése. Ilyen módon globális méretű hálózatok alakulnak ki, amelyek növelik a támadási felületet. A támadások egyre gyakoribbak és összetettebbek, különösen az olyan célzott támadások, mint a Stuxnet, amely komoly károkat okozhat fizikai infrastruktúrákban is.[4] Tanulmányunk célja, hogy bemutassa a PLC-k és a SCADA-rendszerek főbb sebezhetőségeit, a támadási módszereket és a védekezési lehetőségeket. Különösen a kritikus infrastruktúrák biztonsága áll a középpontban, és arra törekszünk, hogy átfogó képet adjunk a lehetséges megoldásokról, amelyekkel megvédhetjük ezeket a rendszereket

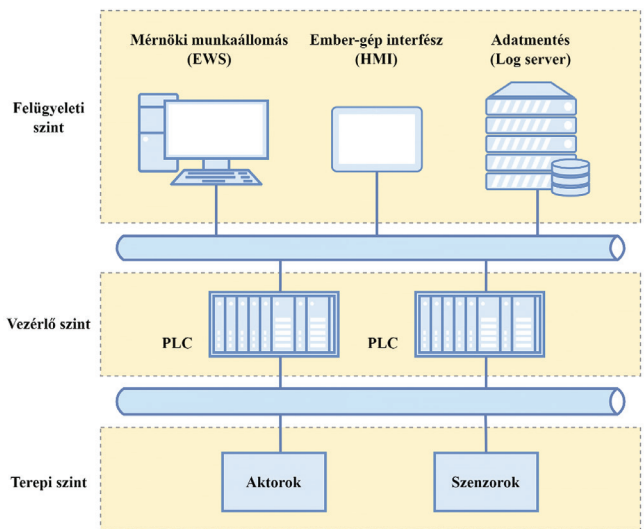
[3] Haig et al. 2009: 48–51.
[4] Sommestad–Ericsson–Nordlander 2010: 1.

a kiberfenyegetésekkel szemben. Ezen túlmenően bemutatunk egy általunk kutatott AI-alapú védelmi megoldást, amely segíthet a Modbus protokollon keresztül történő támadások és szenzormeghibásodások észlelésében. Ez magában foglalja egy konfigurálható neurális hálózat kialakítását, annak tanítását és vizsgálatát.

A PLC-k és a SCADA-rendszerek szerepe

A PLC egy speciális mikroszámítógép, amelyet kifejezetten ipari folyamatok irányítására és automatizálására terveztek.[5] Alapvető funkciója, hogy a szenzoroktól érkező jeleket fogadja, majd ezek alapján meghatározza a szükséges kimeneti állapotokat, amit továbbít a működtető eszközök felé, például motorok, szelepek, fűtőelemek vagy más ipari berendezések vezérlése céljából. A PLC-k tehát közvetlen kapcsolatban állnak az ipari folyamatokkal, és a legfontosabb szerepük ezek közvetlen automatizálása és felügyelete.

A SCADA-rendszerek a PLC-k és más vezérlő rendszerelemek felügyeletére és irányítására szolgálnak. Jellemzően egy központi vezérlő számítógépből, egy operátori állomásból és különböző adatgyűjtő eszközökből épülnek fel (1. ábra).[6] Ezek a megoldások lehetővé teszik, hogy az ipari folyamatokat távolról is figyelemmel lehessen kísérni és szükség esetén beavatkozni. A rendszer összegyűjti az adatokat a terepi eszközökről, és ezeket valós időben továbbítja az operátori felügyeletre. Alkalmazásuk kiterjed az ipari gyártásra, az energiatermelésre, a közművekre, mint például a víz- és gázellátás, valamint a közlekedési hálózatok irányítására is.



1. ábra: Egy általános ICS felépítése
Forrás: Geng et al. 2024: 8388 alapján a szerzők szerkesztése

[5] Allison et al. 2020: 1–2.
[6] Yalçın–Çakır–Ünaldı 2024: 39550–39551.

A PLC-k és a SCADA-rendszerek létfontosságúak az ipari folyamatok hatékony és biztonságos irányítása szempontjából. Lehetővé teszik a folyamatok automatizálását, ennek révén csökkenthetők az emberi hibák, növelhető a termelési hatékonyság, valamint biztosítható a folyamatok tervezett és zavartalan működése. Azonban a nagymértékű hálózatba szervezés egyre nagyobb kihívásokat is jelent, különösen a kiberbiztonsági fenyegetések tekintetében. Az ilyen rendszerek korábban zárt hálózatban működtek, azonban a modern ipari trendek fokozott hálózati összekapcsolódást eredményeztek, ezáltal növelve a támadási felületet, így különösen érzékennyé váltak a kibertámadásokra.[7] A Stuxnet-támadás például rávilágított arra, hogy a PLC-k sebezhetősége komoly fenyegetést jelenthet a kritikus infrastruktúrákra. Ebben az esetben a támadók egy kártékony program segítségével manipulálták az urándúsító centrifugák működését, és hosszú ideig észrevétlenül befolyásolták a rendszer működését.[8] Ez az incidens világszerte felhívta a figyelmet arra, hogy az ipari rendszerek támadások elleni védelme létfontosságú.

Az ipari rendszerek sebezhetősége

Az ipari vezérlőrendszerek, főként a PLC-k és a SCADA-k, rendkívül sebezhetők a kibertámadásokkal szemben, különösen az elmúlt évek technológiai fejlődésének köszönhetően. Az eredetileg zárt hálózatokban működő egységek mára egyre inkább kapcsolódnak a globális hálózatokhoz, ami növeli a sebezhetőséget.[9] A legtöbb ipari rendszer tervezésekor nem volt prioritás a kiberbiztonság, hiszen az üzemszerű működés során fizikailag is izolálva volt a külvilágtól.

A kommunikációs protokollok hiányosságai

A SCADA-rendszerek kommunikációs protokolljainak biztonsági hiányosságai kiemelkedő szerepet játszanak a sebezhetőségében. A Modbus, a DNP3 (Distributed Network Protocol 3 – Elosztott hálózati protokoll 3) és más hasonló protokollok eredetileg nem tartalmaztak beépített biztonsági mechanizmusokat, mivel azok zárt hálózati környezetben működtek. A modern ipari rendszerek azonban jellemzően kapcsolódnak az internethez, ezáltal a támadók távoli hozzáférést szerezhetnek, és kihasználhatják a protokollok gyenge pontjait. Ezek a sebezhetőségek lehetővé teszik, hogy a támadók különböző módszereket alkalmazzanak a rendszerek kompromittálására, például a közbeékelődéses támadásokat *(man-in-the-middle),* amelyek során hamis adatokat továbbíthatnak, illetve megváltoztathatják a rendszer által küldött üzeneteket.

[7] Hankó 2023: 147.
[8] Hankó 2023: 157.
[9] Vásárhelyi 2024: 104.

Támadási típusok és kockázatok

Az egyik leggyakrabban alkalmazott támadási módszer a hamis adatinjekciós támadás *(false data injection,* FDI) amelynek során a támadók manipulálják a szenzorok által küldött adatokat, és így megzavarják a PLC-k által vezérelt fizikai folyamatokat.[10] A FDI-támadások különösen veszélyesek, mivel a rendszer továbbra is úgy működik, mintha minden üzemszerű lenne, miközben a valós fizikai környezet eltér a tervezett működéstől. Egy másik jelentős kockázat a vezérlőprogramok vagy a *firmware* manipulációja.[11] A támadók képesek lehetnek arra, hogy rosszindulatú kódokat juttassanak a PLC-kbe, amelyek megváltoztatják a vezérlő programokat.[12] Ez különösen kritikus lehet olyan ipari környezetekben, ahol a rendszerek közvetlenül kapcsolódnak a fizikai eszközökhöz, mint például az energiatermelés vagy a vízszolgáltatás. A Stuxnet-támadás klasszikus példája annak, hogy milyen pusztító hatást lehet kiváltani a sebezhetőségek kihasználásával. Ebben az esetben a támadók rosszindulatú kódot juttattak be a Siemens gyártmányú PLC-kbe, amelyek irányították az iráni urándúsító centrifugákat, és megzavarták azok működését. Az ilyen FDI-támadások viszonylag egyszerűen kivitelezhetők, így meglátásunk szerint jelentős kockázatot hordoznak magukban.

Tervezési hiányosságok és kulturális tényezők

Az ipari rendszerek tervezési hiányosságai gyakran a fejlesztési prioritásokból adódnak. Az ipari vezérlőrendszereket sokszor gépész- és automatizálási mérnökök tervezik, akik elsődlegesen a funkcionális folyamatokra és az automatizálásra összpontosítanak, nem pedig a kiberbiztonságra. Ennek eredményeként a rendszerek gyakran olyan egyszerű megoldásokra támaszkodnak, amelyek nem tartalmaznak megfelelő biztonsági elemeket, mivel ebben a környezetben a biztonsági funkciók hozzáadása növelheti a költségeket, és bonyolultabbá teheti a rendszerek üzemeltetését.[13] A tervezési hiányosságok mellett kulturális tényezők is szerepet játszanak a rendszerek sebezhetőségében. Sok ipari rendszer esetében a kiberbiztonság nem része a vállalati kultúrának, különösen olyan iparágakban, ahol a fő hangsúly a termelési hatékonyságon van. A biztonsági intézkedések bevezetése gyakran költséges és időigényes, így a vezetők és a mérnökök hajlamosak figyelmen kívül hagyni ezeket a kockázatokat. Tapasztalataink szerint az információbiztonsági szempontokat a kivitelezés szűk határideje is háttérbe szoríthatja, így a PLC esetében az alapvető hozzáférést megakadályozó jelszavakat sem állítják be.

[10] Dér 2024: 52–53.
[11] Malchow et al. 2015: 326–327.
[12] Yang–Cheng–Chuah 2018: 2–3.
[13] Patel–Bhatt–Graham 2009: 139.

A kritikus infrastruktúrák kockázatai

A PLC-k és a SCADA-rendszerek sebezhetősége különösen fontos a kritikus infrastruktúrák szempontjából, például az energiahálózatok, a vízellátó és a forgalomirányító rendszerek esetében. Ezek az infrastruktúrák elengedhetetlenek a modern társadalmak működésének aspektusából, amelyekben a kibertámadás hatására fellépő üzemzavar súlyos következményekkel járhat, beleértve az energiaellátás megszakítását, a vízhiányt vagy akár közlekedési káoszt. Az energiahálózatok különösen veszélyeztetettek, mivel ezek függési viszonyban vannak egymással, és így nagyobb eséllyel válnak támadások célpontjává. A tárgyalt rendszerek alapvető fontosságúak az energiatermelés, -elosztás és -fogyasztás szabályozásában.[14] Más területeken fellépő üzemzavar is kritikus lehet, amire jó példa a Maroochy vízszolgáltatót ért támadás, amelyet egy korábbi alkalmazott sikeresen hajtott végre. Ennek során több millió liter szennyvíz ömlött ki a környező területre, ami jelentős környezeti és gazdasági károkat okozott.[15]

Védelmi törekvések

Az ipari vezérlőrendszerek kibertámadások elleni védelme összetett kihívás, amely számos védelmi mechanizmus alkalmazását igényli. A fizikai védelemtől kezdve a tűzfalakon, behatolásészlelő rendszereken (*intrusion detection system,* IDS) át egészen a mesterséges intelligencia (*artificial intelligence,* AI) alapú anomáliadetektálásig számos megközelítés létezik.[16] Az AI-alapú megoldások különösen hatékonynak bizonyulnak, mivel képesek a rendszerek valós idejű monitorozására és az anomáliák automatikus felismerésére, ami potenciális támadásokra utalhat.[17]

Fizikai védelem és hagyományos tűzfalak

Az ipari rendszerek elsődleges védelmi vonala a fizikai hozzáférés ellenőrzése, amely biztosítja, hogy csak jogosult személyek befolyásolhassák a működésüket. Az ilyen rendszerek esetében fontos, hogy a fizikai hozzáférést szigorúan ellenőrizzék, különösen olyan helyeken, mint az erőművek, a víztisztítók vagy a közlekedési csomópontok.[18] Ezen túlmenően a hagyományos hálózati védelmi megoldások, mint például a tűzfalak, továbbra is kulcsfontosságúak. A tűzfalak a hálózati hozzáférést szabályozva megakadályozzák az illetéktelen kapcsolatokat és behatolásokat. Az alapvető csomagszűrő tűzfalaktól az állapotalapú és alkalmazásrétegbeli tűzfalakig a rendszerek különböző hálózati védelmi funkciókat látnak el, amelyek biztosítják, hogy csak a megbízható és engedélyezett forgalom érhesse el az infrastruktúrákat. A fizikai védelem szó szerint is értelmezhető. Léteznek megoldások, amikor valóban fizikailag, közvetlenül

[14] Kralovánszky 2019: 44.
[15] Slay–Miller 2008: 74–75.
[16] Aldossary–Ali–Alasaadi 2021: 742.
[17] Yalçın–Çakır–Ünaldı 2024: 39557.
[18] Bognár–Bonnyai–Vámosi 2019: 98.

kell az eszközön engedélyezni például egy firmware frissítést. Ez nagyban megnehezíti a támadó dolgát, viszont a tervezett műveletet is, így meglátásunk szerint ennek alkalmazását mérlegelni szükséges. Jelentős kockázatú rendszerek esetén érdemes lehet közvetlen emberi beavatkozástól függővé tenni minden jelentős változtatás engedélyezését.

AI-alapú anomália detektálása

A mesterségesintelligencia-alapú megoldások az utóbbi években jelentős fejlődésen mentek keresztül, és ma már kulcsfontosságú szerepet játszanak az ipari rendszerek védelmében. Az AI-alapú megoldások képesek folyamatosan monitorozni a rendszerek működését, és azonosítani azokat a mintákat vagy anomáliákat, amelyek kibertámadásra utalhatnak. Az AI-alapú anomália detektálása különösen hatékony a SCADA-rendszerek esetében, ahol a hagyományos védelmi eszközök, mint például a tűzfalak, nem képesek effektíven észlelni az olyan összetett támadásokat, mint a hamis adatinjektálás. A megfelelően megalkotott AI-modell képes folyamatosan elemezni a SCADA-rendszerek által kezelt adatokat, és összehasonlítani azokat a normál működés során megszokott mintákkal. Ha eltérést észlelnek a szokásos működéstől, akkor riasztást küldhetnek és potenciális támadást jelezhetnek.[19] Véleményünk szerint ez a megoldás az adatkommunikáció jellegére összpontosít, így inkább olyan rendszerekben lehet jól alkalmazni, ahol a tényleges adattartalom nehezen vagy egyáltalán nem hozható összefüggésbe a fizikai folyamat rendeltetésszerű működésével. Más szóval a kommunikáció változó jellegének kiszűrésére alkalmas, mint például a többletadatcsomagok megjelenése.

AI-alapú prediktív védelem

Az AI nemcsak az anomáliák detektálásában játszik szerepet, hanem képes előre jelezni a potenciális támadásokat is. A prediktív analitika révén az egyes AI-architektúrák képesek előre megjósolni a rendszerekben bekövetkező változásokat, és jelezni, ha egy támadás valószínűsíthető. Ez különösen hasznos lehet akkor, ha a fizikai paraméterek, mint például a nyomás, a hőmérséklet vagy a folyadékszintek, kritikusak a működés szempontjából. Ezek a prediktív rendszerek képesek monitorozni a fizikai folyamatokat, és előre jelezni, hogy mikor léphetnek fel rendellenességek, még mielőtt azok ténylegesen megtörténnének. Például egy prediktív algoritmus észlelheti, ha egy folyamat során a nyomás kezd eltérni a normál értékektől, és figyelmeztetést küldhet, mielőtt a rendszer hibába ütközne. Ezáltal a támadások korai észlelése lehetővé válik, még azelőtt, hogy azok jelentős károkat okoznának.[20] Szemben az anomáliadetektálással ez a megoldás az adattartalomra fókuszál. Egy-egy szenzor által mért érték normális trendtől való eltérését képes jelezni.

[19] Yalçın–Çakır–Ünaldı 2024: 39557.
[20] Salehi–Siavash 2021: 7377.

Fizikai modellek alkalmazása

Az AI-alapú védelem másik fontos aspektusa a fizikai környezet modellezése. Az ilyen rendszerek összehasonlítják a folyamatok tényleges fizikai állapotát a számítógépes modellek által előre jelzett állapottal, így képesek felismerni azokat a rendellenességeket, amelyek a támadások eredményeként léphetnek fel. Ez különösen hatékony a hamis adatinjekciós támadások ellen, ahol a támadók megpróbálják megtéveszteni a rendszereket azzal, hogy hamis adatokat küldenek be. A fizikai modellek segítségével a rendszerek képesek felismerni, ha a kapott adatok nem felelnek meg a valós fizikai környezetnek.[21] Az ilyen védekezési módszer különösen hasznos lehet a kritikus infrastruktúrák esetében. A fizikai modellek lehetővé teszik a rendszerek számára, hogy azonnal észleljék a rendellenességeket, és gyorsan reagáljanak a potenciális támadásokra. Véleményünk szerint ez a legkifinomultabb, viszont a legtöbb előkészületet igénylő megoldás, amelyhez a fizikai folyamat pontos ismerete és modellezése nélkülözhetetlen. A folyamat változásakor a teljes modell újraalkotása és az AI-tanítási folyamatok újbóli elvégzése szükséges. A felügyelt folyamat és a kockázatok tükrében szükséges mérlegelni, hogy egy ilyen jellegű többletráfordítás indokolja-e a tárgyalt rendszer kidolgozását és telepítését a védelem fokozása érdekében.

AI-alapú megoldás a Modbus mérgezéses támadásának feltárására

Meglátásunk szerint a különféle védelmi mechanizmusok együttes alkalmazása, valamint azok folyamatos fejlesztése vezet rendszereink sebezhetőségének csökkentéséhez. Ezáltal szükségesnek látjuk ilyen irányú kutatások folytatását, amihez kialakítottunk egy olyan környezetet, amely valós hardveren nyújt lehetőséget a megoldások teszteléséhez. Jelen kutatásunk középpontjában olyan AI-alapú megoldás áll, amely a Modbus kommunikációs protokoll elleni hamis adatinjekciós támadások felismerését és elhárítását szolgálja. A Modbus széles körben használt ipari protokoll, amely eredetileg nem tartalmazott biztonsági mechanizmusokat, így különösen sebezhető az olyan támadásokkal szemben, amelyek során a támadók rosszindulatú módon megváltoztatják a rendszerben továbbított adatokat. Célunk, hogy az ilyen típusú támadások valós idejű felismerésére hatékony, AI-alapú anomáliadetektálási rendszert alkossunk, amely nem befolyásolja egy meglévő rendszer felépítését vagy működését. Más szóval a korábbi struktúra megtartása mellett legyen lehetséges a védelem implementálása. Az előző fejezetben említett védelmi törekvések közül az anomáliadetektálás tűnik a legszélesebb körben alkalmazható megoldásnak. Könnyen integrálható meglévő rendszerbe annak leállítása nélkül, és a tanítási folyamat is egyszerűen elvégezhető. A fizikai folyamat modellezése és a konkrét szenzoradatok ismerete nem szükséges, így egy fokozott védelmet biztosító, mindemellett költséghatékony megoldást kínál.

[21] Salehi–Siavash 2021: 7379.

A Modbus FDI-támadások jellemzői

A Modbus protokoll esetén a hamis adatinjekciós támadások során a támadók megváltoztatják a rendszer által feldolgozott adatokat, így a vezérlőrendszerek helytelen utasításokat hajtanak végre, aminek következménye lehet a folyamatok hibás működése vagy teljes leállása. Mivel a Modbus protokoll alapvetően nem tartalmaz hitelesítési mechanizmusokat, a támadók képesek hamis parancsokat és fals értékeket küldeni a vezérlőrendszereknek anélkül, hogy észlelhető lenne a támadás. Mivel ez a támadási módszer többletcsomagok rendszerbe juttatásával jár, a megjelenése detektálható.

Prediktív adatkezelés

A jellemző támadási lehetőségek bemutatásán túlmenően célunk egy valós megoldás megalkotása, amely egy folyamat szenzorrendszerének modellezését irányozza elő, neurális hálózati megközelítéssel. Ez a védelmi rendszer képes az egyes érzékelők működését valós időben előre jelezni a bemeneti adatok alapján. Jelen modellünk egy nyomásszenzor működését hivatott leképezni, ez egy gőztartály nyomását méri, amely összefüggésben van a rendszer többi paraméterével. Gyakorlatilag egy gőzkazán szabályozását megvalósító folyamatról van szó. Jelen esetben Modbus TCP/IP protokoll hordozza az adatokat, amelyeket az Ethernet-hálózat megcsapolásával olvasunk be, ezzel biztosítva a szenzoradatok valós idejű és megbízható hozzáférését. Maga a kommunikációt figyelő és adatokat kinyerő eszköz az Ethernet-hálózat szempontjából láthatatlan, nem rendelkezik saját identitással, fizikai címmel. A neurális hálózati modellünkhöz használt bemeneti és kimeneti változókat az 1. táblázat foglalja össze.

A hálózat kimenete maga az elvárt gőznyomás értéke, amely a bemeneti paraméterek függvényében alakul. A cél a bemeneti és kimeneti összefüggések azonosítása és előrejelzése annak érdekében, hogy a folyamathoz csatlakoztatott védelmi rendszer a nem várt működést detektálni tudja. Ennek eléréséhez egy perceptronalapú neurális hálózatot alkalmazunk, amely teljesen kapcsolt rétegekből áll.

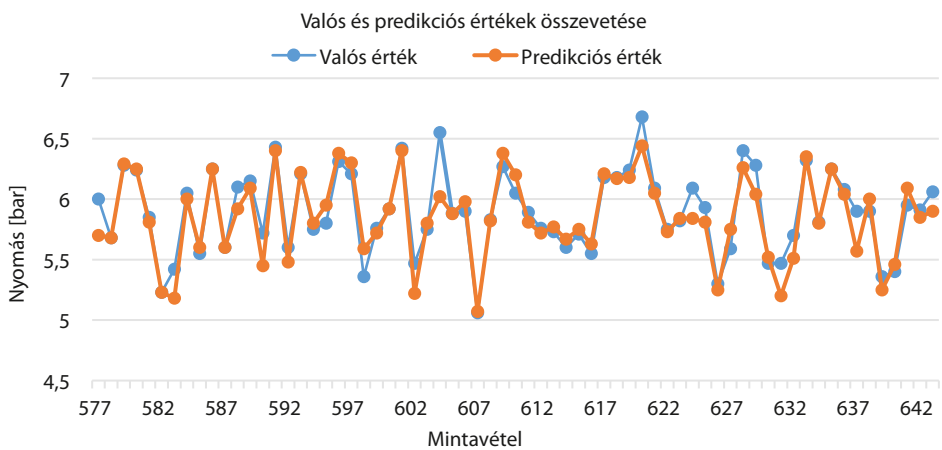
Ez a megközelítés jól kezeli a nemlineáris összefüggéseket, és egyszerű architektúrája révén gyorsan és hatékonyan tanítható. Első körben a tanítási folyamathoz szintetikus adatokat használtunk.

1. táblázat: A perceptron háló bemeneti és kimeneti változói

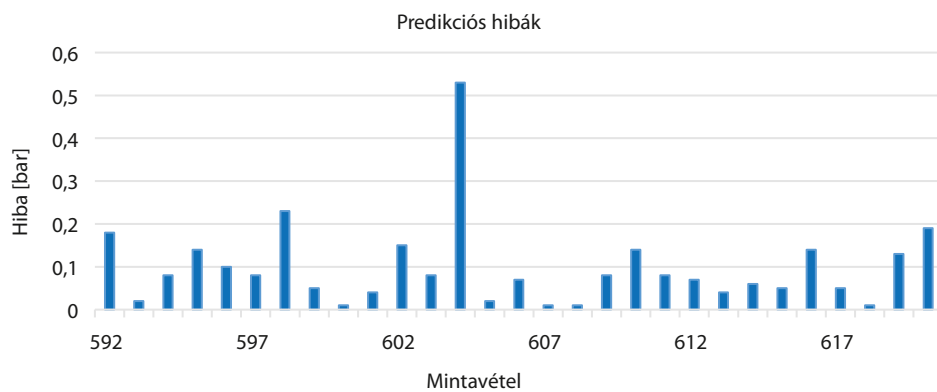
	Paraméter	**Tartomány**	**Dimenzió**
A perceptron háló bemenete	A beáramló víz mennyisége	0–10	l/sec
	A beáramló víz hőmérséklete	0–100	°C
	A kiáramló gőz mennyisége	0–5	kg/sec
	A kiáramló gőz hőmérséklete	100–150	°C
A perceptron háló kimenete	Gőznyomás	0–10	bar

Forrás: a szerzők szerkesztése

Az így létrehozott adatsor egy olyan szcenáriót modellez, amelyben a víz hőmérséklete kezdetben 40 °C, majd lineárisan emelkedik 100 °C-ra 1 óra alatt. A szimulált szenzoradatokra zajjelet szuperponálunk, hogy a szimuláció realisztikus legyen, mivel a valóságos mérési értékek is eltérnek az ideálistól. Továbbá így biztosítható, hogy a tanító és a tesztadatok valamelyest eltérjenek egymástól. Modellünk tanítását követően összevetettük a valós és a prognosztizált értékek időbeni lefutását, ami a 2. ábrán látható. Megállapítható a két adatsor közötti szoros összefüggés, ezáltal a betanított háló alkalmazhatósága. Normális működés esetén a két értéknek jelentős korrelációt kell mutatnia. Lehetnek pontok, ahol nagyobb eltérés tapasztalható, de ezek nem befolyásolják az adatsorok trendjét. A 3. ábrán külön kiemeltük az adatsor azon részét, amelyen a legnagyobb eltérés figyelhető meg. A rendellenes működés detektálása a korrelációban bekövetkező változáson alapszik.



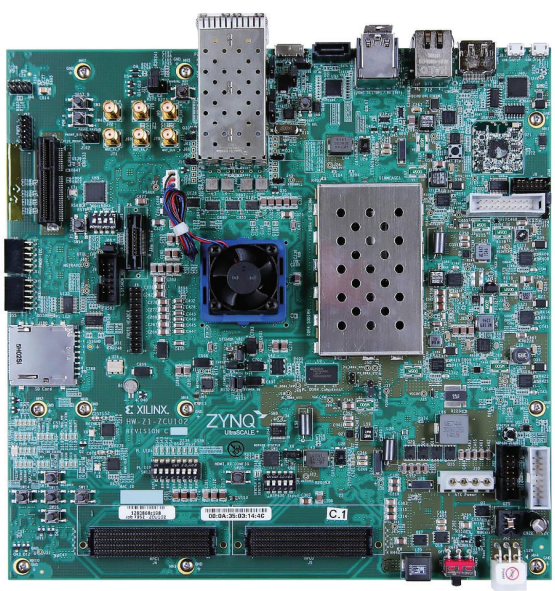
2. ábra: A valós és a modell által számított nyomásérték együtt futása
Forrás: a szerzők szerkesztése



3. ábra: A valós és a predikciós érték közötti eltérések mértéke (maximum: 0,53 bar)
Forrás: a szerzők szerkesztése

A nyomásszenzor modellezésére alkalmazott perceptronalapú megközelítés hatékonyan kezelte a bemeneti változók és a nyomás közötti összefüggéseket, a modell képes volt előre jelezni a szenzor által mért nyomást. További érzékelők perceptron modelljének implementációjával és azok összekapcsolásával fokozhatjuk modellünk integritását. Ezen architektúra dedikált adatvalidációs pontjai a valós szenzoradatok folyamatos korrelációs vizsgálatával lehetőséget biztosítanak az anomáliák és azok tendenciájának felismerésére, valamint a rendszer állapotának folyamatos monitorozására. Valós környezetben a tanítószettek rögzítése és a tanítási folyamat könnyen elvégezhető normális üzem közben.

Továbbá fontosnak tartjuk kiemelni, hogy ez a megoldás nem kizárólag szándékos károkozás esetén adhat jelzést – nem várt hardveres meghibásodásra való figyelmeztetésre is alkalmas. Neuralgikus tulajdonsága a vázolt megoldásnak, hogy a meglévő ipari rendszer megbontása és leállítása nélkül alkalmazható. Meglátásunk szerint ez sok esetben elvárás lehet, mivel egy magasabb biztonsági szint elérése már meglévő rendszer esetén kizárólag annak teljes újratervezésével és kiépítésével lenne lehetséges, ami jelentős költséggel és a folyamatok leállításával jár. A szóban forgó AI-modell hardveres implementációját és tesztelését egy AMD ZCU102 FPGA kártyán (4. ábra) végezzük kutatásunk soron következő fázisaként. Ez lehetővé teszi a kutatást generált adatokon és valós rendszereken egyaránt. Így valós körülmények között is megfigyelhetővé válik annak működése, és további gyakorlati tapasztalatok is gyűjthetők, amelyek egy jól alkalmazható rendszer megalkotását vetítik előre. Az általunk alkotott megoldás nem korlátozódik Ethernet-alapú kommunikációra, így irreleváns a protokollt hordozó fizikai réteg. Más szóval a Modbus protokollt tekintve nem számít, hogy Ethernet, RS232 vagy RS485 a médium, a megoldás ugyanúgy alkalmazható.



4. ábra: AMD ZCU102 FPGA fejlesztőkártya
Forrás: Advanced Micro Devices

A kutatásunkhoz kialakított rendszer hardveres szempontból kielégítő mind a prediktív, mind a fizikaimodell-alapú védelem kialakításához, így kiváló alapot ad a komplexebb megoldások kutatásához és fejlesztéséhez. További célkitűzéseink közé tartozik a perceptron háló optimalizálása, több szenzor modelljének implementálása, illetve az automatizálható szenzortanítási folyamat kidolgozása, amelyek mind hozzájárulnak egy könnyen telepíthető védelmi megoldás megvalósításához.

Összegzés

Az ipari vezérlőrendszerek, különösen a PLC-k és a SCADA-rendszerek kulcsfontosságú szerepet játszanak a modern ipari és kritikus infrastruktúrák működésében, mivel ezek biztosítják a különböző folyamatok automatizálását és távoli irányítását. Azonban a technológiai fejlődés és a hálózati integráció révén ezek a rendszerek sebezhetőbbé váltak a kibertámadásokkal szemben. A kommunikációs protokollok, mint a Modbus és a DNP3, alapvetően nem tartalmaznak biztonsági mechanizmusokat, így könnyen manipulálhatók olyan támadási módszerekkel, mint a hamis adatinjekciós támadások. Az ipari vezérlőrendszerek elleni támadások súlyos következményekkel járhatnak, különösen a kritikus infrastruktúrák esetén, ahol ezek a rendszerek alapvető fontosságúak. A szóban forgó rendszerek védelme nem kizárólag fizikai hozzáférés-ellenőrzést és hagyományos tűzfalakat igényel, hanem fejlett megoldásokat is, mint például az AI-alapú anomáliadetektálás és a prediktív elemzés. Ezek lehetővé teszik a rendszerek valós idejű monitorozását, és képesek felismerni azokat a mintákat és rendellenességeket, amelyek kibertámadásokra utalhatnak. Kialakítottunk egy környezetet, amelyben a vonatkozó kutatások hatékonyan végezhetők. Célunk volt egy perceptron neurális hálózat kialakítása, amely hatékony megoldást kínálhat a Modbus protokollon keresztül történő támadások és esetleges hardveres meghibásodások felismerésére egyaránt. A neurális hálózat architektúráját megalkottuk oly módon, hogy az konfigurálható legyen az ipari rendszerben jelen lévő érzékelők reprezentációjára, és szintetikus adatok segítségével elvégeztük annak tanítását. Rendszerünk jelenleg egy szimulált gázkazán működése közben fellépő szenzoradatok megfigyelésére és jövőbeli állapotbecslésére alkalmas. Kutatásunk következő szakaszában az így megalkotott rendszer hardveres implementációja következik. Összességében elmondható, hogy az ipari rendszerek kiberbiztonsága integrált védelmi megközelítést igényel, amely kombinálja a fizikai és a hálózati biztonságot az AI-alapú rendszerekkel. Az ilyen irányú kutatások és fejlesztések továbbra is elengedhetetlenek, hogy AI-technológiával kiegészülve hatékonyabban védekezhessünk az egyre összetettebb kibertámadások ellen.

Felhasznált irodalom

Aldossary, Lina Abdulaziz – Ali, Mazen – Alasaadi, Abdulla (2021): Securing SCADA Systems against Cyber-Attacks using Artificial Intelligence. *2021 International Conference on Innovation and Intelligence for Informatics, Computing, and Technologies,* 739–745. Online: https://doi.org/10.1109/3ICT53449.2021.9581394

Allison, David et al. (2020): PLC-Based Cyber-Attack Detection: A Last Line of Defence. *IAEA International Conference on Nuclear Security: Sustaining and Strengthening Efforts,* 1–10. Online: https://conferences.iaea.org/event/181/contributions/15513/attachments/9194/12424/CN278_PLC-based-Detection.pdf

Bognár Balázs – Bonnyai Tünde – Vámosi Zoltán (2019): *Kritikus infrastruktúrák védelme I.* Budapest: Dialógus Campus Kiadó.

Dér Attila (2024): Villamosenergia-rendszerek aktuális kiberbiztonsága. *Biztonságtudományi Szemle,* 6(2), 47–55.

Geng, Yangyang et al. (2024): Control Logic Attack Detection and Forensics Through Reverse-Engineering and Verifying PLC Control Applications. *IEEE Internet of Things Journal,* 11(5), 8386–8400. Online: https://doi.org/10.1109/JIOT.2023.3318988

Haig Zsolt et al. (2009): *A kritikus információs infrastruktúrák meghatározásának módszertana*. [H. n.]: ENO Advisory Kft.

Hankó Viktória (2023): SCADA-rendszerek kiberbiztonsága a létfontosságú rendszerelemek tekintetében 1. *Hadmérnök,* 18(3), 145–160. Online: https://doi.org/10.32567/hm.2023.3.10

Kralovánszky Kristóf (2019): A villamosenergia-rendszer kiber- és nemzetbiztonsági kockázatai (1. rész). *Nemzetbiztonsági Szemle*, 7(3), 40–57. Online: https://doi.org/10.32561/nsz.2019.3.4

Malchow, Jan-Ole et al. (2015): PLC Guard: A Practical Defense against Attacks on Cyber-Physical Systems. *IEEE Conference on Communications and Network Security (CNS),* 326–334. Online: https://doi.org/10.1109/CNS.2015.7346843

Patel, Sandip C. – Bhatt, Ganesh D. – Graham, James H. (2009): Improving the Cyber Security of SCADA Communication Networks. *Communications of the ACM,* 52(7), 139–142. Online: https://doi.org/10.1145/1538788.1538820

Salehi, Mohsen – Siavash, Bayat-Sarmadi (2021): PLCDefender: Improving Remote Attestation Techniques for PLCs Using Physical Model. *IEEE Internet of Things Journal,* 8(9), 7372–7379. Online: https://doi.org/10.1109/JIOT.2020.3040237

Slay, Jill – Miller, Michael (2008): Lessons Learned from the Maroochy Water Breach. In Goetz, Eric – Shenoi, Sujeet (szerk.): *Critical Infrastructure Protection.* Boston: Springer, 73–82. Online: https://doi.org/10.1007/978-0-387-75462-8_6

Sommestad, Teodor – Ericsson, Göran N. – Nordlander, Jakob (2010): SCADA System Cyber Security – A Comparison of Standards. *IEEE PES General Meeting,* 1–8. Online: https://doi.org/10.1109/PES.2010.5590215

Vásárhelyi Örs (2024): A veszélyes üzemek információbiztonsági képességeinek fejlesztési lehetőségei napjaink kihívásainak tükrében. *Belügyi Szemle,* 72(1), 89–111. Online: https://doi.org/10.38146/BSZ.2024.1.6

Yalçın, Nesibe – Çakır, Semih – Ünaldı, Sibel (2024): Attack Detection Using Artificial Intelligence Methods for SCADA Security. *IEEE Internet of Things Journal,* 11(24), 39550–39559. Online: https://doi.org/10.1109/JIOT.2024.3447876

Yang, Huan – Cheng, Liang – Chuah, Mooi Choo (2018): Detecting Payload Attacks on Programmable Logic Controllers (PLCs). *IEEE Conference on Communications and Network Security (CNS)*, 1–9. Online: https://doi.org/10.1109/CNS.2018.8433146