HADMÉRNÖK
VÉDELEMINFORMATIKA
18. évfolyam (2023) 3. szám 145–160.
DOI: 10.32567/hm.2023.3.10

Hankó Viktória[1]

SCADA-rendszerek kiberbiztonsága a létfontosságú rendszerelemek tekintetében 1.[2]

Cybersecurity of SCADA Systems from Critical Infrastructure Aspect 1

Absztrakt

Napjainkban a technológiai fejlődéssel a kiberbiztonság szerepe is egyre meghatározóbb, hiszen mind a magánszemélyeknek, mind a vállalatoknak lépést kell tartani a kibertámadások alakulásával – legyen szó azok számosságáról vagy módozatairól. Ezeknek a támadásoknak kiemelt célpontjai az ipari létesítmények, létfontosságú rendszerelemek, amelyeknek meghatározó elemei a SCADA-rendszerek. Ezzel összefüggésben elmondható, hogy ezekben a létesítményekben az átlagosnál jóval magasabb szintű védelemre van szükség szerepükből fakadóan. A tanulmány első részében a szerző ismerteti a SCADA-rendszer alapfogalmait, valamint azokat az előírásokat, jó gyakorlatokat, amelyek a létesítéshez, illetve működtetéshez szükségesek. Továbbá bemutatja a korábbi, illetve az aktuális kiberbiztonsági kihívásokat mind általános, mind pedig SCADA-rendszerre fókuszálva – a támadási metódus, a támadás éve, valamint az érintett szektor besorolása alapján.

Kulcsszavak: SCADA, kiberbiztonság, létfontosságú rendszerelem

[1] Doktori hallgató, Nemzeti Közszolgálati Egyetem Katonai Műszaki Doktori Iskola, e-mail: viktoria.hanko@protonmail.com

[2] A cikk a Kulturális és Innovációs Minisztérium ÚNKP-22-I-NKE-36 kódszámú Új Nemzeti Kiválóság Programjának a Nemzeti Kutatási, Fejlesztési és Innovációs Alapból finanszírozott szakmai támogatásával készült.

Abstract

Today, as technological advances continue, the role of cybersecurity is becoming increasingly important, as both individuals and companies need to keep up with the evolution of cyberattacks – in terms of both, their number and their methods. Industrial facilities and critical systems, of which SCADA systems are a key component, are prime targets for these attacks. In this context, these installations require a much higher level of protection than the average due to their role. In the first part of the article, the author describes the basic concepts of SCADA systems, as well as the specifications and good practices required for their installation and operation. It also describes past and current cybersecurity challenges, both general and SCADA system-focused, based on attack method, year of attack, and classification of the sector involved.

Keywords: SCADA, cybersecurity critical infrastructure

Bevezetés

Az Industrial Control Systems, azaz ipari vezérlőrendszerek (ICS) és a Supervisory control and data acquisition, azaz a felügyeleti ellenőrző és adatgyűjtő rendszerek (SCADA) az ipari létesítmények és a létfontosságú rendszerelemek, vagy a köznyelvben ismert kritikus infrastruktúrák működésének kritikus elemei. A világ számos ipari területén exponenciálisan növekszik a SCADA-rendszerek használata. Az információs és kommunikációs technológia fokozott és jelentős növekedése arra kényszeríti a szervezeteket, hogy SCADA-rendszereiket a szabadalmaztatott technológiáról és a protokollalapú rendszerekről az internetalapúakra állítsák át. Ez a paradigmaváltás megnövelte a SCADA-rendszereket célzó kockázatokat is.[3] A kritikus infrastruktúrában számos szervezet telepített SCADA-/ICS-rendszert a folyamatok vezérlésének és az adatgyűjtésnek az automatizálására. Ezek a rendszerek nagy értékű célpontokká váltak az üzleti műveletek megzavarására törekvő támadók számára.[4] Ennek kitűnő példája, hogy 2022 augusztusában[5] az Egyesült Királyságban egy zsarolóvírus-csoport legalább egy vízszolgáltatót megtámadott, de némi zavar van abban, hogy valójában kinek a rendszereit törték fel. A Cl0p csoport weboldalán megjelent, hogy betörtek a Thames Water rendszereibe, amely az Egyesült Királyság legnagyobb víz- és szennyvízszolgáltatójaként hirdeti magát, és 15 millió embert szolgál ki. Kiberbiztonsági szakértők azonban rámutattak, hogy bár a Cl0p a Thames Watert nevezi meg a weboldalán, a betörés bizonyítékaként kiszivárgott fájlok valójában egy másik, a South Staffordshire nevű vízszolgáltatóhoz tartoznak, amelynek leányvállalatai, a South Staffs Water és a Cambridge Water 1,6 millió embert és több tízezer vállalkozást szolgálnak ki az Egyesült Királyságban. Pár nappal később a South Staffordshire megerősítette, hogy kiberbűnözők célpontja lett.

[3] Krasznay 2019: 25–29.
[4] Tóth 2022: 123–132.
[5] Kovacs 2022.

Ebből fakadóan jelen kutatás célja a releváns hazai és nemzetközi szakirodalmak vizsgálatával meghatározni azokat a kiberbiztonsági kihívásokat, amelyek a SCADA-rendszereket érintik. Első lépésként szükséges felmérni, hogy milyen elemekből épül fel egy ilyen rendszer, illetve mely folyamatok során alkalmazzák ezeket a különböző létfontosságú rendszerelemek létesítményeiben. Ezáltal összegyűjtöm és rendszerezem a lehetséges kiberbiztonsági fenyegetéseket, mind általánosan, mind pedig rendszerspecifikusan.

Kutatási módszertan

Elsődlegesen a hazai és nemzetközi releváns szakirodalmak feldolgozásával a SCADA-rendszerek felépítését, használatát, valamint működésének szabályait határozom meg, a létfontosságú rendszerelemek definiálása mellett. A jogszabályok, szabványok esetében összehasonlító elemzést végzek a hazai és nemzetközi szabályozások tekintetében. Ezt követően rendszerezem a kiberbiztonsági fenyegetéseket – annak bekövetkezési éve, a támadás típusa, illetve az érintett szektor szempontjai alapján.

SCADA-rendszerek és a létfontosságú rendszerelemek

Az ICS egy általános kifejezés, amely többféle vezérlőrendszer-típust foglal magában, beleértve a felügyeleti vezérlő és adatgyűjtő (SCADA-) rendszereket, a Distributed Control Systems, azaz elosztott vezérlőrendszereket (DCS) és más vezérlőrendszer-konfigurációkat, például az ipari ágazatokban és a kritikus infrastruktúrákban – vagy a magyar szabályozói megnevezés szerint létfontosságú rendszerelemekben – megtalálható Programmable Logic Controllers, vagyis programozható logikai vezérlőket (PLC). Az ipari vezérlőrendszer olyan vezérlőelemek (például elektromos, mechanikus, hidraulikus, pneumatikus) kombinációiból áll, amelyek együttesen működnek egy ipari cél (például gyártás, anyag- vagy energiaszállítás) elérése érdekében.[6]

A DCS-ek olyan számítógépes szoftvercsomagok, amelyek kommunikálnak a vezérlő hardverrel, és Human Machine Interface-t, azaz központosított ember-gép interfészt (HMI) biztosítanak a vezérelt berendezések számára.[7] A PLC olyan szilárdtestes vezérlőrendszer, amely felhasználó által programozható memóriával rendelkezik utasítások tárolására, illetve olyan speciális funkciók megvalósítása céljából, mint a bemenetek/kimenetek vezérlése, logika, időzítés, számlálás, három üzemmódú vezérlés, kommunikáció, aritmetika, valamint adat- és fájlfeldolgozás.[8]

A SCADA-rendszerek több komponensből tevődnek össze – hardverkomponensekből és szoftverprogramokból, ahol a hardver magában foglalja a Remote Terminal Units, azaz a távoli terminálegységeket (RTU), a Master Terminal Unitot, vagyis a főterminálegységet (MTU), a működtetőket és az érzékelőket. A szoftverprogramok a HMI-ből,

[6] National Institute of Standards and Technology 2020.
[7] Dunn 2015: 103–110.
[8] Stouffer 2020.

a Historian, tehát a központi adatbázisból és más felhasználói szoftverekből állnak. Ezek a szoftverek biztosítják a hardver és a szoftver közötti kommunikációs interfészt. A fizikai környezet kapcsolódik a működtető eszközökhöz és érzékelőkhöz, amelyek tovább kapcsolódnak az RTU-khoz. Az RTU-k összegyűjtik az érzékelők információit és adatait, és a telemetriai adatokat továbbítják az MTU-nak a SCADA-rendszer megfigyelésére és vezérlésére.[9] A mélyebb betekintés érdekében az egyes komponensek működésének, feladatainak ismertetése is szükséges, amelyek a következők:

- Az RTU felelős a valós idejű adatok és információk gyűjtéséért a fizikai környezethez LAN-/WAN-kapcsolaton keresztül csatlakoztatott érzékelőkből. Az RTU-k továbbítják az információkat az MTU-nak. Ezek felelősek továbbá a rendszerhez kapcsolódó fizikai eszközök aktuális állapotadatainak továbbításáért.
- Az MTU a központi felügyeleti állomás. Feladata a vezérlés, az RTU-gépek kommunikációs kapcsolatokon keresztüli vezérléséért és irányításáért felelős. Válaszol az RTU-tól érkező üzenetekre is, valamint feldolgozza és tárolja az adatokat.
- A HMI kommunikációs interfészt biztosít a SCADA hardver- és szoftverkomponensek között. Felelős a SCADA működési információinak vezérléséért, például az RTU és MTU közötti vezérlésért, felügyeletért és kommunikációért, szöveg, statisztika vagy más érthető tartalom formájában.
- A Historian a kétirányú kommunikációs adatok, események és riasztások felhalmozására szolgál. Leírható központi adatbázisként vagy távoli helyen található szerverként. A Historiant a HMI-n megjelenő grafikus trendek feltöltéséhez kérdezik le.
- A kommunikációs hálózat kommunikációs szolgáltatásokat nyújt a SCADA-rendszer különböző összetevői között. A használt közeg lehet vezeték nélküli vagy vezetékes.[10]

A SCADA-rendszer fő célja az ipari folyamatok berendezéseinek felügyelete és vezérlése. Így több területen is alkalmazzák ezeket: gyártás, vízgazdálkodás, olaj- és gázellátás, szállítás, megújuló energiaforrások, valamint az áramelosztás és -szabályozás területén is. Ezekben az iparágakban a SCADA-rendszerek értékes információkat szolgáltatnak a kulcsfontosságú érdekelt feleknek. A rendszer segítségével javíthatják az ipari üzemek teljesítményét, nyomon követhetik az üzemek hatékonyságát, és a rendszertől kapott üzeneteken keresztül mérsékelhetik a hibákat és a leállásokat. Napjaink fejlett ipari világában a SCADA-rendszerek kulcsfontosságúak az ipari üzemek hatékonyabb működéséhez, mivel sokkal könnyebben és gyorsabban gyűjtik össze a lényeges adatokat. Ez sok vállalkozásnál lehetővé teszi az erőforrások jobb elosztását. A SCADA-rendszer számos különböző típusú berendezéshez csatlakozik: az időjárás-érzékelőktől és szivattyúktól az energiatermelésig és a motorokig mindent felügyel és vezérel, attól függően, hogy milyen adatokra van szükség.[11]

[9] Yadav–Paul 2021.
[10] Pathak–Patel 2014: 1639–1699.
[11] Lásd: https://scada-international.com/what-is-scada/

A rendszer felépítése és alkalmazási területei mellett érdemes kitérni arra, hogy általánosságban milyen előnyei lehetnek a használatának. Ennek részleteit az 1. táblázat foglalja össze.

1. táblázat: A SCADA-rendszer előnyei

Tulajdonság	Leírás
Sokoldalúság	A SCADA-t heterogén eszközök összekapcsolására fejlesztették ki. A számos rendelkezésre álló meghajtó lehetővé teszi a csatlakozást bármilyen típusú és összetettségű eszközhöz, így lehetséges a PLC, valamint a speciális célú eszközök vagy kommunikációs multiplexer vezérlése minden átviteli módszerrel és médiával.
Sebesség	Az eseményvezérelt architektúra rendkívül gyors válaszidőt tesz lehetővé, ezért a rendszer teljesítményét nem befolyásolja a csatlakoztatott bemenetek/kimenetek száma.
Hatékonyság	A SCADA korlátozott memória- és feldolgozási teljesítményt igényel, ami lehetővé teszi a költséghatékony konfigurációkat, amelyek még mindig képesek használni a rendszer összes funkcióját.
Könnyű használat	A kezdeményezést fejlesztő környezet és a természetes használat: az interfész, valamint a projekt helyességének bármikori ellenőrzése lehetővé teszi a komplett alkalmazások órák alatti fejlesztését, napok vagy hónapok helyett.
Megbízhatóság	A SCADA moduláris és védett felépítése az egyik olyan elem, amely növeli a rendszer stabilitását és megbízhatóságát, lehetővé téve az üzemeltető számára, hogy csak kiválasztott modulokat kapcsoljon ki és frissítsen anélkül, hogy az egész rendszer leállna.
Kompakt jelleg	A SCADA-t kifejezetten a rendszer erőforrásainak hatékony felhasználására tervezték, amit a nagymértékben optimalizált kódok és algoritmusok révén érnek el.
Biztonság	Az összes végrehajtott művelet szigorúan ellenőrzött és auditált. Az üzemeltetők a rendszernek csak az általuk engedélyezett részét használhatják.
Funkciók	A SCADA leegyszerűsíti az adatbázis létrehozását és a konfigurációs eljárást az űrlapok kitöltésére, így csak a projekt valóban szükséges paramétereit határozza meg. Ezek a módszerek nemcsak a tervező feladatát könnyítik meg, hanem ténylegesen meg is mutatják a megfelelő módszert a világos és teljes dokumentáció automatikus létrehozására.
Szelektív riasztáskezelés	A riasztások logikai csoportokba rendezhetők és prioritással láthatók el, így lehetővé téve az adott üzem különböző részeihez kapcsolódó értesítések áttekintését, valamint a kevésbé jelentős riasztások elrejtését egy adott állapotban.
Online konfiguráció	Minden SCADA-projekt-paraméter – akár adatbázis-objektum, akár grafikus szimbólum – online hozzáadható, módosítható vagy törölhető, miközben az összes valós idejű felügyeleti és vezérlési tevékenység aktív marad. Ez a funkció növelheti a projektek összehangolásának sebességét, amelyet általában az ügyfél telephelyén végeznek el az összes eszköz rendszeres működése mellett.

Forrás: a szerző szerkesztése G. L. 2016 alapján

Az előző rész alapján kijelenthető, hogy ezek a rendszerek kiemelt jelentőségűek egy ország és annak állampolgárai szempontjából egyaránt. Ebből következik, hogy a biztonság is kiemelt szerepet kap a rendszer kialakításánál és működtetésénél.[12] Különböző

[12] Paráda–Farkas 2020: 159–182.

előírásoknak kell megfelelni a biztonságos működés érdekében, amelyek egyik pillérét általánosságban SCADA biztonsági keretrendszernek nevezik. Ez különféle biztonsági intézkedéseket foglal magában, amelyek képesek kezelni a különböző problémákat:

- adminisztratív intézkedések: szervezet vezetése és biztonsága, szabványok, irányelvek és kivételek, kockázatértékelés, oktatás és képzés, megfelelőségi keretrendszer;
- SCADA-intézkedések: sérülékenységmenedzsment, fizikai biztonság, hálózati biztonsági ellenőrzések, identitás- és hozzáférés-kezelés, adatvagyon-menedzsment;
- alkalmazás és adatbiztonság: adatbiztonság, alkalmazásbiztonság, rosszindulatú kódok megelőzése és észlelése, változáskezelés;
- rendszer biztosítása: biztonságos konfiguráció, rendszer ellenálló képessége, üzletmenet-folytonosság és katasztrófa-helyreállítás tervezése;
- ellenőrző intézkedések: forensics, fenyegetés monitorozása, incidenskezelés;
- külső intézkedések: partnerbiztonsági menedzsment, szállítói biztonsági menedzsment.

Az előbbi intézkedések összefoglalva egy biztonságpolitikát alkotnak. Ezek a politikák, stratégiák létfontosságúak a fenntartható biztonsági rendszer kiépítéséhez.[13] Emellett a megfelelő adminisztráció is elengedhetetlen, ugyanis az előbb említett elemek nélkül lehetetlenné válik a rendszer megfelelő működése, hiszen kiszolgáltatott lesz a különböző sebezhetőségeknek.[14] Azonban nemcsak politikát, stratégiát, hanem más konkrét biztonsági dokumentumot, például biztonsági tervet és végrehajtási iránymutatást is lehet és kell készíteni a SCADA-rendszerben alkalmazandó konkrét gyakorlatok meghatározása érdekében.[15]

Emellett az ISA112 SCADA-rendszerek szabványügyi bizottsága aktívan dolgozik egy sorozat ISA-szabvány és műszaki jelentés kidolgozásán. A 2016-ban létrehozott bizottság munkájában jelenleg több mint 200 SCADA-szakértő vesz részt a világ minden tájáról, akik az iparágak széles körét képviselik. A két önkéntes társelnök által vezetett bizottság arra törekszik, hogy a következő felek között egyenletes egyensúly legyen: végfelhasználók, gyártók, forgalmazók, tanácsadók, mérnöki irodák, vállalkozók, rendszerintegrátorok, kormányzati szabályozók és más érdekelt felek. A szabvány- és jelentéssorozat a csővezetékek, a víz- és szennyvíz-, az energia-, az olaj- és gázipar, valamint más iparágak SCADA-rendszereinek rendszertervezésével, megvalósításával, üzemeltetésével és karbantartásával foglalkozik, így támogatva e rendszerek általános integritását és megbízhatóságát. A szabványok és a műszaki jelentések célja, hogy útmutatást nyújtsanak a SCADA-rendszerek tervezéséhez, megvalósításához, üzemeltetéséhez és karbantartásához azáltal, hogy számos iparágban dokumentálják a legjobb gyakorlatokat. A tervek szerint egy vagy több szabványt dolgoznak ki, amelyeket a megvalósítás részleteit és az iparágspecifikus iránymutatásokat kibővítő műszaki jelentések egészítenek ki. Jelenleg a belső bizottsági véleményezési és szerkesztési feladatok zajlanak, az első ISA112 szabványdokumentum közzétételét 2023 őszére tervezik.[16]

[13] Lásd: www.logsign.com/blog/scada-cybersecurity-framework
[14] Megyeri–Farkas 2017: 198–209.
[15] Lásd: www.logsign.com/blog/scada-cybersecurity-framework
[16] Lásd: www.isa.org/standards-and-publications/isa-standards/isa-standards-committees/isa112

Továbbá vannak bizonyos jogszabályi kötelezettségek is, amelyek vonatkoznak a SCADA-t használó üzemekre, vállalkozásokra, ilyen például az Európai Unió (EU) tagállamaiban érvényes 2016/1148 (EU) európai parlamenti és tanácsi irányelv (2016. július 6.) a hálózati és információs rendszerek biztonságának az egész Unióban egységesen magas szintjét biztosító intézkedésekről, röviden a NIS-irányelv.[17] Ennek hatálya alá tartozik az elektromosság, víz (beleértve a kezelést és a hulladékot), olaj-gáz, egészségügy, szállítás, digitális infrastruktúra (beleértve a felhőalapú tárolást, az online piactereket és a keresőmotorokat) iparágak. Az irányelv nemcsak e szolgáltatások és infrastruktúrák szolgáltatóit és üzemeltetőit érinti, hanem az egész európai társadalmat is. 2018 májusában lépett hatályba az összes EU-tagországban, és különleges követelményeket határoz meg a biztonsági kockázat kezelése, a kibertámadások elleni védelem, a kiberbiztonsági események észlelése és a kiberincidensek hatásának minimalizálása terén. Ez magában foglalja a kritikusinfrastruktúra-szolgáltatók és az alapvető szolgáltatások üzemeltetőinek információtechnológiai rendszereire, valamint az üzemeltetési technológiai rendszerekre vonatkozó irányelvi követelményeket, beleértve az ipari vezérlőrendszereket, például a SCADA-t is.[18] Kiemelendő, hogy a folyamatos fejlődés miatt a jogszabályok előírják, hogy a jogalanyok a védendő üzleti értékek alapján meghatározott kockázatalapú megközelítést alkalmazzanak, valamint megelőző és reagáló biztonsági kontrollokat alakítsanak ki. Ez a megközelítés optimális költségeket biztosíthat az informatikai, információs vagy kiberbiztonsági irányítási rendszer számára.[19]

Mindemellett az Európai Kiberbiztonsági Ügynökség (ENISA) jelentése tartalmazza a különböző szabványokat az ipari irányítórendszerekre vonatkozóan, amelyben megjelennek kifejezetten a SCADA-rendszerekre vonatkozó szabványok, iránymutatások. Ennek összefoglalását a 2. táblázat tartalmazza.[20]

2. táblázat: Szabványok és iránymutatások

Hatókör	Típus	Név	Bevezetés dátuma	Rövid leírás
Nemzetközi	Szabvány	IEEE 1711. Próbahasználati szabvány az alállomási soros vonal kiberbiztonságára szolgáló kriptográfiai protokollhoz	2011. február	Az IEEE 1711 egy speciális soros biztonsági protokollt határoz meg kétféle kriptográfiai modul számára: SCADA kriptográfiai modulok (SCM) a soros SCADA-csatorna védelmére és karbantartási kriptográfiai modulok (MCM) a karbantartási csatorna védelmére, amely általában egy betárcsázós kapcsolat.

[17] A cikk készítésének ideje alatt megjelenés alatt volt a NIS2-irányelv, azonban még nem lépett hatályba, így a szerző a korábbi irányelvet veszi alapul.
[18] Lásd: www.awencollective.com/nis-directive
[19] Bederna–Rajnai–Szádeczky 2021: 139–148.
[20] ENISA 2011.

Hatókör	Típus	Név	Bevezetés dátuma	Rövid leírás
Multi-laterális kezdemé-nyezések	Iránymu-tatás (jó gyakorlat)	Ipari vezér-lőrendszerek kiberbiztonsági értékelése. A jó gyakorlat útmutatója	2011. április	A dokumentum célja, hogy megismertesse az objektum tulajdonosait a kiberbiztonsági tesztelés általános folyamatával, és bete-kintést nyújtson a konkrét tesztelési mód-szerekbe, hogy a tulajdonosok megtanulják előírni az egyéni értékelést, amely maximali-zálja a tesztelési költségvetésük kimenetelét.
Nagy-Britannia	Iránymu-tatás (jó gyakorlat)	Jó gyakorlatok útmutató-ja – Folya-matirányítás és SCADA-biz-tonság	2008. június	Az iránymutatás hét elemből álló keretrend-szert javasol a következőkre a folyamatirá-nyítás biztonságának kezeléséhez. Általános útmutatás • Üzleti kockázat • Biztonságos architektúra bevezetése • Reagálási képességek kialakítása • Tudatosság és készségek fejlesztése • Harmadik fél kockázatának kezelése • Projektek bevonása • Folyamatos irányítás kialakítása
Nagy-Britannia	Iránymu-tatás (jó gyakorlat)	Tűzfal telepítése SCADA- és fo-lyamatirányító hálózatokhoz. A jó gyakorlat útmutató	2008. június	Ez a dokumentum a SCADA-tűzfal-telepítés jelenlegi gyakorlata vizsgálatának és össze-állításának eredménye. A cél az volt, hogy megvizsgálja a tűzfal-architektúrák, a tele-pítés és az ipari vezérlőkörnyezet védelmére használt menedzsment „korszerűségét”.
Svédország	Iránymu-tatás (jó gyakorlat)	Útmutató az ipari ve-zérlőrendszer fokozott biztон-ságához	2010. május	Ez az útmutató alapvető ajánlásokat tartal-maz az ipari vezérlőrendszerek biztonságára vonatkozóan. A dokumentum tippeket is ad arra vonatkozóan, hogy hol találhat további információkat. Az általunk nyújtott ajánlá-sok nemzetközileg elismert ajánlásokhoz, gyakorlatokhoz és szabványos munkamód-szerekhez kapcsolódnak.
Amerikai Egyesült Államok	Útmutató (műszaki jelentés és jó gya-korlat)	NIST SP 800-82. Út-mutató az ipari vezérlőrendsze-rek (ICS) biztон-ságához	2011. június	A dokumentum célja, hogy útmutatást adjon az ICS rendszerek biztonságossá téte-léhez, beleértve a SCADA-, a DCS és más, vezérlési funkciókat ellátó rendszereket. A dokumentum áttekintést ad az ICS-ről és a tipikus rendszertopológiákról, azonosít-ja e rendszerek tipikus fenyegetéseit és se-bezhetőségeit, és javasolt biztonsági ellenin-tézkedéseket kínál a kapcsolódó kockázatok mérséklésére.

Hatókör	Típus	Név	Bevezetés dátuma	Rövid leírás
Amerikai Egyesült Államok	Útmutató	Terepi eszköz-védelmi profil SCADA-rendszerekhez közepes robusztusságú környezetekben	2006. június	Ez a védelmi profil meghatározza az Egyesült Államok kormánya vagy kereskedelmi szervezete által közepes robusztusságú környezetben használt SCADA terepi eszközök minimális biztonsági követelményeit. A SCADA-eszköztulajdonosok számára ez a védelmi profil hasznos a vásárlási specifikációk során figyelembe vehető követelmények azonosításában. Alternatív megoldásként az eszköztulajdonosok megkövetelhetik a termékektől, hogy igazolják a jelen védelmi profilnak való megfelelést.
Amerikai Egyesült Államok	Iránymutatás (jó gyakorlat)	API 1164, Pipeline SCADA-biztonság	2009. június	Ez az iránymutatás kifejezetten arra szolgál, hogy az üzemeltetők rendelkezésére bocsássa a SCADA biztonságával kapcsolatos iparági gyakorlatok leírását, és hogy biztosítsa a megfelelő biztonsági gyakorlatok kialakításához szükséges keretet az üzemeltető egyes vállalatain belül.
Amerikai Egyesült Államok	Szabvány	12. számú AGA jelentés. A SCADA-kommunikáció kriptográfiai védelme	2006. március	Az AGA 12 sorozat célja, hogy időt és energiát takarítson meg a SCADA-rendszerek tulajdonosainak azáltal, hogy egy olyan átfogó rendszert javasol, amelyet kifejezetten a SCADA-kommunikáció védelmére terveztek. A végfelhasználók az AGA 12 sorozatot használhatják a SCADA kiberbiztonsági megoldás beszerzése általános követelményeinek meghatározására, ha ezt az előírást beépítik a beszerzési követelményeikbe. A rendszerintegrátorok az AGA 12 sorozatot használhatják annak biztosítására, hogy a SCADA-kiberbiztonságot megfelelően specifikálják, és hogy a rendszer tesztelési terve megfeleljen a biztonsági megoldás üzembe helyezéséhez szükséges valamennyi követelménynek. Végül a SCADA hardver-, szoftver- és firmware-gyártói használhatják az AGA 12 sorozatot annak biztosítására, hogy termékkínálatuk megfeleljen a végfelhasználó SCADA-kiberbiztonsággal kapcsolatos igényeinek.

Forrás: a szerző szerkesztése ENISA alapján

A táblázat alapján látható, hogy az Amerikai Egyesült Államokban már korábban, 2006-tól kezdődően nagy hangsúlyt fektetnek a SCADA-rendszerek biztonságos kialakítására és működtetésére, aminek oka a vállalatok üzleti kockázatainak csökkentése is. Az iránymutatások, útmutatók mellett megtalálható egy szabvány is, azonban ez európai viszonylatban nem mondható el – a kontinensen útmutatások, jó gyakorlatok vannak érvényben. Továbbá megállapítható az is, hogy időben viszonylag szorosan követi az amerikai tevékenységeket az európai gyakorlat. Elmondható azonban az is, hogy nemzetközi szinten, illetve multilaterális kezdeményezések útján implementálható szabvány, valamint további jó gyakorlat egyaránt megtalálható mindkét kontinensen.

Létfontosságú rendszerelemek megjelenési formái

Magyarországon a létfontosságú rendszerelem kifejezés van érvényben a törvényi szabályozás szerint, azonban a gyakorlatban rendszerint használják a kritikus infrastruktúra kifejezést is – nemzetközi viszonylatban utóbbi megnevezést használják kizárólagosan.[21]

A hazai szabályozás értelmében a létfontosságú rendszerelem a törvény 1. számú mellékletében meghatározott ágazatok valamelyikébe tartozó szolgáltatás, eszköz, létesítmény vagy rendszer olyan rendszereleme, illetve azok által nyújtott szolgáltatások, amelyek elengedhetetlenek a létfontosságú társadalmi feladatok ellátásához, továbbá amelynek kiesése a meghatározott feladatok folyamatos ellátásának hiánya miatt jelentős következményekkel járna.

Az 1. számú mellékletben nevesített ágazatok és a hozzájuk tartozó alágazatok a következők:

- *Energia* – villamosenergia-rendszer létesítményei (kivéve az atomerőmű nukleáris biztonságára és sugárvédelmére, fizikai védelmére, valamint biztosítéki felügyeletére vonatkozó szabályozás hatálya alá tartozó rendszerek és rendszerelemek), kőolajipar, földgázipar és távhő;
- *Közlekedés* – közúti, vasúti, légi, vízi közlekedés és logisztikai központok;
- *Agrárgazdaság* – mezőgazdaság, élelmiszeripar és elosztó hálózatok;
- *Egészségügy* – aktív fekvőbeteg-ellátás, és a működtetéséhez szükséges szolgáltatások, mentésirányítás, egészségügyi tartalékok és vérkészletek, magas biztonsági szintű biológiai laboratóriumok és gyógyszer-nagykereskedelem;
- *Társadalombiztosítás* – társadalombiztosítási ellátások igénybevételéhez kapcsolódó informatikai rendszerek és nyilvántartások;
- *Pénzügy* – pénzügyi eszközök kereskedelmi, fizetési, valamint klíring- és elszámolási infrastruktúrái és rendszerei, bank- és hitelintézeti biztonság és készpénzellátás;
- *Infokommunikációs technológiák* – internethozzáférési szolgáltatás és internetinfrastruktúra, elektronikus hírközlési szolgáltatások, elektronikus hírközlő hálózatok, műsorszórás, postai szolgáltatások és kormányzati elektronikus információs rendszerek;
- *Víz* – ivóvíz-szolgáltatás, felszíni és felszín alatti vizek minőségének ellenőrzése, szennyvízelvezetés és -tisztítás, vízbázisok védelme és árvízi védművek, gátak;

[21] 2012. évi CLXVI. törvény.

- *Honvédelem* – honvédelmi rendszerek és létesítmények;
- *Közbiztonság-védelem* – rendvédelmi szervek infrastruktúrái.

Emellett a jogszabály nevesíti a nemzeti létfontosságú rendszerelemet is, amelyet szintén a törvény alapján jelölnek ki, és annak kiesése a létfontosságú társadalmi feladatok folyamatos ellátásának hiánya miatt, elsősorban Magyarországon lenne jelentős hatással. Továbbá megjelenik az alapvető szolgáltatás fogalma is, amely úgy definiálható, hogy a kritikus társadalmi vagy gazdasági tevékenységek fenntartásához szükséges, elektronikus információs rendszertől függő, az alapvető szolgáltatások jegyzékében feltüntetett szolgáltatás.[22] Az egyes ágazatonkénti, valamint ágazatonként lebontott alapvető szolgáltatások jegyzéke a 65/2013. (III. 8.) Korm. rendelet 3. mellékletében található meg.

A magyar szabályozáshoz hasonlóan a korábbi alfejezetben említett NIS-irányelv is alkalmazza az alapvető szolgáltatások kifejezést, kifejezetten szereplőként hivatkozva azon – a II. mellékletben – említett közjogi vagy magánjogi szervezetre, amely a kritikus társadalmi és/vagy gazdasági tevékenységek fenntartásához alapvető szolgáltatást nyújt, az adott szolgáltatás nyújtása hálózati és információs rendszerektől függ, és az említett szolgáltatást érintő biztonsági esemény jelentős zavart okozna a szolgáltatás nyújtásában. Az irányelv ágazatok és alágazatok tekintetében bizonyos eltérést mutat a hazai szabályozáshoz képest – ennek oka, hogy az iránymutatást az országspecifikus tényezők határozzák meg a saját jogszabály kialakítása folyamán.[23] Elmondható, hogy a magyar szabályozás bővebb, több ágazatot nevesít, illetve az alágazatok is részletesebbek, specifikusabbak.

A hazai és EU-s viszonylathoz képest az amerikai A kritikus infrastruktúrák biztonsága és ellenálló képessége elnöki politikai irányelv 21 (PPD-21) nemzeti politikát dolgoz ki a biztonságos, működőképes és ellenálló infrastruktúrák megerősítésére és fenntartására. Ez 16 olyan infrastrukturális ágazatot nevesít, amelynek fizikai vagy virtuális eszközei, rendszerei és hálózatai létfontosságúak az Egyesült Államok számára. Ezek működésképtelensége vagy megsemmisülése gyengítő hatással lenne a biztonságra, a nemzetgazdaság biztonságára, a nemzeti közegészségügyre vagy közbiztonságra, vagy ezek bármely kombinációjára. Az irányelv a következő ágazatokat nevezi meg:

- vegyipari ágazat;
- kereskedelmi létesítmények ágazata;
- kommunikációs ágazat;
- kritikus termelési ágazat;
- gátágazat;
- védelmi ipari bázis ágazat;
- sürgősségi szolgáltatási ágazata;
- energiaágazat;
- pénzügyi szolgáltatások ágazata;
- élelmiszeripari és mezőgazdasági ágazat;
- kormányzati létesítmények ágazata;

[22] 2012. évi CLXVI. törvény.
[23] 2016/1148 (EU) irányelv.

- egészségügyi és közegészségügyi ágazat;
- informatikai ágazat;
- nukleáris reaktorok, anyagok és hulladékok ágazat;
- közlekedési rendszerek ágazata;
- víz- és szennyvízrendszerek ágazata.[24]

Megfigyelhetők hasonlóságok a korábban ismertetett szabályozásokkal, azonban az amerikai jogszabály nem nevesít alágazatokat. Mindazonáltal szükséges nagyobb figyelmet szentelni az informatika ágazatának. Ez a szektor központi szerepet játszik a nemzet biztonsága, gazdasága, valamint közegészségügye és közbiztonsága szempontjából, mivel a vállalkozások, kormányok, felsőoktatási intézmények és magánszemélyek egyre inkább függnek az informatikai ágazat funkcióitól. Ezek a virtuális és elosztott funkciók hardvert, szoftvert, informatikai rendszereket és szolgáltatásokat foglalnak magukban, valamint – a kommunikációs ágazattal együttműködve – kialakítják és biztosítják az internetet. Az ágazat összetett és dinamikus környezete megnehezíti a fenyegetések azonosítását és a sebezhetőségek értékelését, illetve megköveteli, hogy ezeket a feladatokat együttműködő és kreatív módon oldják meg a szervezetek. Az informatikai ágazat funkcióit olyan szervezetek – gyakran tulajdonosok és üzemeltetők, valamint a hozzájuk tartozó egyesületek – kombinációja működteti, amelyek fenntartják és újjáépítik a hálózatot, beleértve az internetet is. Bár az informatika infrastruktúra bizonyos fokú ellenálló képességgel rendelkezik, az egymástól függő és összekapcsolt kialakítás kihívásokat és lehetőségeket is jelent a köz- és magánszektor felkészültségi és védelmi tevékenységeinek összehangolása szempontjából. A létfontosságú rendszereknek – legyenek azok orvosi eszközök, internetre csatlakozó autók, SCADA, ICS vagy más rendszerek – döntő szerepük van a mai világban. Egyre több ilyen rendszer kapcsolódik össze a dolgok internetével (Internet of Things/IoT), azaz egyre nyilvánvalóbbá válik, hogy ezeket a rendszereket megfelelően kell védeni a hackerektől és a kibertámadásoktól.[25]

Kiberbiztonsági fenyegetések

Kifejezetten kritikus infrastruktúrát, annak is a SCADA-rendszerét érintő első kibertámadást 1982-ben jegyezték. Szibériai csővezeték-robbanás néven ismert az incidens, amely során a támadók trójai vírust telepítettek a SCADA-rendszerbe, amely a szibériai csővezetéket irányítja. Ez egy 3 kilotonna TNT-vel egyenértékű robbanást okozott. Ezt követően 1992-ben történt a Chevron vészjelző rendszer incidense. A Chevron vészhelyzeti riasztóhálózatának egy elbocsátott alkalmazottja úgy tette tönkre a cég riasztórendszerét, hogy feltörte a New York-i és a kaliforniai San José-i számítógépeket, és úgy konfigurálta át őket, hogy összeomoljanak. A vandalizmusra csak akkor derült fény, amikor a kaliforniai Richmondban található Chevron finomítóban vészhelyzet alakult ki, és a rendszer nem tudta értesíteni a szomszédos közösséget egy mérgező anyag felszabadulásáról. Amikor a rendszer tíz órán át nem működött, 22 államban

[24] Lásd: www.cisa.gov/critical-infrastructure-sectors
[25] Lásd: www.cisa.gov/information-technology-sector

és Kanada hat, meg nem határozott területén emberek ezrei kerültek veszélybe. Két évvel később, 1994. július 8. és augusztus 31. között egy támadó jogosulatlan hozzáférést szerzett a Salt River Project számítógépes hálózatához egy betárcsázós modemen keresztül, hogy hozzáférjen a számlázási programhoz és számlázási információkhoz. Egy backdoor[26]-t telepített a rendszerbe, amely későbbi időpontban való hozzáférést biztosított számára. Abban az időben a Salt River Project víztisztító SCADA-rendszer egy 131 mérföld hosszú csatornarendszert működtetett, amely a Phoenix nagyvárosi körzetében lévő fogyasztóknak szállított vizet. A támadók legalább 5 órán keresztül fértek hozzá a rendszerhez, amely a csatornákat irányította. Kompromittálódtak a víz- és áramfigyelés adatai, valamint a szállításra vonatkozó, pénzügyi, ügyfél- és személyes adatok. Ezek közé tartoztak a bejelentkezési és jelszófájlok, a számítógépes rendszer naplófájljai, valamint a root jogosultságok.[27] Jól látható, hogy már a 2000-es évek előtt megjelentek a SCADA-rendszerek elleni kibertámadások. Az ezredfordulót követően világszinten példaként szolgáló a Stuxnet incidens, amelyben a támadás célpontja az iráni nukleáris létesítmény volt Natanzban. A Stuxnet négy darab 0. napi sebezhetőséget (korábban ismeretlen sebezhetőségeket, így nem volt idő a javítások kifejlesztésére és terjesztésére) használt ki. A féreg a Siemens alapértelmezett jelszavait használta a Windows WinCC és PCS7 programokat futtató operációs rendszerekhez. Ezt kihasználva megváltoztatta az elektromos áram frekvenciáját a hajtóművekben, így magas és alacsony fordulatszámok váltakoztak, ebből következően a centrifugák a normálisnál nagyobb arányban hibásodtak meg.[28]

Az elmúlt években is több létfontosságú rendszerelemet érintő támadásról számoltak be, ezek közül a legjelentősebbeket – amelyekben a SCADA-rendszer is érintett volt – a 3. táblázat tartalmazza.

3. táblázat: A legjelentősebb SCADA-rendszereket célzó kibertámadások 2012–2022 között

Elnevezés	**Év**	**Támadás formája**	**Érintett szektor(ok)**
Shamoon	2012	malware	energia (villamos energia és földgáz)
New York Dam	2013	rendszer feltörése	víz (árvízi védművek, gátak)
German Steel Mill	2014	rendszer feltörése	energia (földgázipar)
Ukrajna villamosenergia-hálózata	2015	malware	energia (villamos energia)
„Kemuri"	2016	rendszer feltörése	víz (ivóvíz-szolgáltatás)
Ukrajna villamosenergia-hálózata II.	2016	malware	energia (villamos energia)
SamSam	2018	ransomware	infokommunikációs technológiák (kormányzati elektronikus információs rendszerek)

(Megjegyzés: a táblázat készítése során a támadások célpontjait figyelembe véve rendeltem hozzá a magyar szabályozásban megnevezett szektorokat.)

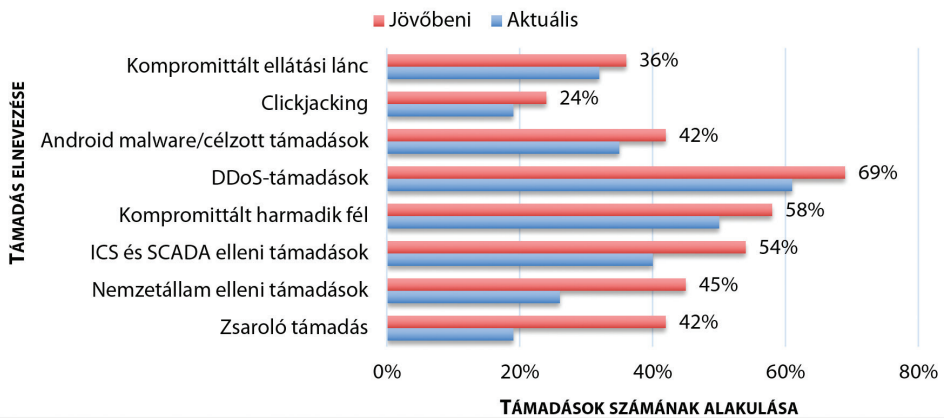
Forrás: a szerző szerkesztése DPS Telecom 2021. alapján

[26] Szoftverbe (vagy ritkább esetben hardverbe) épített olyan funkció, amelynek segítségével illetéktelen személyek hozzáférnek a programhoz, a géphez vagy annak bizonyos részeihez. Lásd: https://lexiq.hu/backdoor

[27] A root jog a legalapvetőbb, mindenre kiterjedő jogosultságot jelenti. Lásd: https://lexiq.hu/root

[28] Miller–Rowe 2012: 51–56.

A Raytheon és a Ponemon Institute 2017-ben készített egy tanulmányt, amelyben több mint 1100 vezető IT-szakembert kérdezett meg az Egyesült Államokban, Európában és a Közel-Keleten/Észak-Afrikában. Arra kérték őket, hogy értékeljék, mely kiberfenyegetések a leggyakoribbak ma, és várhatóan melyek fognak növekedni a következő három évben. A tanulmányban részt vevő szakemberek szerint a SCADA-rendszereket, valamint a nemzetállamokat érintő fenyegetések és a zsaroló támadások gyakorisága a jelenlegi szintekhez képest várhatóan emelkedni fog. Míg jelenleg a szakemberek 40%-a a SCADA-t jelöli meg gyakori problémaként, addig ez a szám 54%-ra ugrik fel a jövőben várható gyakoriság tekintetében.[29] Az elkészített elemzéshez tartozó statisztikai adatokat összefoglaló diagram a következő (1. ábra).



1. ábra: Kibefenyegetések alakulása szakemberek szerint 2017-ben
Forrás: a szerző szerkesztése Petrosyan 2023. alapján

Általánosságban elmondható, hogy újabb és újabb fenyegetéstípusok jelentek meg az idő előrehaladtával – például cryptojacking –, amellyel a szakembereknek korábban nem kellett szembenézniük. Az ipar 4.0 technológiák bevezetésével pedig a rendszerek hálózati támadásoknak való kitettsége fog várhatóan növekedni.[30]

Összegzés

Összegezve a leírtakat elmondható, hogy a SCADA-rendszerek szorosan kapcsolódnak a létfontosságú rendszerelemekhez, hiszen azon létesítményekben alkalmazzák a leginkább ezeket. A szakirodalmi szintetizálás alapján megállapítható, hogy a SCADA az ICS rendszerek egyik ága, valamint további komponenseseket tartalmaz: TRU, MTU, HMI, Historian, illetve egy kommunikációs hálózat. Emellett a rendszereknek számos előnye van, mint például a hatékonyság, a megbízhatóság és az online konfiguráció. A SCADA megfelelő kialakítása és működése, működtetése előírásokhoz

[29] Feldman 2019.
[30] Szádeczky 2021: 111–117.

van kötve, ennek egyik formája a biztonsági keretrendszer, amelyben intézkedések megfogalmazásával segítik elő az említett folyamatot. A keretrendszer mellett különböző szabványok, útmutatások és jó gyakorlatok segítik a szervezeteket, ezek között találhatunk európai, amerikai területi hatályút, de nemzetközi és multilaterális egyezményen alapuló dokumentum is alkalmazható. Ezek az intézkedések 2006 és 2011 között keletkeztek, és bár van olyan részük, amely a mai napig alkalmazandó, bizonyos részük elavult. Ennek okán indult el az ISA112 szabványügyi bizottságának kezdeményezése egy új SCADA-rendszerspecifikus szabvány kialakítására, amely várhatóan 2023 őszén válik elérhetővé. Mindemellett megjelenik még a NIS-irányelv is, amely szintén szabályozza a SCADA-t használó üzemeket, vállalkozásokat. Ezek a szervezetek különböző szektorokba, ágazatokba sorolhatók be. A magyar, az EU-s, illetve az amerikai szabályozások részben átfedéseket tartalmazó ágazatokat nevesítenek. Kiberfenyegetések tekintetében elmondható, hogy kifejezetten a SCADA-rendszerek esetében már 1982-ben detektáltak egy támadást, amelyet trójai vírus telepítésével valósítottak meg. Emellett beszámoltak számos egyéb jellegű incidensről is, legyen szó akár elbocsátott alkalmazott általi vandalizmusról, jogosulatlan hozzáférésről, vagy 0. napi sérülékenység kihasználásáról – ahogy az a leginkább ismert Stuxnet esetében történt. Az utóbbi időben 2013-ban, 2014-ben és 2016-ban számoltak be a legtöbb eseményről, ezek leginkább malware-es támadások voltak, vagy a rendszer feltörését hajtották végre a támadók. A szektorok tekintetében – a magyar szabályozás kategóriáit alkalmazva – elmondható, hogy leginkább az energiaágazat volt a célpont, azonban a vízágazat, valamint az infokommunikációs technológiák ágazati szereplői is beszámoltak őket ért atrocitásról. A SCADA-rendszereket ért támadások formái között megkülönböztethetünk a szoftvereket, illetve a kommunikációt érintő típusokat. A korábban leírtakat figyelembe véve kijelenthető, hogy szükség van a SCADA-rendszerek kiberbiztonsági kockázatainak hatékony kezelésére.

Irodalomjegyzék

Bederna Zsolt – Rajnai Zoltán – Szádeczky Tamás (2021): Business Strategy Analysis of Cybersecurity Incidents. *Land Forces Academy Review,* 26(2), 139–148. Online: https://doi.org/10.2478/raft-2021-0020

Dunn, Thomas (2015): 10 – Basics of Control Systems. In *Flexible Packaging.* Oxford: William Andrew, 103–110. Online: https://doi.org/10.1016/B978-0-323-26436-5.00010-2

ENISA (2011): *Annex III. ICS Security Related Standards, Guidelines and Policy Documents*. Online: www.enisa.europa.eu/publications/annex-iii

Feldman, Sarah (2019): Infographic: IT Says SCADA Will Continue to Be a Frequent Threat. *Statista Infographics,* 2019. március 6. Online: www.statista.com/chart/17267/cyber-security-threats/

G. L., Francis (2016): *SCADA: Beginner's Guide.* [H. n.]: [k. n.].

Kovacs, Eduard (2022): Ransomware Group Claims Access to SCADA in Confusing UK Water Company Hack. *Security Week,* 2022. augusztus 16. Online: www.securityweek.com/ransomware-group-claims-access-scada-confusing-uk-water-company-hack

Krasznay Csaba (2019): Kiberbiztonság a negyedik ipari forradalom korában. *Hiradástechnika: Hírközlés-Informatika,* 74, 25–29.
Megyeri Lajos – Farkas Tibor (2017): Kockázatkezelés, tudomány vagy kuruzslás? *Hadmérnök,* 12(3), 198–209.
Miller, Bill – Rowe, Dale Rowe (2012): A Survey SCADA of and Critical Infrastructure Incidents. *Proceedings of the 1st Annual Conference on Research in Information Technology*, RIIT '12, 51–56. Online: https://doi.org/10.1145/2380790.2380805
National Institute of Standards and Technology (2020): *NIST Special Publication 800-53 Revision 5*. Online: https://doi.org/10.6028/NIST.SP.800-53r5
Paráda István – Farkas Tibor (2020): Felderítés és Analízis a Penetrációs Tesztben – 1. Információgyűjtési Technikák. *Hadmérnök,* 15(1), 159–182. Online: https://doi.org/10.32567/hm.2020.1.11 ; DOI: https://doi.org/10.32567/hm.2020.1.11
Pathak, Neel H. – Patel, Hashmukh (2014): A Review on Modern SCADA Systems and Security Consideration of Individual SCADA System's Components. *International Journal of Engineering Development and Research,* 2(2), 1639–1699.
Petrosyan, Ani (2023): Frequency of Cyber Threats Worldwide by Type 2017 l Statistic. *Statista,* 2023. augusztus 25. Online: www.statista.com/statistics/883591/frequency-cyber-threats-expected-by-senior-it-practitioners-threat-type/
Stouffer, Keith et al. (2020): *NISTIR 8183 Revision 1.* National Institute of Standards and Technology. Online: https://doi.org/10.6028/NIST.IR.8183r1
Szádeczky Tamás (2021): Víz 4.0? A digitális víziközmű-infrastruktúra kiberbiztonsági kitettsége. *Hadtudomány,* 31(4), 111–117. Online: https://doi.org/10.17047/HADTUD.2021.31.4.111
DPS Telecom (2021): *14 Major SCADA Hacks*. 2021. december 23. Online: www.dpstele.com/blog/major-scada-hacks.php
Tóth András (2022): Information Security Challenges and Solutions in Smart Nations. In Kovács, Anna et al. (szerk.): *Security-Related Advanced Technologies in Critical Infrastructure Protection: Theoretical and Practical Approach.* Heidelberg: Springer Netherlands, 123–132. Online: https://doi.org/10.1007/978-94-024-2174-3_10
Yadav, Geeta – Paul, Kolin (2021): Architecture and Security of SCADA Systems: A Review. *International Journal of Critical Infrastructure Protection,* 34, 100433. Online: https://doi.org/10.1016/j.ijcip.2021.100433

Jogi források

2012. évi CLXVI. törvény a létfontosságú rendszerek és létesítmények azonosításáról, kijelöléséről és védelméről. Online: https://net.jogtar.hu/jogszabaly?docid=a1200166.tv
Az Európai Parlament és a Tanács (EU) 2016/1148 Irányelve (2016. július 6.) a hálózati és információs rendszerek biztonságának az egész Unióban egységesen magas szintjét biztosító intézkedésekről. Online: https://eur-lex.europa.eu/legal-content/HU/TXT/PDF/?uri=CELEX:32016L1148