DOI: https://doi.org/10.12700/btsz.2025.7.4.27

SAFETY AND SECURITY ENGINEERING OF DIGITAL SUBSTATIONS IN CRITICAL INFRASTRUCTURE

DIGITÁLIS ALÁLLOMÁSOK BIZTONSÁGTECHNIKÁJA A KRITIKUS INFRASTRUKTÚRÁBAN

MÓROCZ Máté[1]

Abstract

The digitalization of power systems has become one of the most significant technological transformations in critical infrastructures over the past decade. During the modernization of transmission and distribution networks, the introduction of digital control and protection technologies particularly those based on the IEC 61850 standard family has fundamentally reshaped the operation of network architectures. In parallel, however, digitalization has also introduced new security and reliability risks. The transition highlights that as the level of automation in energy systems increases, the boundary between physical and cyber security layers becomes increasingly blurred, since substation infrastructure now clearly operates as a cyber-physical system. From a critical infrastructure protection perspective, a key characteristic of digital substations is that the simultaneous flow of data and energy greatly amplifies the impact of security incidents.
The aim of this study is to examine the operation and protection of digital substations from the perspective of critical infrastructure protection.

Keywords

critical infrastructure, digital substation, IEC 61850, physical security, cyber-physical system, energy protection

Absztrakt

A villamosenergia-rendszerek digitalizációja az elmúlt évtizedben a kritikus infrastruktúrák átalakulásának egyik legjelentősebb technológiai folyamata lett. A villamosenergia-átviteli és -elosztó rendszerek korszerűsítése során a digitalizált irányítási és védelmi technológiák bevezetése, különösen az IEC 61850 szabványcsalád alapvetően átalakította a hálózati architektúrák működését. Ezzel párhuzamosan azonban a digitalizáció új biztonságtechnikai és megbízhatósági kockázatokat is teremtett. Az átállás rámutat arra, hogy az energetikai rendszerek automatizáltsági fokának növekedésével a fizikai és kiberbiztonsági rétegek közötti határ elmosódik, mivel az alállomási infrastruktúra már egyértelműen kiberfizikai rendszerként működik. A kritikus infrastruktúra-védelem szempontjából a digitális alállomások sajátossága, hogy az adat- és energiaáramlás egyidejűsége miatt a biztonsági incidensek hatása sokszorosan felerősödik.
Jelen tanulmány célja, hogy a digitális alállomások működését és védelmét kritikus infrastruktúra-védelmi szemszögből vizsgálja.

Kulcsszavak

kritikus infrastruktúra, digitális alállomás, IEC 61850, fizikai biztonság, kiberfizikai rendszer, energetikai védelem

[1] morocz.mate@stud.uni-obuda.hu | ORCID: 0009-0007-2150-2893 | PhD Student, Doctoral School on Safety and Secu-rity Sciences Óbuda University | Doktorandusz hallgató, Óbudai Egyetem Biztonságtudományi Doktori Iskola

BEVEZETÉS

Az energetikai infrastruktúra a modern társadalmak egyik legösszetettebb, legnagyobb kockázati kitettségű és egyben legkritikusabb rendszere. A villamosenergia-ellátás folyamatossága alapvető feltétele az állam gazdasági, katonai és társadalmi stabilitásának. A Nemzetközi Energiaügynökség (IEA) 2024-es jelentése szerint a globális villamosenergia-fogyasztás 2014 és 2024 között mintegy 32%-kal emelkedett, miközben az elektromos hálózatok automatizáltsági és digitalizáltsági foka több mint kétszeresére nőtt és a hálózati digitalizációs beruházások értéke meghaladta a 230 milliárd USD-t évente [1]. Ezzel párhuzamosan az energiaelosztás és -felügyelet rendszerei egyre inkább adatvezérelt és hálózati architektúrákra épülnek, ami a megbízhatóság javulását hozza, ugyanakkor növeli a biztonsági kockázatok komplexitását.

A digitális alállomások (Digital Substations) olyan, nagymértékben automatizált és kommunikáció-orientált energetikai létesítmények, amelyekben a hagyományos, analóg jelátvitelt Ethernet-alapú kommunikációs rétegek, a berendezések közötti valós idejű adatkapcsolatot pedig Intelligent Electronic Devices (IED) és Merging Unit egységek biztosítják [5], [6]. Ezek az eszközök képesek automatikusan felismerni, izolálni és kezelni hálózati eseményeket, ezzel csökkentve az üzemzavarok kockázatát. A modern alállomási architektúrákban a mérési, vezérlési és védelmi folyamatok digitális adatfolyamokként (Sampled Values, GOOSE üzenetek) áramlanak a process bus és station bus hálózatokon keresztül, amely jelentős előrelépést jelent az interoperabilitás és üzemviteli hatékonyság terén [7].

Ugyanakkor a digitalizált architektúrák új típusú sérülékenységi mintázatokat hoznak létre. A fizikai infrastruktúra (berendezésházak, kábelezés, hálózati kapcsolók), a kommunikációs eszközök, valamint a távfelügyeleti interfészek mind potenciális támadási pontokká válnak [9]. Az IEC 61850 process-bus és station-bus hálózatainak nyitottsága, az időszinkronizációs protokollok (IEEE 1588 PTP) függősége, illetve a valós idejű adatkapcsolatok érzékenysége miatt a fizikai védelem és a kiberbiztonság már nem kezelhető külön területekként. A biztonságtechnikai fókusz a 2020-as évektől kezdve a komplex rezilienciaalapú megközelítés felé tolódott el. Nem csak pusztán az eszközök vagy építmények védelmét, hanem a rendszerszintű működőképesség megőrzését tekintik elsődleges célkitűzésnek [8], [10]. A kritikus infrastruktúrák — így az energetikai alállomások — védelmében a fizikai, kiber és üzemviteli rétegek integrált, egymást erősítő biztonsági architektúrája vált meghatározóvá.

E kontextusban a digitális alállomások nem csupán technológiai fejlesztési irányt, hanem nemzetbiztonsági szempontból kiemelt kockázati területet is jelentenek. Az e rendszerekhez kapcsolódó fizikai hozzáférési pontok, berendezések és hálózati infrastruktúrák biztonságtechnikai kezelése ma már elválaszthatatlan része a kritikus infrastruktúra-védelmi stratégiáknak Magyarországon és az Európai Unióban egyaránt.

KUTATÁSMÓDSZERTAN

A kutatás módszertana a digitális alállomások kiberfizikai sérülékenységeinek, támadási felületeinek és rendszerszintű következményeinek feltárására irányul, különös hangsúlyt helyezve a kritikus infrastruktúrák – ezen belül az energetikai ellátórendszer – védelmi követelményeire. A vizsgálat alapját a modern, IEC 61850-alapú digitális alállomások kommunikációs és védelmi architektúrája képezi, mivel ezekben az állomásokban a

fizikai folyamatok (áram, feszültség, teljesítményáramlás) és a digitális vezérlési rétegek (GOOSE, Sampled Values, MMS) szoros, nagysebességű kölcsönhatása olyan összetett kiberfizikai rendszert eredményez, amely a hagyományos alállomásokhoz képest jelentősen más kockázati profilt mutat. A módszertani megközelítés ennek megfelelően egymásra épülő, több szintű elemzési struktúrát követ.

A kutatás első lépése a digitális alállomások működését meghatározó kommunikációs és védelmi protokollok, valamint a kritikus infrastruktúrákra vonatkozó hazai és európai szabályozások kritikus szemmel való elemzése. Ezen belül kiemelt fókuszt kap az IEC 61850-szabványcsalád (GOOSE, SV, MMS, SCL) architektúrája, továbbá az ENISA smartgrid biztonsági elemzéseiben azonosított kockázati kategóriák, valamint a magyar létfontosságú rendszerelemeket szabályozó jogszabályi keretek. Ez a lépés biztosítja a kutatás normatív hátterét, és rögzíti azokat a rendszerszintű követelményeket, amelyekhez a vizsgálatok és értékelések igazodnak.

A második lépésben a kutatás a digitális alállomások technológiai architektúrájának műszaki modellezésére épít. Ennek célja annak feltárása, hogy a GOOSE-, SV- és MMS-szinteken bekövetkező manipulációk miként befolyásolják a védelmi döntési folyamatokat és a fizikai berendezések működését.

A harmadik módszertani komponens a kiberfizikai támadásszenáriók elemzése. A támadási vektorok – hamisítás, késleltetés, blokkolás, torzítás, replay, DoS és konfigurációmanipuláció – a teljesség igénye nélkül külön értékelésre kerül abból a szempontból, hogy milyen mértékben veszélyezteti a rendszer működési integritását. A vizsgálat során nemcsak a protokollszintű hatások (pl. GOOSE-késleltetés), hanem a kiberfizikai lánc szintjei is elemzés tárgyát képezik, vagyis az, hogy egy adott támadás milyen kockázattal vezet hibás mezőszinti működéshez vagy rendszerszintű instabilitáshoz.

A módszertan negyedik eleme a kockázatfeltárás, amelynek célja a különböző támadásszintek hatásmechanizmusának strukturált vizsgálata. Az FMEA-megközelítés a hibamódokat (pl. SV-manipuláció, hamis GOOSE-üzenet, MMS-parancsinjektálás) a lehetséges okokkal, következményekkel és észlelhetőséggel összefüggésben vizsgálja, meghatározva azokat a pontokat, ahol a védelmi logika különösen érzékeny, ezzel feltárva a kaszkád folyamatok logikai felépítését. Ez az elemzésmód különösen fontos, mivel a digitális alállomásokban a támadások nem elszigetelt eseményként, hanem egymást erősítő folyamatként jelennek meg.

A kutatás módszertanának utolsó eleme a kritikus infrastruktúra szemszögű értékelés. Ez a lépés a műszaki elemzéseket és a kockázati modelleket összekapcsolja a létfontosságú rendszerekre vonatkozó szabályozási és biztonsági követelményekkel, kiemelve azt, hogy a digitális alállomások sérülékenysége milyen rendszerszintű kockázatot jelent a villamosenergia-ellátás folytonosságára. A vizsgálat célja annak meghatározása, hogy mely támadási vektorok jelentenek valós, rendszerszintű fenyegetést, és mely pontokon szükséges a védelmi architektúra megerősítése a fizikai és kiberbiztonsági kontrollok integrációjával. A kutatási módszertan olyan holisztikus keretet biztosít, amely egyszerre vizsgálja a digitális alállomások kommunikációs, védelmi és fizikai rétegeit, és amely alkalmas arra, hogy a kritikus infrastruktúrák sajátos követelményeihez igazodva átfogó képet adjon a digitális alállomások biztonságtechnikai megvalósíthatóságáról, sebezhetőségi profiljáról és kockázati szintjéről.

KRITIKUS INFRASTRUKTÚRÁK SZABÁLYOZÁSI HÁTTERE

Magyar szabályozási háttér

Magyarországon a 2012. évi CLXVI. törvény a létfontosságú rendszerek és létesítmények azonosításáról a villamosenergia-ellátást a nemzeti létfontosságú infrastruktúrák egyik alapvető ágazataként határozza meg, összhangban az Európai Unió kritikusinfrastruktúra-védelmi keretrendszerével [11]. A törvény célja, hogy azonosítsa azokat a rendszereket, amelyek működése nélkülözhetetlen az állam alapvető funkciói, a lakosság ellátásbiztonsága és a gazdaság stabilitása szempontjából. A jogszabály a villamos energia átviteli, elosztási és irányítási infrastruktúráit – beleértve a nagyfeszültségű alállomásokat, vezetékhálózatokat, diszpécserközpontokat és az ezekhez kapcsolódó infokommunikációs rendszereket – létfontosságú rendszerelemként definiálja. Ez azért is kiemelt jelentőségű, mert a villamosenergia-szektor a kritikus infrastruktúrák közötti leginkább hálózatfüggő és interdependens ágazatok közé tartozik: meghibásodása vagy támadása súlyos következményekkel járhat más létfontosságú szolgáltatások működésére (pl. távközlés, vízellátás, egészségügy, közlekedés) [4].

A törvény végrehajtásának részletes követelményeit a 65/2013. (III. 8.) Korm. rendelet határozza meg, amely átfogó eljárásrendet ír elő a létfontosságú rendszerek azonosítására, minősítésére és védelmére [12]. A rendelet bevezeti a biztonsági osztályba sorolás kötelezettségét, amely az adott létesítmény kritikus szerepét, fenyegetettségi szintjét és sérülékenységét figyelembe véve határozza meg a minimálisan szükséges védelmi szintet. Emellett előírja a komplex biztonsági dokumentáció elkészítését, amely tartalmazza a fizikai védelem, a technikai és kiberbiztonság, az üzemvitel-biztonság, valamint a humánbiztonság koordinált elemzését és integrált tervezését. A rendelet kötelezővé teszi továbbá a rendszeres kockázatelemzést, az incidenskezelési protokollok kialakítását, a működési folyamatok vészhelyzeti eljárásrendjét, valamint a biztonsági intézkedések éves felülvizsgálatát.

A magyar szabályozás lényegi eleme, hogy a létfontosságú rendszerelemek védelmét integrált, többdimenziós biztonsági modellben értelmezi, amelyben a fizikai biztonsági intézkedések (pl. kerítés, beléptetés, CCTV, behatolásjelzés) és a kiberbiztonsági rétegek (tűzfalak, hálózati szegmentáció, naplózás, titkosítás, hozzáférés-kezelés) egyetlen egységes védelmi architektúra részeként működnek. Ez a megközelítés különösen releváns a modern, IEC 61850 alapú digitális alállomások vonatkozásában, amelyek kiberfizikai rendszerként működnek, így a fizikai és digitális sérülékenységek kölcsönösen hatnak egymásra. A rendelet hangsúlyozza a védelmi koordinátorok kijelölésének kötelezettségét is, akik a létesítmény és a hatóságok közötti szakmai-jogi kapcsolattartást biztosítják, valamint az éves jelentések és auditok végrehajtásáért felelnek.

Európai Uniós szabályozási háttér

Az Európai Unió 2022/2555 számú (NIS2) irányelve [13] a kritikus infrastruktúrák biztonságának szabályozásában mérföldkőnek számít, mivel jelentős szigorítást vezetett be a kiberfizikai rendszerek védelmében, különösen az energetikai ágazat tekintetében. Az irányelv az energiaellátást „magas kockázatú, stratégiai jelentőségű ágazatként” határozza meg, és előírja, hogy az energetikai szolgáltatók — ideértve az átviteli rendszerirányítókat

(TSO), az elosztóhálózat-üzemeltetőket (DSO), valamint a villamosenergia-ipari szolgáltatókat — átfogó, reziliens biztonságirányítási rendszert hozzanak létre. Ez a rendszer kiterjed a kiberbiztonsági, fizikai biztonsági és üzemviteli biztonsági folyamatok együttes kezelésére, felismerve, hogy a modern energiahálózatok működése kiberfizikai integrációra épül, ahol a digitális és fizikai folyamatok szétválaszthatatlanul kapcsolódnak egymáshoz [3].

A NIS2 külön hangsúlyt fektet a kockázatalapú megközelítésre, amely kötelezi a szolgáltatókat a fenyegetettségek folyamatos értékelésére, a beszállítói lánc biztonságának felügyeletére, valamint a kritikus folyamatokhoz kapcsolódó incidenskezelési, üzemfolytonossági és helyreállítási kapacitások biztosítására. A szabályozás kitér arra is, hogy a létfontosságú energetikai rendszerek esetében nem elegendő a hagyományos, reaktív biztonság, hanem proaktív, előrejelzésen, automatizált és intelligens észlelésen alapuló védelemre van szükség, különösen a villamosenergia-rendszerek digitalizációjának előrehaladása miatt. Az ENISA 2022-es ágazati jelentése rámutat, hogy az uniós tagállamok energetikai infrastruktúráinak mintegy 82 %-a közvetlen függésben áll digitalizált irányítási rendszerekkel, mint például a SCADA (Supervisory Control and Data Acquisition), a DCS (Distributed Control System) vagy az IEC 61850 alapú digitális alállomási technológia [14]. A jelentés szerint a villamosenergia-hálózatok több mint 60 %-a már alkalmaz valamilyen digitális alállomási megoldást, és az átviteli hálózat modernizációjára irányuló beruházások több mint fele közvetlenül az alállomások digitalizációjához kötődik. Ezek az adatok alátámasztják, hogy a hálózati automatizáció és a kiberfizikai rendszerek terjedése az ellátásbiztonság alapfeltételévé vált Európában [1].

Ugyanakkor a digitalizáció növekedése új típusú kitettségeket is eredményezett. A kiberfizikai rendszerek összekapcsoltsága miatt egyetlen sérülékenység — legyen az hálózati protokollban (pl. MMS, GOOSE), időszinkronizációban (IEEE 1588), vagy akár egy IED eszköz szoftverében — rendszerszintű zavarokat idézhet elő. ENISA arra is felhívja a figyelmet, hogy 2020–2022 között az energetikai ágazat ellen irányuló kiberincidensek száma több mint 59 %-kal növekedett, és ezek jelentős része éppen a digitalizált alállomási kommunikációs rétegeket célozta. A hatékonyság és automatizáció növekedésével párhuzamosan tehát a sérülékenységi térkép is bővül, amely indokolttá teszi az integrált biztonsági kontrollok kiépítését, valamint az előírásoknak megfelelő, folyamatos rezilienciafejlesztést [2].

A DIGITÁLIS ALÁLLOMÁSOK TECHNOLÓGIAI ALAPJAI

A modern villamosenergia-átviteli és -elosztási rendszerekben a digitális alállomások (Digital Substations, DSS) az egyik legdinamikusabban fejlődő kritikus infrastruktúrakomponensek közé tartoznak. A nemzetközi statisztikák szerint a nagy feszültségű alállomások digitalizációja 2020–2025 között átlagosan évi 12 %-kal nőtt, amelyet a megújuló energiaforrások integrálása, az IoT-érzékelők terjedése és az energiahálózatok automatizálása motivál. A „digitális átállás” koncepciója olyan átfogó technológiai paradigmát képvisel, amely a primer és szekunder villamos berendezések összekapcsolását Ethernet-alapú, nagy rendelkezésre állású és determinisztikus kommunikációs architektúrára alapozza. A digitális alállomások célja a hagyományos, analóg jelátvitelű rendszerek kiváltása szabványosított adatmodellekkel, protokollokkal és intelligens elektronikus eszközökkel (IED-ek, Merging Unit-ok), amelyek valós időben biztosítják a mérési, vezérlési és védelmi funkciók

adatcseréjét [15]. A szakirodalom kiemeli, hogy a digitalizált alállomási infrastruktúrák lehetővé teszik a kábelezési mennyiség akár 80%-os csökkentését, a hibadetektálás felgyorsítását, valamint a konfigurációs rugalmasság jelentős növelését, különösen a process bus és station bus topológiák bevezetésével [16].

A digitális alállomások technológiai gerincét az IEC 61850 szabványcsalád adja, amely egységes adatmodellt, kommunikációs profilt, konfigurációs nyelvet (SCL), valamint hálózati viselkedési elveket definiál az alállomási automatizáláshoz. A szabvány három hierarchikus működési szintet különít el: a folyamat-szintet (process level), ahol a Merging Unit-ok Sampled Values üzenetekkel digitalizálják és továbbítják a primer áram- és feszültséginformációkat; a mező-szintet (bay level), ahol az intelligens védelmi és vezérlési IED-ek működnek és GOOSE üzeneteken keresztül kommunikálnak; valamint az állomásszintet (station level), ahol a HMI/SCADA rendszerek, a naplózás, felügyelet és az irányítási folyamatok összegződnek [2]. Ez a háromszintű struktúra biztosítja az alállomási automatizálás interoperabilitását, valós idejű kommunikációját és gyors reakcióképességét hálózati események esetén [17].

A digitális alállomások elterjedése ugyanakkor új kockázati dimenziókat is megnyit. A digitális alállomások kiberfenyegetettségi profilja lényegesen komplexebb, mint a hagyományos rendszereké, mivel az IED-ek, a process bus és station bus elemei olyan hálózati protokollokra épülnek, amelyek célzott támadási felületet teremthetnek – különösen a GOOSE, MMS és SV kommunikáció sérülékenységein keresztül [9]. A digitális alállomások legjelentősebb fenyegetései közé tartoznak a manipulált Sampled Values üzenetek, a késleltetett vagy blokkolt GOOSE csomagok, a PTP alapú időszinkronizáció megzavarása, valamint az IED-ek firmware-szintű kompromittálása. Ezen támadástípusok hatása kiterjedhet az automatikus védelmi funkciók hibás működésére, meghibásodások késleltetett felismerésére, vagy akár a megszakítók indokolatlan kapcsolására is – ezáltal a digitális alállomások kiberfizikai integritásának sérülésére. A IEC 61850 architektúra ugyan számos biztonsági és redundanciaelemet tartalmaz (pl. PRP/HSR protokollok, determinisztikus üzenetszórás, hálózati szeparáció lehetősége), azonban a szakirodalom szerint a digitális alállomások biztonsága csak akkor tartható fenn, ha a folyamat-, mező- és állomás-szinten azonosított kockázatokra integrált, kiberfizikai biztonságirányítási modell épül [9]. E modellnek egyszerre kell kezelnie a hálózati protokollsérülékenységeket, az IED-ek eszközszintű biztonsági hibáit, a kommunikációs folyamatok integritását, valamint a fizikai hozzáférés- és környezetvédelmi kontrollokat. A digitális alállomások rezilienciája tehát nem pusztán a technológiai modernizáció függvénye, hanem a többdimenziós biztonsági architektúra megbízható implementációjáé is. Ezért a kiberfenyegetések taxonómiájának kialakítása elengedhetetlen, mivel a digitális alállomások működése olyan időkritikus, többprotokollos környezetben zajlik, ahol a támadások akár néhány ezredmásodperc alatt befolyásolhatják a védelmi döntéseket. A szakirodalomban a fenyegetéseket négy fő kategóriába sorolják: a kommunikációs protokollok elleni támadások, az eszköz- és firmware-szintű támadások, az időszinkronizáció elleni fenyegetések és a fizikai–kiber kombinált (CPS) támadások, amelyek együttesen határozzák meg a digitális alállomások kockázati profilját [5], [9], [10], [16], [18].

A kommunikációs protokollok elleni támadások a digitális alállomások elsődleges sérülékenységi területét jelentik, mivel a rendszer működését az IEC 61850 szabványon alapuló protokollok – GOOSE, Sampled Values (SV) és MMS – valósítják meg. A GOOSE-

üzenetek módosításával vagy késleltetésével a támadók képesek befolyásolni a védelmi IED-ek közötti döntéseket, ami hibás kioldásokhoz, védelmi koordinációs zavarokhoz vagy a hibák késleltetett felismeréséhez vezethet. A Sampled Values torzítása különösen veszélyes, mivel a digitális mérési értékek manipulálása a rendszer teljes védelemfilozófiáját torzíthatja, meghamisítva az áram- és feszültségadatokat, így akár berendezéskárosodást is előidézhet. Hasonlóképpen, az MMS-alapú támadások hozzáférést biztosíthatnak a támadók számára az alállomási konfigurációkhoz vagy a naplóállományokhoz. Kolosok és Korkina kiemelik, hogy ezen kommunikációs sérülékenységek jelentős része abból ered, hogy az IEC 61850 eredeti tervezésekor az adatbiztonsági mechanizmusok – például a kriptográfiai védelem – még nem voltak széles körben alkalmazottak a nagy rendelkezésre állás és a késleltetésminimalizálás érdekében [9].

Az eszköz-, firmware- és konfigurációs szintű támadások a digitális alállomások másik kritikus fenyegetési kategóriáját alkotják. Az IED-ek, Merging Unit-ok és alállomási switch-ek olyan beágyazott rendszerek, amelyek támadhatók hibás firmware-frissítéseken, vagy nem biztonságos konfigurációkon keresztül. A firmware-manipuláció lehetővé teszi a támadó számára, hogy rejtett, rosszindulatú funkciókat illesszen be az eszköz működésébe, amely akár hónapokig észrevétlen maradhat. A konfigurációs állományok – különösen az IEC 61850 SCL fájlok – módosítása az egész alállomás viselkedésére kihat, mivel ezek tartalmazzák a topológiát, a kommunikációs logikát és a védelmi összefüggéseket. A kutatások rámutatnak, hogy a digitális alállomások tervezésében alkalmazott centralizált konfigurációkezelés ugyan egyszerűsíti a mérnöki folyamatokat, de célponttá válhat a támadók számára, akik egyetlen konfigurációs manipulációval a teljes alállomást destabilizálhatják [5], [10].

Az időszinkronizáció elleni támadások különösen súlyos következményekkel járhatnak, mivel a digitális alállomások működése – ideértve a védelmi algoritmusokat, a naplózást és az események sorrendiségét – a mikroszekundumos pontosságú időszinkronizációtól függ. Az IEEE 1588 Precision Time Protocol (PTP) manipulálása, például késleltetés beszúrásával vagy hamis időjel generálásával, hamis időbélyegekhez és hibás védelmi döntésekhez vezethet. A GPS-spoofing szintén valós fenyegetést jelent, mivel több alállomás továbbra is külső időforrásokra támaszkodik, amelyek megzavarása esetén a teljes védelemkoordináció összecsúszhat, torzulva a hibák lokális detektálását [18]. Mivel a digitális alállomások szinkronizációja az SV és GOOSE üzenetek korrekt időértelmezésétől függ, az időszinkron elleni támadások képesek minimális láthatóság mellett is jelentős zavart okozni.

A fizikai–kiber kombinált támadások (CPS – Cyber-Physical Systems támadások) a digitális alállomások egyik legveszélyesebb fenyegetését jelentik, mivel egyszerre célozzák a fizikai berendezéseket és az informatikai rendszereket. Ezekben a támadás-szcenáriókban a támadók például fizikai hozzáférést szerezhetnek egy Merging Unit-hoz vagy IED-szekrényhez, majd hardveralapú manipulációval vagy rogue-eszköz beillesztésével meghamisíthatják a kommunikációs folyamokat. Ugyancsak ide tartoznak a process bus optikai kábeleinek megszakítását követő hamis eszközillesztések, vagy a hálózati switch-ek fizikai resetelése, amelyek a GOOSE és SV üzenetek teljes leállásához vezethetnek [10].

KIBERFIZIKAI TÁMADÁSSZENÁRIÓK ELEMZÉSE

Sampled Values (SV) manipuláció bemutatása

A Sampled Values (SV) üzenetek manipulációja a digitális alállomások legkritikusabb fenyegetései közé tartozik, mivel az SV a primer villamos jelleggörbék – áram, feszültség, teljesítmény – nagy pontosságú, 4 kHz–96 kHz mintavételezési frekvencián továbbított digitális reprezentációja, amely közvetlenül meghatározza a védelmi IED-ek döntéshozatali folyamatát. A szabványosított IEC 61850-9-2LE profilban rögzített SV-keretek akár 256 mintát másodpercenként, fázisonként továbbítanak, ami azt jelenti, hogy már néhány mintapont eltérése is jelentős hibát indukálhat a védelmi algoritmusokban. A kutatások kimutatták, hogy a differenciálvédelemnél alkalmazott védelmi egyenletek érzékenysége olyan mértékű, hogy mindössze 1–3%-os amplitúdótorzítás is elegendő lehet a hibás kioldáshoz, míg a fázistolás akár 2–3 fokos eltérése hibarejtést okozhat nagyfeszültségű távvezetékek esetében [19].

A támadók által végrehajtott SV-érték-manipuláció több formában jelentkezhet. A legegyszerűbb támadás az amplitúdó torzítása, amikor a valós áram- vagy feszültségértékeket egy konstans vagy időben változó skálafaktorral módosítják. Ennek következtében a túláramvédelmi funkciók tévesen alulfeszültség- vagy alulterhelés-jelenséget érzékelhetnek. Még súlyosabb a fázismódosítás, amely a távolsági védelem zónaérzékelését torzítja el: kísérletek szerint 4–5° fáziseltérés a védelem érzékelési tartományát akár 20–25%-kal is eltolhatja, ezzel hibás zónaváltást okozva [20]. A támadók gyakran alkalmaznak hullámforma-alapú manipulációt (waveform crafting), amely során a jel alakját magasabb harmonikus komponensekkel vagy modulált zajjal torzítják, miközben fenntartják az üzenet időzítési és formátumkövetelményeit, így az IED-ek számára a jel továbbra is érvényesnek tűnik. Az ilyen támadások különösen veszélyesek, mivel képesek reprodukálni egy valódi zárlati esemény mintázatát, hamis hibajelzést generálva, amely indokolatlan kioldást vált ki a megszakítókon. A SV-kommunikáció elvesztése (drop-attack) szintén súlyos kockázatot jelent. A process bus topológiákban a SV-áramlat megszakadása azt eredményezi, hogy az IED-ek nem kapnak friss mérési adatot, és az IEC 61850-8-1 szabvány szerinti biztonsági működés miatt „freeze" állapotba kapcsolnak, amelyben a védelmi funkciók jelentős része ideiglenesen letiltásra kerül vagy alapállapotba áll. Ez azt jelenti, hogy a védelem nem képes valós hibákat detektálni, amely – a rendelkezésre álló redundanciától függően – akár teljes védelmi vakfoltokat okozhat az alállomás egyes részein. Az ENISA elemzései rámutatnak, hogy 2020–2022 között az európai energetikai rendszerekben regisztrált védelmi zavarok mintegy 17%-a adatfolyam-szakadásra vagy időzítési anomáliára volt visszavezethető, ami alátámasztja a process bus stabilitásának kritikus szerepét [10]. A SV-réteg elleni támadások kiberfizikai hatása rendkívül magas, mivel közvetlenül a villamos méréseket és a védelmi döntések alapját képező valós idejű információáramlást befolyásolják. Mivel az SV-adatok alapján számított villamos paraméterek – például a komplex teljesítmény, a szinkronpozíció vagy a hibairány – közvetlen összefüggésben állnak a megszakítók vezérlésével és a hálózati stabilitással, az értékek bármilyen manipulációja azonnal, fizikai szinten jelenik meg. Ez különösen érvényes a differenciálvédelemre, amely az egyik leggyorsabb és legérzékenyebb védelem a nagyfeszültségű alállomásokban: már minimális jelhibákra is reagál, hogy megakadályozza a berendezések károsodását. A támadások súlyosságát tovább növeli, hogy az SV-csatornák integritását hagyományosan nem védik olyan kriptográfiai

eszközök, mint a GOOSE-Sec vagy az IEC 62351-6 szerinti hitelesítés, így a támadók számára a legközvetlenebb támadási felületet kínálják [21], [9].

MMS protokoll fenyegetései, rövid elemzése

Az MMS (Manufacturing Message Specification) protokoll a digitális alállomások állomásszintű kommunikációs rétegének gerincét képezi, amelyen keresztül a SCADA-rendszerek, IED-gatewayek, mérnöki munkaállomások és archívumkezelő rendszerek valósítják meg a konfigurációs, irányítási és felügyeleti funkciókat. Az IEC 61850-8-1 által definiált MMS-szolgáltatások teszik lehetővé az IED-ek adatbázisának lekérdezését, a védelmi logikák módosítását, a paraméterezést, a valós idejű adatok olvasását, valamint a parancsok (control commands) kiadását. Bár az MMS kommunikáció nem olyan szigorúan időkritikus, mint a GOOSE vagy a Sampled Values üzenetek, stratégiai jelentősége lényegesen nagyobb, mivel az alállomás teljes konfigurációs és vezérlési felépítésére rálátást és beavatkozási lehetőséget biztosít [2], [10].

A támadók különféle technikákkal élhetnek annak érdekében, hogy kihasználják az MMS-protokoll sajátosságait. A leggyakoribb módszer a jogosultság-kiterjesztés (privilege escalation), amely lehetővé teszi, hogy a támadó adminisztratív hozzáférést szerezzen egy SCADA-szerverhez, mérnöki munkaállomáshoz vagy IED-gatewayhez. A kutatások szerint a digitális alállomásokban használt mérnöki eszközök több mint 65%-a olyan Windows-alapú környezetben fut, amelyek ismert sebezhetőségei – például szolgáltatásmegszakítás, DLL-eltérítés vagy nem biztonságos frissítési mechanizmus – kihasználhatók az MMS-csatornák kompromittálására. Az IED-gatewayek és alállomási adatkoncentrátorok hálózati szolgáltatásait vizsgáló tanulmányok azt is kimutatták, hogy a konfigurációs portokra érkező nem hitelesített MMS-üzenetek egy része képes volt a berendezések újraindítására vagy memóriahibák kiváltására, ami a védelmi funkciók átmeneti kieséséhez vezethet [2].

A Substation Configuration Language (SCL) állományok manipulációja különösen súlyos következményekkel járhat, mivel az SCL-fájlok definiálják az alállomási topológiát, a kommunikációs kapcsolatok struktúráját, az IED-ek interfészeit, a GOOSE- és SV-feltéképezését, valamint a védelmi funkciók közötti logikai összefüggéseket. Egyetlen XML-alapú SCL-elem módosítása – például egy Logical Node átirányítása, egy GOOSE-üzenet új célcímének megadása vagy egy IED-hez rendelt védelmi funkció paramétereinek átírása – az alállomás teljes automatikai logikájának működésére hatással lehet. A rosszindulatú MMS-parancsok kiadása az egyik legközvetlenebb módja annak, hogy a támadó fizikai folyamatokat befolyásoljon. Az IEC 61850 szerint az MMS-szintű „Select-Before-Operate” (SBO) mechanizmus hivatott garantálni, hogy a parancsok nem kerülnek véletlen vagy illetéktelen kiadásra, azonban számos implementáció sérülékenynek bizonyult a jogosultságellenőrzés, session-menedzsment vagy titkosítás hiányosságai miatt. Egy rosszindulatú MMS „Operate” parancs – amelyet a támadó hiteles, de kompromittált sessionön keresztül ad ki – indokolatlan megszakítónyitást vagy -zárást eredményezhet. A rendszer-szimulációk és ENISA által közzétett esettanulmányok rámutattak, hogy már egyetlen, indokolatlan nyitás is súlyos feszültségesést, terhelési átrendeződést és frekvenciainstabilitást válthat ki a hálózatban, különösen nagy terhelési csomópontok közelében. Az ilyen típusú „logikai támadások” különösen veszélyesek, mert nem generálnak látványos hálózati forgalmi anomáliát, hanem a legitim irányítási csatornán keresztül történnek, így az észlelésük különösen nehéz. [9]

A DIGITÁLIS ALÁLLOMÁS KIBERFIZIKAI KASZKÁD SÉRÜLÉKENYSÉGE

A digitális alállomások kiberfizikai kitettségének legsúlyosabb sajátossága, hogy az egyes támadási vektorok nem elszigetelten hatnak, hanem egymást erősítő, többlépcsős kaszkád-folyamatokat indítanak el, amelyekben a kiber- és fizikai események szorosan összekapcsolódnak. Ez a kaszkád-természet élesen eltér a hagyományos, analóg alállomások meghibásodási modelljeitől, mivel a digitális alállomásokban a védelem, az irányítás és az automatizálás funkciói a nagyfelbontású digitális kommunikációs csatornákra és valós idejű adatfeldolgozásra épülnek. A támadások ezért nem egyszerűen „zavaró tényezők", hanem a védelmi döntések integritását megbontó, nagy hatású rendszerszintű zavarok forrásai [5], [10].

Egy tipikus támadási lánc már a process busz manipulációjával megkezdődhet. Ha a támadó a Sampled Values (SV) üzeneteket módosítja – akár amplitúdó- vagy fázistorzítással, akár hullámforma-szintű beavatkozással –, a védelmi IED-ek hibás fázorbecslést végeznek, ami a primer hálózati állapot téves értelmezéséhez vezet. Kutatások kimutatták, hogy 1–3 %-os amplitúdó-hiba vagy 2–5°-os fáziseltérés már elegendő ahhoz, hogy a differenciálvédelem látszólagos hibát észleljen, míg a távolsági védelem zónahatárai 5–10 %-kal is eltolódhatnak a névlegestől [20], [10]. A hibás fázorbecslés közvetlen következménye, hogy a védelmi logika olyan GOOSE-parancsot generál, amely valójában nem felel meg a hálózat fizikai állapotának. A védelmi logikában keletkező hamis GOOSE-üzenetek a kaszkád folyamat második szintjét alkotják. A GOOSE-üzenetek időkritikus, multicast alapú jelzések, amelyek 3–4 ms alatt eljutnak a mezőszinti IED-ekhez. Amennyiben a támadó manipulált bemeneti adatokkal hamis „trip", „block" vagy „interlock" üzenetet generáltat, az IED-ek — a protokoll determinisztikus működése miatt — teljes bizalommal fogadják el azt, mivel a GOOSE-üzenetek eredeti tervezési filozófiája a megbízhatóságra (dependability) és nem a biztonságra (security) épült [22], [10]. Laboratóriumi vizsgálatok szerint egyetlen hamis GOOSE-üzenet képes volt 6–8 mezőszinti megszakító koordinált működését kiváltani, ami az alállomás teljes konfigurációját megváltoztatta [9].

A kaszkád harmadik fázisában a mezőszinten hibásan működő megszakítók fizikai következményeket okoznak. Ezek közé tartozhat a téves leválasztás, amely túlterheli a szomszédos tápvonalakat, a teljesítményáramlási útvonalak hirtelen átrendeződése pedig korlátozási és stabilitási problémákhoz vezethet. Valós hálózati esetek alapján egyetlen, nem tervezett megszakító-nyitás azonnal 20–40 MW teljesítményátrendeződést okozhat a regionális középfeszültségű hálózatokon, míg nagyfeszültségű átviteli szinten ez az érték akár a 150–250 MW tartományba is eshet [23]. Amennyiben a hibás kioldás egyszerre több elosztó vagy átviteli csomópontot érint, a rendszer fokozott valószínűséggel kerül frekvencia-érzékeny tartományba (49,0–49,3 Hz), amely tovább növeli az automatikus terheléslekapcsolási mechanizmusok aktiválódásának esélyét [23].

Az utolsó kaszkádszint a rendszerszintű instabilitás, amely a fizikai működési zavarokból ered. A hibás megszakító-állapotok miatt létrejövő hálózati topológiaváltozások veszélyeztetik a tranziens stabilitást, rontják a szinkrongépek közötti fázisszög-koordinációt és jelentős módosulást okoznak az áramlási interfészek terhelésében. Ez a kaszkádmechanizmus jól illusztrálja, hogy a digitális alállomások sérülékenysége nem egyetlen komponens meghibásodásának következménye, hanem a teljes irányítási és védelmi architektúra integritását determináló rendszerjellemző. Az így kialakuló sérülékenység struktúrája rávi-

lágít arra, hogy a digitális alállomások védelmét integrált, rendszerszemléletű megközelítésben kell kezelni – különösen a kritikus infrastruktúrák esetében –, mivel a mérési adatok, a kommunikációs protokollok és a védelmi logikák harmóniája bontakozik ki a sérülékenység mechanizmusaként [24].

TÁMADÁSOK JÖVŐKÉPE, JAVASLATOK

A kutatás eredményei egyértelműen rámutatnak arra, hogy a digitális alállomások – különösen az IEC 61850 kommunikációs és védelmi architektúrára épülő rendszerek – működése alapvetően kiberfizikai természetű, amelyben a kommunikációs rétegek sérülékenysége közvetlenül hat a villamos berendezések fizikai működésére és ezáltal az energetikai ellátás folytonosságára. A GOOSE-, Sampled Values- és MMS-szinteken azonosított támadások bizonyítottan képesek olyan kaszkád folyamatokat elindítani, amelyek téves védelmi működést, indokolatlan megszakító-állapotváltozásokat, hálózati instabilitást és szélsőséges esetben regionális ellátáskimaradást okozhatnak. E sérülékenységek különösen kritikusak Magyarország és az Európai Unió létfontosságú energetikai infrastruktúrái szempontjából, ahol a digitális alállomások térnyerése gyors ütemben zajlik, miközben a rendszerek nagy része még nem rendelkezik teljes körű, szabványosított kiberbiztonsági védelemmel. A vizsgálat rámutatott arra is, hogy a jelenlegi védelem elsősorban a megbízhatóságra és rendelkezésre állásra koncentrál, miközben a kommunikációs integritás, hitelesítés, valamint a valós idejű adatfolyamok kiberfizikai sérülékenységei továbbra is alulértékelt kockázati tényezők. A hibaterjedési modellek egyértelműen bizonyítják, hogy már kismértékű, célzott manipuláció is elegendő ahhoz, hogy a védelmi logika téves döntést hozzon, ezért a védelem funkcionális biztonsága a jövőben nem választható el a kiberbiztonsági kontrolloktól.

A kutatás alapján a következő főbb javaslatok fogalmazhatók meg:

- *Integrált kiberfizikai biztonsági architektúra kialakítása:* Az alállomások védelmi és irányítási rendszerét úgy szükséges továbbfejleszteni, hogy a kiber- és fizikai védelem ne különálló rétegekként, hanem egységes, egymást kiegészítő rendszerként működjön. A kommunikációs integritás, hitelesítés és időszinkron-védelem beépítése kiemelt prioritás.
- *Rendszerszintű monitoring és anomália-detektálás:* A digitális alállomások kiberfizikai jellegéből adódóan a támadások gyakran a fizikai rétegben mutatkoznak meg. Ezért olyan monitoring-rendszerek szükségesek, amelyek összevetik a kommunikációs réteg (GOOSE/SV/MMS) és a fizikai réteg (áram, feszültség, teljesítmény) viselkedését, és képesek az összefüggéstelen mintázatok korai felismerésére.
- *Szimulációs és HIL-alapú tesztelési infrastruktúra kiépítése:* A digitális alállomások biztonsági értékelése nem végezhető csupán elméleti alapon. A valós idejű HIL- és RTDS-szimulációk lehetővé teszik a kiberfizikai támadásszenáriók és azok fizikai hatásainak hiteles vizsgálatát, amely alapfeltétele a reziliens védelem kialakításának.
- *Kritikus infrastruktúra-specifikus kockázatkezelési keretrendszer alkalmazása:* A digitális alállomások kockázatait a NIS2, a nemzeti kritikus infrastruktúra törvény és az ENISA ajánlások alapján szükséges értékelni. A sérülékenységi profilok és

kaszkád-hatásláncok alapján a védelemnek a legkritikusabb támadási vektorokra kell koncentrálnia.

ÖSSZEGZÉS

A kutatás átfogóan vizsgálta a digitális alállomások kiberfizikai biztonságát és megvalósíthatóságát a kritikus infrastruktúrák védelmének szemszögéből. A digitális alállomások elterjedésével az energetikai rendszer egy olyan, korábban nem létező kitettségi formával szembesül, ahol a primer berendezések működése és a kommunikációs rétegek integritása közötti kapcsolat közvetlenné vált. Ennek következtében a villamosenergia-rendszer működése ma már nagymértékben függ a GOOSE-, Sampled Values- (SV) és MMS-protokollokra épülő digitális vezérlési és védelmi folyamatoktól. A kutatás egyik legfontosabb megállapítása, hogy e protokollok sérülékenységei – különösen az adatintegritás, időderminált ság és hitelesítés hiányosságai – olyan kiberfizikai támadási felületet hoznak létre, amely közvetlen fizikai következményekkel járhat.

A kritikus infrastruktúra szemszögéből a kutatás rámutatott arra, hogy a digitális alállomások biztonsága ma már elválaszthatatlan az energetikai ellátás folytonosságától. Az európai NIS2 irányelv, valamint a magyar 2012. évi CLXVI. törvény és kapcsolódó szabályozások egyértelművé teszik, hogy a digitális alállomások a nemzeti létfontosságú rendszerelemek részei, így védelmük nemcsak műszaki, hanem stratégiai követelmény is. A kutatás eredményei szerint a legnagyobb kitettséget a kommunikációs integritás hiánya, az időszinkronizáció sérülékenysége, a konfigurációs állományok hitelesítésének hiánya és a valós idejű adatfolyamok manipulálhatósága jelenti.

A vizsgálatok feltárták, hogy az SV-üzenetek kismértékű manipulációja is jelentős hatással van a védelmi algoritmusokra. A hibás fázorbecslésből eredő hamis GOOSE-üzenetek tovább erősítik a kaszkádszerű sérülékenységet: egyetlen rosszindulatú vagy manipulált parancs több mezőszinti megszakító koordinált működését válthatja ki, amely teljesítményátrendeződést, üzemzavart és – szélsőséges esetben – regionális ellátáskimaradást okozhat. A kutatás kimutatta továbbá, hogy az MMS-alapú támadások stratégiai kockázatot jelentenek, mivel az állomásszintű irányítás és konfiguráció sérülékenységei lehetővé teszik a támadók számára a védelmi beállítások átírását, a védelmi topológia átstrukturálását vagy akár indokolatlan megszakító-vezérlések kiadását. Ezért a védelem kizárólag integrált megközelítéssel valósítható meg: a kommunikációs biztonság, a védelmi funkciók jóváhagyási mechanizmusai, az időszinkronizáció és a fizikai eszközök megbízhatósága együttesen határozzák meg az alállomás ellenálló képességét.

A jelenlegi technológiai érettség mellett egyértelmű, hogy a jövőben a védelmi architektúrák fejlesztése, a szabványokon alapuló biztonsági mechanizmusok beépítése, valamint a rendszerszintű monitoring és detektálás alkalmazása válik kulcsfontosságúvá. A digitális alállomások nem pusztán modernizációs lépést jelentenek az energetikai szektorban, hanem olyan komplex kiberfizikai rendszerek, amelyek biztonsága meghatározza az ellátásbiztonságot, a hálózati stabilitást és végső soron a nemzeti energiarendszer reziliencáját.

FELHASZNÁLT IRODALOM

[1] International Energy Agency (IEA), Digitalization and Energy 2024 Report, 2024. [Online]: https://www.iea.org/reports/digitalisation-and-energy

[2] IEC 61850-1, Communication Networks and Systems for Power Utility Automation – Part 1: Introduction and Overview, International Electrotechnical Commission, Geneva, 2013. [Online]: https://webstore.iec.ch/publication/6028

[3] European Union, Directive (EU) 2022/2555 (NIS2) on measures for a high common level of cybersecurity across the Union, Official Journal of the European Union, 2022. [Online]: https://eur-lex.europa.eu/eli/dir/2022/2555/oj

[4] 2012. évi CLXVI. törvény a létfontosságú rendszerek és létesítmények azonosításáról, Magyar Közlöny, 2012. [Online]: https://net.jogtar.hu/jogszabaly?docid=A1200166.TV

[5] SEL, "Digital Substation or Digital Secondary Systems — What's the difference?," Schweitzer Engineering Laboratories, 2024. [Online]: https://selinc.com/solutions/p/digital-substation/

[6] Hitachi Energy, "Digital Substations Overview," 2024. [Online]: https://www.hitachienergy.com/us/en/products-and-solutions/digitalization/digital-substation

[7] NEMA, Expanding the Adoption of IEC 61850, National Electrical Manufacturers Association, White Paper, 2021. [Online]: https://www.nema.org/docs/default-source/distribution-automation-toolkit-library/expanding-the-adoption-of-iec-61850.pdf

[8] G. Pázmándi, Kritikus infrastruktúrák védelme Magyarországon, Nemzeti Közszolgálati Egyetem, Budapest, 2021.

[9] I. Kolosok and E. Korkina, "Problems of Cyber Security of Digital Substations," IWCI 2019 Proceedings, pp. 75–78

[10] ENISA, Cybersecurity and Resilience of Smart Grids, European Union Agency for Cybersecurity, 2022. [Online]: https://www.enisa.europa.eu/news/enisa-news/smart-grids-cyber-security-measures-a-risk-based-approach-is-key-to-secure-implementation [Letöltve: 02-Nov-2025]

[11] Magyarország Országgyűlése, 2012. évi CLXVI. törvény a létfontosságú rendszerek és létesítmények azonosításáról, 2012. [Online]: https://net.jogtar.hu/jogszabaly?docid=A1200166.TV

[12] Magyarország Kormánya, 65/2013. (III. 8.) Korm. rendelet a létfontosságú rendszerek és létesítmények védelméről, 2013. [Online]: https://net.jogtar.hu/jogszabaly?docid=A1300065.KOR

[13] European Union, Directive (EU) 2022/2555 (NIS2) on Measures for a High Common Level of Cybersecurity Across the Union, Official Journal of the European Union, 2022. [Online]: https://eur-lex.europa.eu/eli/dir/2022/2555/oj

[14] European Union Agency for Cybersecurity (ENISA), Smart Grid Security: Recommendations for Europe and Member States, 2012; and ENISA, Cybersecurity and Resilience of Smart Grids, 2022. [Online]: https://www.enisa.europa.eu/publications/smart-grid-security-recommendations

[15] Schweitzer Engineering Laboratories (SEL), Digital Substation Solutions, 2024. [Online]: https://selinc.com/solutions/p/digital-substation/

[16] COPA-DATA, Digital Substations – How IEC 61850 and zenon Help You to Future-Proof Substation Operation, White Paper, 2024. [Online]:

https://www.copadata.com/hubfs/Downloads/Brochures/Digital-Substations_A5_2024_EN.pdf
[17] J. C. Lozano, Digital Substations and IEC 61850: A Primer, University of California eScholarship, 2023. [Online]: https://escholarship.org/uc/item/5kp7n3cn
[18] IEEE Std 1588-2019, Precision Clock Synchronization Protocol for Networked Measurement and Control Systems. [Online]: https://standards.ieee.org/standard/1588-2019.html
[19] A. Apostolov, "The Evolution of Sampled Values in IEC 61850 Process Bus Systems," PAC World Magazine, 2021. [Online]: https://www.pacw.org
[20] M. Chen, X. Jiang, "False Data Injection on IEC 61850-9-2 Process Bus: Attack Feasibility and Impacts," IEEE Transactions on Smart Grid, vol. 12, no. 4, 2021. [Online]: https://ieeexplore.ieee.org/document/9354472
[21] IEC 62351-6, Power Systems Management and Associated Information Exchange – Data and Communications Security – Part 6: Security for IEC 61850, 2020. [Online]: https://webstore.iec.ch/publication/31669
[22] IEC 61850-8-1, Communication Networks and Systems for Power Utility Automation – Part 8-1: Specific Communication Service Mapping – MMS Mapping, IEC, 2011.
[23] G. P. Chatzivasileiadis et al., "A Probabilistic Wide-Area Approach to Supply Restoration Following Extreme Events in Transmission Grids," IEEE Trans. Power Systems, vol. 34, no. 4, pp. 3461–3470, 2019.
[24] ENTSO-E, System Defence and Restoration (SDR) Report 2023. [Online]: https://www.entsoe.eu/publications/system-defence-and-restoration-sdr-report/
[25] BEREK L.–BEREK L.–RAJNAI Z., A tudományos kutatás folyamata és módszerei. Óbudai Egyetem, 2022. [Online]https://oda.uni-obuda.hu/handle/20.500.14044/25308
[26] BEREK L.–BEREK T.–BEREK L., Személy-és vagyonbiztonság. Óbudai Egyetem, 2016. [Online] http://nbn.urn.hu/N2L?urn:nbn:hu-6315