Vass Attila
Maros Dóra
Berek Lajos

Az interdependencia kérdése az energetikai rendszer és a híradástechnika esetén a kritikus infrastruktúrák biztonsága védelmében

Napjainkra a biztonság mint fogalom új értelmet nyert, már korántsem azt jelenti, mint ötven éve. A mai rendszerek jóval összetettebbek, mint bármikor eddig a történelem során. Az országoknak immáron nem elsősorban az időjárás viszontagságaival vagy a látható ellenségekkel kell szembenézniük. Megjelent egy újfajta veszélyforrás: a terrorizmus. A rendszerek összetettségéből, valamint az ebből adódó, az országok közötti kölcsönös együttműködésből kialakult kritikus infrastruktúrák veszélyeztetettsége az elmúlt időszakban megnövekedett. Ezért a kormányok eltérő stratégia mentén, de azonos céllal biztonsági intézkedéseket hoztak a további merényletek megakadályozására.
Kulcsszavak: CIP, CIWIN, Zöld könyv, SCADA, energetika, híradástechnika, interdependencia, EPCIP

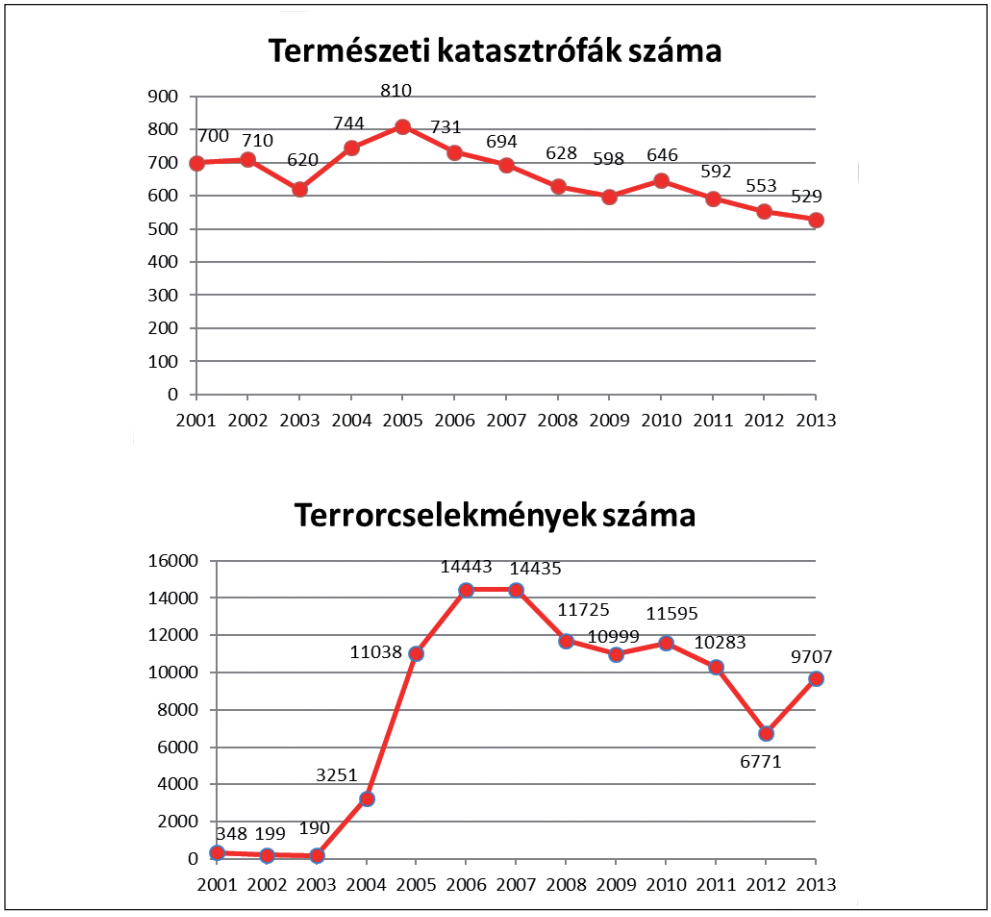
Kritikus infrastruktúra

A kritikus infrastruktúra mint fogalom az 1990-es évektől vált ismertté. Kidolgozását az Egyesült Államok szorgalmazta, bár első körben csak mint új tématerület vetődött fel. Azonban a történelem során olyan események következtek be, melyek azt mutatták, hogy igenis szükség van alkalmazására. Ezen objektumok felderítését az egyes országok saját magukra nézve állapították meg, ebből kifolyólag eltérő jellegű objektumokat neveztek meg. Ezért a legfontosabb besorolások a következők lettek:

– energetikai ágazat,
– információs, illetve távközlési ágazat,
– közlekedési és szállítmányozási ágazat,
– banki és gazdasági ágazat,
– egészségügyi ágazat.

Ezen ágazatok teljes vagy részleges megsemmisülése fennakadást okozhat egy állam működésében. Napjainkra a technológiai szektor jelentős mértékű fejlődést mutat, illetve hozott magával. Életünket is egyszerűbbé teszik, és kölcsönös függést eredményeznek a felhasználó és az adott terület között. Így ezek hiánya a morál jelentős csökkenését okozza a társadalomban. Ezt az alapvető megállapítást a különböző radikális csoportok, illet-

ve terrorszervezetek is felismerték, ezért támadásaik elsősorban olyan objektumok ellen irányulnak, amelyek potenciálisan több állampolgárt érintenek, ezzel is demoralizálva a nemzeteket. Míg ezeknek korábban csak a természeti csapások ellen kellett védekeziük, és azokra kidolgozni akcióterveket, a XXI. század leginkább a terrorcselekményektől és a kiberbűnözéstől visszhangzik. A WITS (Worldwide Incident Tracking System) szerint a terrorcselekmények száma az elmúlt években a következőképpen alakult.



1. ábra: Események gyakorisága a természeti és terrorcselekmények arányában (forrás: www.ifrc.org/en/publications-and-reports/world-disasters-report/world-disasters-report-2014/data/)

A két diagram jól szemlélteti az elmúlt évek eseményeit, azonban a két csoportosítás esetében meg kell jegyezni, hogy az infrastruktúrákra ható események ennél jóval összetettebbek. Ezért egy újabb csoportosítás szükséges a megértéshez.

1. Szándékos emberi beavatkozások:
   – terrorcselekmények,

– zavargások,
– háborúk,
– puccs.

2. Természeti eredetű katasztrófák:
   – árvíz, belvíz,
   – földrengés, vulkánkitörés,
   – szélsőséges időjárás,
   – tüzek,
   – szökőár, cunami.
3. Ipari katasztrófák:
   – nukleáris eredetű,
   – vegyi eredetű,
   – közlekedéssel kapcsolatos.
4. Technológiai és civilizációs függőségből adódó katasztrófák:
   – éhínség,
   – járványok,
   – kibertámadások,
   – növekvő populáció.

A kritikus infrastruktúra értelmezése

Az eltérő csoportosítások eltérő akciótervek kidolgozását jelenti, azonban ezt még nehezíti az országok gazdasági és ideológiai különbözősége is. Viszont némi könnyebbséget jelent, hogy a nemzetek szervezetekbe tömörülve, azonos állásponthoz tartozva kívánják a kritikus infrastruktúra definícióját meghatározni. [1], [2] Ebből az együttműködésből szintén különböző vélemények alakultak ki, de nem olyan szerteágazóak, mintha minden ország külön-külön értelmezné. Az USA szorgalmazta ennek bevezetését az ún. patrióta törvényen keresztül, melyet George W. Bush fogadott el a 2001. szeptember 11-i merénylet után. A dokumentum elsősorban a rendfenntartó, hírszerző, valamint az állami szervezetek munkáját könnyíti meg oly módon, hogy az eddig engedélyhez kötött hírszerző, illetve ellenőrző tevékenységeket végzésmentessé tette. Röviden ugyan, de a kritikus infrastruktúrák leírásával és védelmével is foglalkozik a törvény. Ennek értelmében a kritikus infrastruktúrák „olyan rendszerek és eszközök, amik fizikálisan vagy virtuálisan fontosak az Egyesült Államok számára, és azok megsemmisülése vagy működésképtelenné válása gyengítő hatással van a biztonságra, a nemzetgazdaság biztonságára, a nemzeti közegészségügyre, valamint a nemzeti közbiztonságra vagy ezek bármely kombinációjára”.[1]

[1] USA Patriot Act of 2001, SEC. 1016. Critical Infrastructures Protection.

A kritikus infrastruktúra szektorai
Mezőgazdaság és élelmezés
Védelmi ipar
Energetika
Közegészségügy és egészségügy
Műemlékek és jelképek
Bankok, pénzügyi szervezetek
Ivóvíz-ellátás és közművek
Vegyészet
Kereskedelmi szervezetek
Gátak
Sürgősségi szolgáltatások
Hasadóanyag-kereskedelem, energiatermelés és -kezelés
Informatika és hírközlés
Posta és szállítmányozás
Közlekedési rendszerek
Kormányzati szervezetek

1. táblázat: Az USA által meghatározott kritikus infrastruktúrák

A NATO álláspontja szintén megváltozott 9/11 után, ezért részben átvették az amerikai példát, de attól kismértékben eltér. A kidolgozásra két évet kellett várni, ezért 2003-ban a Polgári Védelmi Bizottság (CPC) javaslatára a Felső Szintű Polgári Veszélyhelyzeti Tervezési Bizottság (SCEPC) elfogadta a tervezetet. Itt a kritikus infrastruktúrák „olyan berendezések, szolgáltatások és információs rendszerek, amelyek létfontosságúak a nemzet számára, és azok megsemmisülése vagy működésképtelenné válása veszélyeztetné a nemzetbiztonságot, a nemzetgazdaságot, a közegészségügyet és a kormány hatékony és biztonságos működését”.[2]

Az Európai Unió 2005-ben kérte fel a NATO-t, hogy dolgozzon ki számára egy többoldalú megközelítést. Az első ilyen dokumentum *A kritikus infrastruktúrák védelme a terrorizmus elleni védelemben,* aminek értelmében a definíción a következőket értik: „Azok a fizikai és információtechnológiai berendezések, hálózatok, szolgáltatások és eszközök,

[2] EAPC 2003, Annex 1, p. 2.

melyek megsemmisülése vagy működésképtelenné válása súlyos hatással lenne a polgárok egészségére, biztonságára és gazdasági jólétére, valamint a tagállamok hatékony működésére. A kritikus infrastruktúra kiterjeszthető a következő ágazatokra: gazdasági ágazat, beleértve a banki és pénzügyi szektort, a szállítási és elosztási ágazat, energetika, közművek, egészségügy, élelmiszer-ellátás, kommunikációs szektor, valamint a kulcsfontosságú állami szolgáltatások. Az ágazatok némely létfontosságú eleme nem tekinthető »infrastruktúrának«, viszont olyan hálózatok, melyek hatással vannak egy-egy létfontosságú szolgáltatásra."[3]

2006-ban az EU saját maga kezdte meg az EPCIP jóval személyre szabottabb változatának megfogalmazását. „A kritikus infrastruktúrák olyan eszközök vagy azok részei, melyek elengedhetetlenek a létfontosságú társadalmi feladatok ellátásának fenntartásához, ideértve az ellátást, az egészségügyet, a biztonságot, az emberek gazdasági és társadalmi jólétét."[4] Ezen meghatározás jóval szélesebb körben alkalmazható, viszont jóval összetettebb, mint az eddigi megfogalmazások. Azonban az EPCIP nem nevezhető univerzális CIP-nek, mivel az európaiságot kell támogatnia, illetve figyelembe vennie. Ezért ezt a következőképpen hangsúlyozták: „Az európai kritikus infrastruktúra (ECI) olyan kritikus infrastruktúra, amelynek megsemmisülése vagy működésképtelenné válása jelentős hatással van két vagy több tagállamra, vagy egyetlen tagállamra, ha annak kritikus infrastruktúrája egy másik tagállamban található. Ez magában foglalja a különböző ágazatok kölcsönös függését."[5]

Az EU, a NATO és az Egyesült Államok által használt terminológiát egyes országok nem követték, mert a hidegháború alatt kidolgozott stratégiát kívánták megtartani. Ide sorolhatók a Balti-tenger országai, amelyek jóval egyszerűbben képzelik el ezt a rendszert. Számukra a megfogalmazás kibővül egyfajta nemzeti segélyhívó, valamint válságkezelő rendszerekkel. Az ECI-hez legközelebb álló BSR-ország Németország, már számos megfogalmazást napvilágra hozott, ezek közül az egyik nagy hasonlóságot mutat az európai variánssal: „A kritikus infrastruktúrák olyan szervezetek és intézmények, amelyek fontosak a közjólét számára, olyan módon, hogy megsemmisülésük vagy működésképtelenné válásuk tartós ellátási hiányt eredményez, valamint jelentős károkat okoz a közbiztonságban vagy egyéb drámai következménnyel jár. Az állami és a magánszektor csak abban az esetben képes a zavartalan működésre, ha a kritikus infrastruktúrák működésében nem lép fel zavar, és ezáltal képesek ellátni feladataikat."

[3] Commission 2004, pp. 3–4.
[4] Commission 2006a, p. 15.
[5] Uo.

A kritikus infrastruktúra szektorai	Alszektorok
Energetika	Olaj- és gázkitermelés, -feldolgozás, -tárolás és -szállítás Villamos energia termelése és elosztása
Nukleáris ipar	Kitermelés, szállítás, tárolás és kezelés
Információs és kommunikációs technológia	Információs rendszerek és hálózatok védelme Ipari felügyeleti és automatizálási rendszerek Internet Vezetékes távközlési hálózat Mobil távközlési hálózat Rádiós és navigációs rendszerek Műholdas rendszerek Műsorszóró rendszerek
Víz	Ivóvíz-ellátás Vízminőség ellenőrzése Környezettudatos ivóvíz-felhasználás
Élelmiszeripar	Élelmiszer-védelem és -biztonság
Egészségügy	Orvosi és kórházi ellátás Gyógyszerek, vakcinák és oltóanyagok Biológiai laboratóriumok és kutatóközpontok
Pénzügy	Fizetési, értékpapír-elszámolási és -kiegyenlítési infrastruktúrák és rendszerek Szabályozott piacok
Közlekedés	Közúti közlekedés Vasúti közlekedés Légi közlekedés Belvízi hajózás Óceáni és tengeri szállítás
Vegyipar	Előállítás, tárolás és feldolgozás Veszélyes vegyi anyagok szállítására használt csővezetékek
Űrkutatás	Űrkutatás
Kutatás	Kutatólaboratóriumok

2. táblázat: Az EU által meghatározott kritikus infrastruktúrák

A kritikus infrastruktúra szektorai	Alszektorok
Szállítás és közlekedés	Légi, tengeri, vasúti, helyi, belvízi szállítás
Energetika	Villamos energia, nukleáris erőművek, fosszilis üzemanyagok
Veszélyes anyagok	Vegyi és biológiai veszélyes anyagok
Távközlés és informatika	Távközlés és információs technológia
Pénzügyek és biztosítások	Biztosítások, pénzügyi szolgáltatások
Szolgáltatások	Polgári védelem, sürgősségi betegellátás, élelmiszer- és vízellátás, hulladékkezelés
Közigazgatás és igazságszolgáltatás	Rendőrség, vám- és szövetségi fegyveres erők
Egyéb	Média, kulturális tárgyak, kutatási létesítmények, nemzeti műemlékek és jelképek

3. táblázat: A Németország által meghatározott kritikus infrastruktúrák

Magyarország a kritikus infrastruktúra terén egy az Európai Bizottság által 2005-ben kiadott dokumentumot, a Zöld könyvet alkalmazza. A dokumentum lényegében egy útmutatás, mely a szektorban szereplő kulcsfontosságú kritikus infrastruktúrákra világít rá. Teszi ezt olyan módon, hogy a tagállamokra lebontva is tartalmaz részfeladatokat. Az alapkoncepció azonban azt sugallja, hogy egy tagállam a teljes unió része, ezért kötelezettséggel tartozik a csoport felé, a másik megállapítás szerint egy gyenge ország könnyű támadási felületet jelent, ezért törekedni kell az átlaghoz közeli biztonsági rendszer eléréséhez. Ebből kifolyólag a különböző országok csak hasonló megoldásokat fognak követni, mivel ideológiájuk és gazdasági helyzetük eltérő. Az egyes infrastruktúrák biztonsági meghatározásai, illetve szintjei eltérőek lehetnek, ami elvben nem probléma, de rendszeres koordinációt jelent, ami pedig rendszeres auditok meglétét teszi szükségessé. Ezek értelmében a Zöld könyv a következők szerint fogalmazza meg a kritikus infrastruktúrát: „A létfontosságú EU-infrastruktúra fogalmát a határon átnyúló hatás határozná meg, vagyis az, hogy egy baleset súlyos hatással járhat-e azon tagállam területén kívül is, melyben a létesítmény található. Továbbá figyelembe kell venni azt a tényt is, hogy a tagállamok közötti, a CIP-pel kapcsolatos kétoldalú együttműködési megállapodások jól bevált és hatékony eszközt jelentenek valamely két tagállam határán lévő létfontosságú infrastruktúrák védelmében. Az ilyen együttműködések kiegészítenék az EPCIP-et.

Az ECI-k magukban foglalhatnák azon fizikai forrásokat, szolgáltatásokat, információtechnológiai berendezéseket, hálózatokat és infrastrukturális eszközöket, melyek működésének megzavarása vagy megsemmisítése súlyos hatással járna a következők egészségére, biztonságára, illetve gazdasági vagy szociális jólétére:

a) két vagy több tagállam – ide tartoznának (adott esetben) bizonyos kétoldalú létfontosságú infrastruktúrák;
b) három vagy több tagállam – nem tartoznának ide a kétoldalú létfontosságú infrastruktúrák.

E választási lehetőségek előnyeinek mérlegelésekor figyelemmel kell lenni a következőkre:

– Az a tény, hogy valamely infrastruktúrát ECI-nek nyilvánítottak, nem jelenti azt, hogy emiatt szükségszerűen kiegészítő védekezési intézkedésekre lenne szükség. A fennálló védekezési intézkedések, mint például a tagállamok közötti kétoldalú megállapodások, teljesen megfelelőek lehetnek; ez esetben nem érinti őket az adott infrastruktúra ECI-vé nyilvánítása.
– Az a) lehetőség választása több infrastruktúra ECI-vé nyilvánítását eredményezné.
– A b) választási lehetőség azt jelenti, hogy csak két tagállamot érintő infrastruktúra esetén a közösség nem lépne fel még akkor sem, ha e két tagállam közül valamelyik nem tartja megfelelőnek a védelmi szintet, és a másik tagállam elutasítja a szükséges lépések megtételét. A b) lehetőség választása továbbá a tagállamok közötti nagyszámú kétoldalú megállapodáshoz vagy véleménykülönbségekhez vezethetne. Így előfordulhat, hogy a gyakran páneurópai szinten működő ágazatoknak különböző megállapodások eltérő hálózatával kell szembenéznie, ami járulékos költségeket okozhat.

Továbbá elfogadott, hogy figyelembe kell venni az EU-n kívüli vagy kívülről eredő olyan létfontosságú infrastruktúrákat is, melyek kapcsolatban vannak az EU tagállamaival vagy azokra adott esetben közvetlenül kihatnak."[6]

A szabályozási rendszer

Ahhoz, hogy a kritikus infrastruktúra védelmi rendszere megfelelően működjön, folyamatokat, illetve egy szabályzási rendszert kellett létrehozni. Ennek a rendszernek részét képezik az auditok, valamint az egyes tagállamokra vonatkozó betartandó utasítások. A rendeletek elfogadására rányomta bélyegét a vonat elleni 2004-es madridi és a 2005-ös londoni bombatámadás. A merényletek után világossá vált, hogy a kritikus infrastruktúrákat már nem csak a természet erőitől kell megvédeni: sokkalta nagyobb problémát okoznak a terroristaszervezetek, valamint az információs technológiai hálózatok ellen irányuló hackertámadások. Ennek megfelelően az Európai Bizottság 2004-ben létrehozta *A létfontosságú infrastruktúrák védelme a terrorizmus elleni küzdelemben* dokumentumot, ami javaslatot tett a hatékonyabb védelem kialakítására. Ebből kifolyólag létrehozták a már

[6] Commission (2005) 576.

említett EPCIP-et, a „Kritikus Infrastruktúrák Európai Programját", valamint a CIWIN-t, a „Kritikus Infrastruktúrák Figyelmeztető Információs Hálózatát".

EPCIP

Az EPCIP [3], [4] legfőbb célkitűzése, hogy javítsa a kritikus infrastruktúrák védelmét az Európai Unión belül. Ezen célok elérése érdekében az alábbi elveket fogalmazzák meg:

– Szubszidiaritás: értelmezése szerint olyan döntések, melyeket a legalacsonyabb szinten kell meghozni a legmagasabb szakértelem mellett. A dokumentum szerint azonban olyan azonosított kritikus infrastruktúrát jelent, mely egy adott tagállamban található, de az egész uniónak érdeke fűződik megóvásához. Ehhez olyan módon járul hozzá, hogy a létrehozott pénzügyi alapból jelentős forrást biztosít.
– Kiegészítés: az unió és a tagállamok együttes védelmét élvező infrastruktúra védelem szempontjából redundanciába ütközhet, ami jelentős összegbe kerül. Ezért ennek elkerüléséhez – a tagállam által biztosított intézkedéseken felül – az EU kiegészítésként egyéb biztonsági intézkedéseket hozhat.
– Titkosság: az egész kritikus infrastruktúra rendszer a biztonságra és a tagállamok közötti kölcsönös bizalomra épül. Tehát az ebből az okból készített dokumentumokat (CIPI), terveket a megfelelő prioritás meghatározása után titkosítani kell, és csak az előírt események bekövetkezése során szükséges elővenni.
– A szereplők együttműködése: ahhoz, hogy az unió teljes területén biztosítottak legyenek a létfontosságú infrastruktúrák, az EPCIP kidolgozásához a lehető legtöbb szereplőt be kell vonni a tervezésbe: a 27 tagállam képviselőit, szervezeteit, szerveit, valamint az infrastruktúrák közvetlen vezetőit és üzemeltetőit.
– Arányosság: az EPCIP eredményes kidolgozására abban az esetben van lehetőség, ha – a biztonsági kockázatnak megfelelően – a megállapított biztonsági résekkel, illetve hiányosságokkal szemben az ellenlépések arányosak lesznek.
– Ágazatonkénti megközelítés: az EPCIP nem alkalmazható egyetlen ágazatra; hatékony működéséhez azonosítani kell a szükséges ágazatokat, és azokra egyenként megállapítani a megfelelő intézkedéseket. (Az ágazatokat a korábbiakban már felsoroltuk.)

Ahhoz, hogy a tagállamok képesek legyenek azonosulni a védelem fontosságával, ki kell jelölniük, hogy milyen hatásfokkal kívánnak fellépni a behatások ellen. Ezért a Zöld könyv három eltérő védelemi stratégiát jelöl meg. Ezek közül kell az országoknak megjelölni, illetve kidolgozni azt, ami a saját ideológiájukhoz a legközelebb áll. A három lehetőség a következő:

– Mindenfajta veszéllyel szembeni védelem: ezen lehetőség során az adott állam figyelembe veszi a szándékos károkozás, valamint a természeti katasztrófák lehetőségét. Kiemelt figyelmet azonban csak a természeti katasztrófák kapnak.

– Mindenfajta veszéllyel szembeni védelem, különös tekintettel a terrorizmusra: a második megközelítés számításba veszi a természet viszontagságaiból adódó káreseményeket, viszont a terrorcselekményeket helyezi a középpontba.
– Terrorveszéllyel szembeni védelem: ez a lehetőség csak és kizárólag a terroristatámadásokra összpontosít.

EPCIP-keret

Az Európai Unió a felépítéséből adódóan több kisebb-nagyobb országot gyűjt egybe, amik ennek révén kölcsönösen függenek egymástól. Így gyakran megtörténhet, illetve meg is történt már, hogy egy állam területén található kulcsfontosságú objektum megsemmisülése vagy működésképtelenné válása során az EU egy jelentős része bizonyos létfontosságú szolgáltatás nélkül maradt. Vegyük például az igen összetett energetikai rendszert. A teljes unió területén lévő erőművek olyan szabályzási rendszerben vesznek részt, ahol a generátorok mintha egyetlen tengelyre lennének felhelyezve. Bármely nagyobb erőmű vagy kábelszakasz kiesése esetén jelentős területek maradhatnak villamos energia nélkül. Természetesen a rendszer tartalmaz tartalékokat , de bármely eshetőségre egy ilyen összetett rendszert nem lehet méretezni. Ezért egy ilyen rendszer biztonságát mindig a leggyengébb elem biztonsága határozza meg. Tehát létre kell hozni egy olyan közös védelmi rendszert, ahol a hálózat szereplői együttesen kommunikálnak, valamint együttműködnek egymással. Az ilyen egységes védelmi rendszerhez segítséget nyújt a Zöld könyv: kijelöli azt az egységes EPCIP-keretet, amit minden tagállamnak vagy résztvevőnek ismernie és betartania kell. Ez tartalmazhat közös célokat, illetve tagállamokra lebontott feltételeket is. Az interdependenciák figyelembevételével a következőket fogalmazták meg:

– A kritikus infrastruktúrák védelmének közös alapelvei.
– Közösen megállapított szabályzatok és szabványok.
– A kritikus infrastruktúra ágazatainak kidolgozása.
– Közös fogalom-meghatározások ágazatonként.
– A kritikus infrastruktúrák védelmének prioritásai.
– A bevont szereplők részletes feladatleírása.
– Közösen megállapított irányadó szintek.
– Az eltérő, de közösen megállapított ágazatok infrastruktúrájának összehasonlítása, a prioritások meghatározására vezető módszerek kidolgozása.

CIWIN

A CIWIN [5] egyike az EPCIP által tartalmazott biztonsági programoknak. Elfogadását 2006-ban kezdték meg. Ezen kezdeményezés figyelembe veszi, hogy az európai polgárok, valamint az uniós gazdaság jóléte bizonyos szolgáltatásoktól is függ. Ilyenek a telekommunikáció mint az egyes tagállamok közötti elsődleges információs csatorna, az energetikai hálózat mint közös kapcsolódási felület, melytől az államok kölcsönösen függenek, a pénzügy, a közlekedési rendszer, az egészségügy és az ivóvíz- és élelmiszer-ellátási rendszer. A CIWIN-nek nem más a célja, mint a tagállamok közötti biztonságos és strukturált információcsere fenntartása. Ennek hatására a tagállamok megismerhetik egymás gyakorlati rendszerét, illetve használhatják a sürgősségi riasztórendszereket. Azonban jelenleg az EU-ban nem léteznek a CIP-el kapcsolatos információcserét, illetve riasztásokat szabályozó rendelkezések. A tagállamok területén számos sürgősségi rendszer működik. Ezek a rendszerek azonban csak egy-egy ágazatot fognak át, ezzel ellentétben a CIWIN az összes ilyen jellegű rendszert fogná át, területtől függetlenül. Sajnos a CIP-feleknek, illetve az ezzel kapcsolatos szervezeteknek ezekre a rendszerekre nincs rálátásuk. Így tehát az érintett felek számára csak és kizárólag a segélyhívó rendszerek hozzáférhetőek.

Az ágazati határozatok a következők:

– közösségi Polgári Védelmi Mechanizmusról szóló határozat (2007/779/EK),
– radiológiai veszélyhelyzet esetén bekövetkező információcserén alapuló szabályozás (87/600/Euratom),
– az állatbetegségek közösségen belüli bejelentésekről szóló irányelv (82/894/EGK),
– a növények vagy növényi területeket károsító szervezeteknek a közösségbe történő behozatal, illetve a terjesztés elleni védekezésekről szóló irányelv (2000/29/EK),
– a közösségben kialakuló fertőző betegségek, járványok felügyeleti és ellenőrzési hálózatának létrehozásához szükséges határozat (2119/98/EK),
– a termékbiztonságról szóló irányelv (2001/95/EK),
– az élelmiszer-biztonságra vonatkozó, illetve az Európai Élelmiszer-biztonsági Hatóság létrehozásáról szóló rendelet (178/2002/EK),
– integrált számítógépes állategészségügyi rendszer kifejlesztéséről szóló határozat (2003/623/EK),
– belső eljárási szabályzat módosításáról szóló határozat (2006/25/EK).

A CIWIN bevezetése csak szoros együttműködés és szabályozás mellett lehetséges, ezért következő pontokat fogalmazták meg a felügyeletéhez, a hatékony alkalmazásához:

– a teljes rendszer működéséhez legalább 20 tagállam együttműködése szükséges,
– a publikussá tett információkat létrehozásuk előtt minősíteni kell, és csak a minősítés nélkülieket kell megosztani,
– a kritikus infrastruktúra szervezetei információcserére a CIWIN-t használják.

A CIWIN funkciói és területei

A tagállamok bármelyike részt vehet a létfontosságú infrastruktúrák figyelmeztető információs hálózatában, ennek feltétele a fent említett pontok betartása, valamint egy megállapodás aláírása, ami biztonsági technikákat, követelményeket tartalmaz. Az elfogadás után a partnerek a következő két funkciót kell megvalósítaniuk:

– a kritikusinfrastruktúra-védelemmel kapcsolatos információcsere megosztása elektronikus úton,
– veszélyhelyzeti jelzőrendszerek funkcióinak lehetővé tétele az Európai Bizottság és a részt vevő tagállamok részére.

Az elektronikus információcsere ellátáshoz különböző területeket rögzítettek, mivel a tagállamok területén fellelhető infrastruktúrák oly mértékben eltérőek lehetnek, hogy azok egyetlen téma alá sorolása nem lehetséges. Megkülönböztetünk fix és dinamikus területekből álló rendszereket. Fix vagy rögzített területnek nevezzük azt a rendszerelemet, mely tartalma szerint módosítható, de egyéb ágazat nem kapcsolható hozzá, illetve nem is nevezhető át. Ilyen területek a következők:

– „A tagállamok azon területei, amelyek minden egyes részt vevő ország számára megteremtik annak lehetőségét, hogy a CIWIN-portálon saját területet hozzanak létre. E terület felépítése, adminisztrációja és tartalma a tagállamok kizárólagos felelősségi körébe tartozik. A terület kizárólag az érintett tagállam felhasználói számára lesz majd hozzáférhető." [COM(2008) 676, I. melléklet]
– „Ágazati területek, 11 külön ágazattal: vegyipar; energia; pénzügy; élelmiszer; egészségügy; IKT; nukleárisfűtőanyag-ipar; kutatási létesítmények, űrkutatás, közlekedés és vízügy. Lesz egy ágazatokat átfogó alterület több ágazatot érintő általános témák és kérdésekhez." [COM(2008) 676, I. melléklet]
– „A CIWIN végrehajtó szerv területe, amely stratégiai koordinációs és együttműködési platformként szolgál, és amelynek célja a létfontosságú infrastruktúrák védelme tekintetében a tevékenységek és a kommunikáció előmozdítása és erősítése. Ez a terület kizárólag a CIWIN végrehajtó szervei számára lesz elérhető." [COM(2008) 676, I. melléklet]
– „EU külső együttműködési terület, amely a létfontosságú infrastruktúrák védelme terén a külső együttműködés és az Európai Unión kívül a létfontosságú infrastruktúrák védelmére vonatkozó előírások tekintetében az ismeretek bővítésére összpontosít." [COM(2008) 676, I. melléklet]
– „Kapcsolattartói címtár a CIWIN többi felhasználójára vagy a létfontosságú infrastruktúrák védelmének szakértőire vonatkozó elérhetőségi adatok keresésének megkönnyítésére." [COM(2008) 676, I. melléklet]

A dinamikus területek ezzel ellentétben szabadon módosíthatók, de ehhez engedély, illetve kérvény szükséges, és amint elérték létrehozásuk célját, a kezdeményezés automatikusan megszűnik. Ezek a következők:

– „szakértői munkacsoport számára fenntartott terület a CIP szakértői csoportok munkájának támogatására" [COM(2008) 676, II. melléklet],
– „projektterület, amely a Bizottság által finanszírozott projektekre vonatkozó információkat tartalmaz" [COM(2008) 676, II. melléklet],
– „riasztási területek, amelyek a sürgősségi riasztórendszerben indított riasztás esetén hozhatók létre, és amelyek a CIP-pel kapcsolatos tevékenységek során kommunikációs csatornaként szolgálnak majd" [COM(2008) 676, II. melléklet],
– „egyedi témák területe, amely konkrét témákra összpontosít" [COM(2008) 676, II. melléklet].

A híradástechnika és az energetika kapcsolata

Az eddigiekben láthatóvá vált, hogy a hírközlés és az energetika a kritikus infrastruktúra tárgykörébe esik. Megítélésük és fontosságuk vitathatatlan az Egyesült Államok, a NATO, az Európai Unió és a Balti-tengeri országok körében is. Adódik ez abból, hogy összetettségük messzemenőkig megelőzi a többi rendszert, és mivel kiterjedésük ekkora, az egyes országok kölcsönösen függenek egymástól. Az energetika területén több olyan rendszer működik, melyek működéséhez elengedhetetlen a megfelelő információcsere. Kiterjedése miatt csak ilyen módon felügyelhető. Mivel megannyi rendszer létezik, ezen írás keretein belül mindegyik tárgyalása nem lehetséges, ezért csak a SCADA rendszert kívánjuk elemezni a híradástechnika függvényében.

SCADA

A SCADA egy mozaikszó, mely a Supervisory Control and Data Acquisition-ből ered, ami felügyeleti ellenőrzőt és adatszolgáltatót jelent. Ezek a rendszerek magukban foglalják a központ és a távoli terminálok (RTU), valamint a központ és a programozható logikai vezérlők (PLC) közötti adatkapcsolatot. A rendszer folyamatosan adatokat küld a hálózat állapotáról a diszpécsereknek. Egy SCADA alkalmazhatósága széles keretek között mozog: lehet csak egy irodaházra kiterjedő, de lehet vele monitorozni egy egész ország villamosenergia-termelését és -szállítását. Alapvetően hagyományos PSN-hálózatnak fejlesztették, de mára helyi (LAN), illetve világméretű rendszerek (WAN) is létesíthetők vele, és egyre inkább elterjednek a vezeték nélküli technológiák is. Egy SCADA-rendszer a következő elemekből állhat:

– Egy adott terület adatait gyűjtő RTU-k vagy PLC-k, valamint a hozzájuk tartozó érzékelők, beavatkozók és kapcsolószekrények.
– Kommunikációs rendszer, ami az adatok cseréjét végzi az adatgyűjtőktől a SCADA-központig. Itt beszélhetünk rádiós, telefonos, kábeles, műholdas stb. rendszerekről, illetve ezek kombinációjáról.
– Központi SCADA-szerver vagy MTU.
– Egyedileg elkészített és integrált szoftverek, különböző interfészek, melyek az operátorok munkáját segítik.

Az évek és a fejlesztések során három generáció alakult ki:
– első generáció – monolitikus SCADA,
– második generáció – elosztott SCADA,
– harmadik generáció – hálózati SCADA.

Az első generáció kifejlesztése során elsősorban nagygépes rendszerek álltak rendelkezésre. Ez annyit jelent, hogy hálózati összeköttetés híján a rendszerelemek felügyeletét egyetlen nagyméretű számítógép látta el. Ennek megfelelően az ilyen jellegű megvalósítás különálló rendszerekt eredményez, melyek egymással nemcsak az RTU-okkal kommunikálnak WAN-on keresztül. A protokollok használatát az egyes fejlesztők eltérően oldották meg alacsony támogatás mellett, valamint a különböző gyártók elemei között nem volt átjárhatóság. Az összeköttetés terén a szervergép igen korlátozott tulajdonságokkal bírt. A mestergép egyetlen buszra felfűzött kapcsolaton valósította meg a feldolgozást, ehhez egy CPU volt rendelve. Mivel a rendszer működése akadálytalan kellett legyen, biztonsági szempontból redundanciát kellett alkalmazni. Tették ezt olyan módon, hogy a szerverrel teljesen megegyező számítógépet kapcsoltak a buszrendszerre. Vészhelyzet esetén pedig egyszerűen csak beiktatták a tartalékgépet. Párhuzamos feldolgozásra ezen megoldás nem volt alkalmazható, egyszerre csak egyetlen számítógép végezte az adatok elemzését.

A második generáció már ennél jóval fejlettebb képet mutatott a nanotechnológia és a LAN-technológia elterjedésével. Így már elosztott rendszerről beszélhetünk, ahol az adatok feldolgozása több rendszerben generálódik egyszerre. Az állomások a helyi hálózat révén valós időben képesek az adatokat egymással megosztani. Az ilyen rendszerek a személyi számítógépeknek köszönhetően jóval olcsóbbak lettek, mint az előző generációból vett mainframe rendszerek. A feldolgozás szempontjából az adatok a terepi eszközök felől a kisebb számítógépek felé áramlanak. Az információáramlás során alkalmazott LAN-protokollok nem voltak elegendőek az adatok átvitelére, ezért a fejlesztők megannyi új ötlettel álltak elő. Ez a megoldás azonban ismételten visszahatott az eltérő rendszerek összekapcsolására a kompatibilitás hiányában. Az így megalkotott rendszerek, melyek azonos elemekből épültek fel, immáron nem szenvedtek az átviteli sebesség problémájától. Az elosztott rendszer funkcióját tekintve nemcsak a feldolgozást segíti elő, hanem a redundanciából adódó felépítés javítja a rendszer teljes megbízhatóságát. Az ilyen jellegű rendszer létrehozása nem jelenti az első generációs felépítés teljes ki-

zárását: annak egy részét megtartották, azzal a különbséggel, hogy a tartalékrendszer folyamatosan online állapotban van. Így üzemzavar esetén az átállás igen rövid ideig tart. A sok pozitívum mellett ennek a rendszernek is vannak gyenge pontjai. A legnagyobb problémát a külső hírközlési elemek jelentették. Az RTU-ból beérkező információk áramlását nagy részben akadályozták az egyes gyártók által alkalmazott protokollok. Ennek azonban nemcsak az eltérő kommunikáció szabott határt, hanem a korlátozott hardver- és szoftverállomány is.

A jelenleg alkalmazott harmadik generáció felépítése hasonló a második generációhoz, attól abban tér el, hogy a gyártók a nyitott architektúrát ellenőrzött környezetbe helyezték át. Az elosztás funkciója szintén megmaradt: a hálózati rendszerelemek megosztják egymás között a feladatokat. Az előző generáció hiányosságait kihasználva és a nyílt rendszerekre támaszkodva az új SCADA már nemcsak helyi számítógépes hálózatokat képes kezelni, így lehetővé vált számára a WAN-protokollok használata is. A rendszer így képes hozzáférni harmadik fél által használt perifériákhoz is, pl. nyomtató, meghajtók, hálózati lemezek stb. Így következhetett be, hogy a fejlesztők fokozatosan kiszorították a nagy informatikai cégeket a piacról. A legnagyobb különbséget mégis az internetprotokoll bevezetése jelentette. Ezzel lehetővé vált a terepi szintű adatgyűjtők leválasztása a szerverekről, és az RTU-k ettől kezdve ethernet kapcsolaton érték el az állomásokat.

SCADA-protokollok

Egy SCADA-rendszerben fontos a terepi adatgyűjtők felől érkező információk folyamatos beszerzése. Tehát az RTU elfogadja az adott parancsot, amit a rendszer küld felé, majd beállítja az analóg kimenetet, és a kérésnek megfelelően megküldi az adatokat. Ilyen módon a szerver adatcsomagokat küld a hálózat állapotáról. Az adtok kezelésében nincsen semmilyen kivétel. A címzés összhangban áll a SCADA-számítógépek adatbázisával. Az RTU-k semmilyen más információt nem továbbítanak a környezetből, csak és kizárólag az ellenőrzésük alá tartozó csomópontok adatait. Egy alállomás összesen 27 RTU-modult képes kezelni. A protokoll kétfajta üzenetet vagy üzenetpárokat alkalmaz működéséhez. Az egyik a mesterállomás üzenete, a másik az RTU üzenete; a kezdeményezést mindkét esetben válaszadás követi. Jelenleg az iparban több különböző protokollt alkalmaznak, ezek közül az egyik az IEC 60870-5-101, elosztott hálózat esetén pedig a DNP3.

Az IEC 60870-5 számos keretformátumot, szolgáltatást, valamint több különböző réteget határoz meg. A rétegek meghatározzák, hogy az RTU-k mit hogyan mérjenek és kommunikáljanak további eszközökkel. Továbbá lehetőséget nyújt különbséget tenni az alkalmazási és a fizikai réteg között. Az OSI-modell ilyen fokú kezelése jelentős átjárhatóságot jelent az órajel-szinkronizáció és a fájlátvitel során. Maga a szabvány öt dokumentumot tartalmaz, melyeket az elmúlt évtizedekben alakítottak ki:

– Az IEC 60870-5-1 alapvető követelményeket, szolgáltatásokat tartalmaz az adatkapcsolati és a fizikai rétegek számára. Elsősorban azt határozza meg, hogyan nézzenek ki, illetve milyen formázást alkalmazzanak az adatkeretek, milyen legyen a szinkronizáció sebessége adatkapcsolat esetén.
– Az IEC 60870-5-2 több alternatívát tartalmaz az átviteli eljárásokra, meghatározza a pont–pont topológia használatát, kijelöli az ellenőrző kódok, illetve a szabad felhasználású mezők használatát.
– Az IEC 60870-5-3 szabályokat és specifikációkat tartalmaz alkalmazási szinten az átviteli keretekre. Ezen szabályok mutatnak utat a jövőbeni fejlesztési irányoknak, és alapját képezik az ötödik dokumentumban foglalt megoldásoknak.
– Az IEC 60870-5-4 olyan szabályokat tartalmaz, melyek egy analóg, illetve digitális távvezérlési feladatokat alkalmazó rendszer alapjai.
– Az IEC 60870-5-5 az első dokumentum, ahol megjelenik az OSI-modell alkalmazása. Leírja, miként lehet távvezérlést létrehozni ezen modellt alapul véve.

Az eddig tárgyalt profilok mind meghatároznak egy-egy adott feladatot. Néhány alkalmazási funkció nem található meg az alapvető szabályok között, azonban azt meg kell határozni, mivel ezek nélkül nem üzemképes a távvezérlés. Ilyen események egy állomás indítása, az adatátvitel ciklikus ismétlése, az adatgyűjtők lekérdezése vagy például egy állomás konfigurálása. A feladatok kiszolgálását a 101-es szabvány tartalmazza, mely kijelöli az RTU-k és az intelligens elektronikus eszközök közötti profilt. Vagyis segítséget nyújt a különböző gyártók termékeinek összekapcsolására egyetlen rendszeren belül. A megoldás lényege, hogy a 101-es profil deklarálja az ITU-T szerinti RS-232 és az RS-485 szabványokat, illetve megoldást nyújt az adatok optikai interfészen történő továbbítására is. Az IEC 60870-5-5 szerinti felhasználói rétegben a következő alapvető alkalmazási funkciók valósulnak meg:

– fájlátvitel,
– ciklikus adatátvitel,
– állomásindítás,
– adatgyűjtés,
– óra szinkronizációja,
– események naplózása,
– paraméterek betöltése,
– vizsgálati eljárások alkalmazása.

A DNP3-as protokoll olyan szabályokat határoz meg, melyek ahhoz szükségesek, hogy két eszköz soros kapcsolaton kommunikálni tudjon. A DNP3-t speciálisan a terepi eszközök számára fejlesztették SCADA-RTU, RTU-IED, valamint SCADA-szerver–RTU/IED között. A protokoll hasonló, mint az IEC 60870-5-ös szabvány, néhány kivételtől eltekintve, melyek bizonyos kiegészítéseket, leírásokat tartalmaznak az energetikai ipar számára. Létrejöttét a következő célok tartalmazzák.

– Magas fokú adatintegritás: a DNP3 adatkapcsolati rétege az IEC 60870-5-1 egy módosított változatát alkalmazza.
– Rugalmas szerkezet: az objektum alapú alkalmazási réteg számos átjárhatóságot biztosít a struktúra megtartása mellett
– Magasabb szintű alkalmazhatóság, valamint több üzemelési mód:
  • lekérés,
  • lekérés kivétel hatására,
  • kivétel hatására történő kéretlen jelentések,
  • az előzőek vegyes használata.

A DNP3 elsősorban kétvezetékes átviteli közegre lett kifejlesztve, ahol a sebesség 1200 bit/s. A protokoll a lehető legmagasabb rugalmasság megtartása mellett törekszik az alacsony átviteli sebességre. A DNP3 egy nyílt forráskódú szabvány, elsősorban a gyártók és a felhasználók fejlesztik, illetve tartják karban.

Működése: egy központi szerver figyeli az összes rendszerhez kapcsolódó eszközt. A szerver begyűjti és tárolja az adatokat, és megjeleníti azokat az operátorok számára. Az alállomások gondoskodnak a hozzájuk csatlakozó megszakítók, áram- és feszültségérzékelők, valamint az egyéb eszközök monitorozásáról. Mivel az adatgyűjtés során rengeteg adat keletkezik, ezért az információt lementik és továbbítják a szerver felé, amit az kiértékelve visszajelez az alállomás számítógépeinek, és így megtörténik a megfelelő interakció.

Az előzőekben áttekintettük a fontosabb SCADA-protokollokat. Ezekből kitűnt, hogy a hírközlés fontos eleme az energetikai felügyeleti rendszernek. Üzemképes működése nagyban függ a híradástechnikából átemelt megfelelő szabványok alkalmazásától, mint például az OSI-modell és az ITU-T. A következőkben vizsgáljuk meg az átviteli közegek alkalmazhatóságát!

Átviteli közegek

Az energetikai hálózat nagy kiterjedéssel bír. Az adatok gyűjtése és feldolgozása a terepről nehéz feladat, számításba véve a gazdasági és a technológiai megoldásokat. Számos lehetőség kínálkozik a kommunikációs csatornák kiépítésére, gyakran biztonsági okokból redundanciát alkalmazva.

Csavart érpár

Hagyományos, a híradástechnikából is ismert átviteli közeg. Az egyik leggyakrabban alkalmazott megoldás. Elosztása egyszerű, különösebb infrastruktúrát nem igényel.

Koaxiális kábel

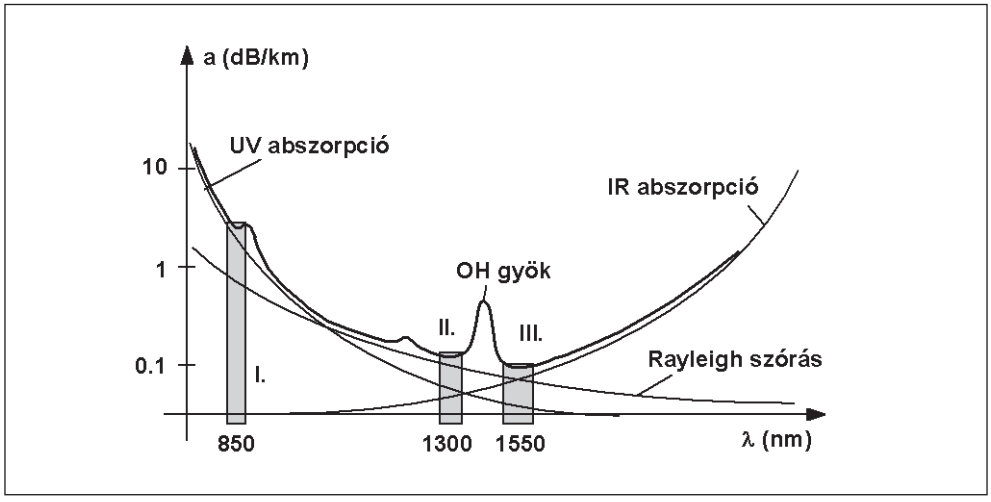
A koaxiális kábelt egy vagy több belső rézér, egy PVC-szigetelő, egy külső réz- vagy alumíniumszálakból szőtt háló, valamint egy külső szigetelés alkotja. A belső éren az átvinni kívánt információ halad, míg a külső háló földpotenciálra van kötve. Ezzel a megoldással több MHz-es jelek is átvihetők. Alacsony csillapítási tényezőjét a megfelelő sodrásirányból és a külső háló miatt éri el. Könnyedén átvihető vele hang-, adat- és képi információ is. Igen népszerű megoldás Európában és az Egyesült Államokban.

Optikai szálak

Az optikai szálas rendszerek elterjedése az 1970-es évektől jellemző. A kereskedelmi forgalomban lévő kábelek vesztesége kevesebb mint 0,3 dB/km. Az ilyen mértékű veszteség hatására akár 140 km-es távolság is áthidalható megfelelő jeladórendszerrel anélkül, hogy repeater beépítésére lenne szükség. Az optikai szálak egy belső magból, valamint egy külső, rugalmas műanyag burkolatból állnak.

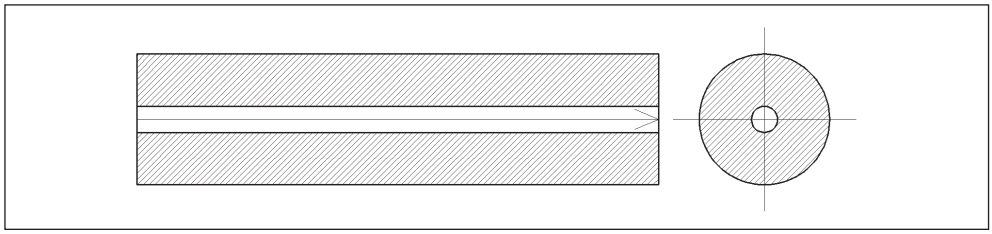
A rendszer a következő három részből tevődik össze:

– fényforrás (LED, laser),
– átviteli közeg (lehet műanyag vagy üveg),
– vevő vagy detektor (fotodióda, fototranzisztor).



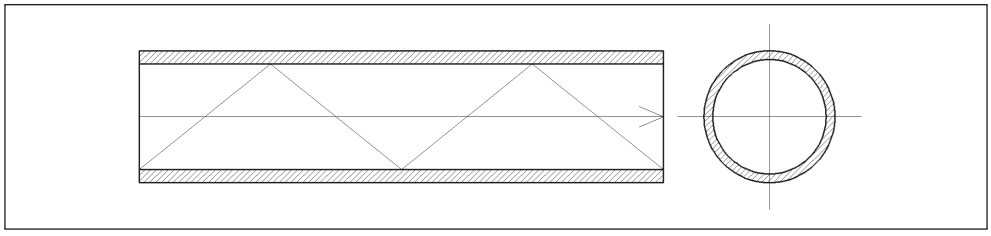
2. ábra: A csillapítás hullámhosszfüggése (forrás: Gyárfás András: Számelmélet dia)

Három fényvezetőszál-típust különböztetünk meg. Működésük alapja a fény terjedése optikailag homogén térben.



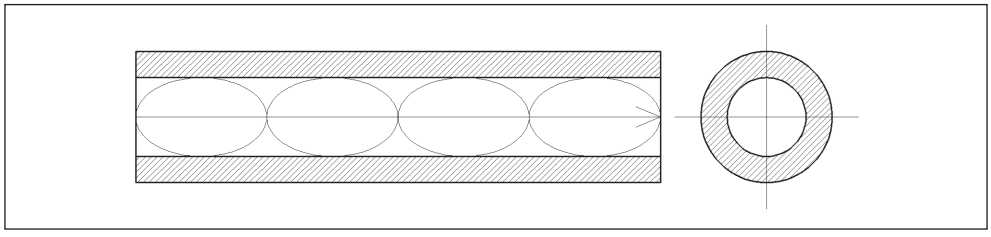
3. ábra: A fény terjedése egymódusú optikai kábelben

Az *egymódusú optikai kábel* jellemzője: a fény egyenes vonalban érkezik be, párhuzamosan az optikai szál magjával. Nincs visszaverődés a reflexiós rétegről. Működése gyors, nem igényel jelregenerációt.



4. ábra: A fény terjedése multimodusú lépcsős indexű optikai kábelben

A *multimódusú lépcsős indexű optikai kábel* jellemzője: a jel bizonyos szögben érkezik, visszaverődéssel továbbítja az adatokat. Visszaverő réteg alkalmazása szükséges.



5. ábra: A fény terjedése multimódusú gradiens indexű optikai kábelben

A *multimódusú gradiens indexű optikai kábel* jele torzult, fontos a jelregeneráló elektronika alkalmazása. Csillapítása erősen függ a közvetítő közeg anyagától, mely lehet kvarc, üveg vagy plexi. Utóbbi esetben törekedni kell az anyag minél tisztább formájú felhasználására.

A villamos ipar számára némileg eltérő technológiákat dolgoztak ki az OPGW-, az ADSS-, valamint a WOC-kábelek. Az OPGW-kábel, azaz a védővezetőbe integrált fényvezető kábel egy vagy több szálat tartalmaz, melyeket különböző fémötvözetekkel vesznek körbe. A csövek felépítése réteges, illetve szálas a nagyobb rugalmasság elérése érdekében.

Az ADSS-kábelek csak szigetelő anyagokból felépített kábelek. Alkalmazhatóak lengőkábelként a távvezetékek mellett vagy bizonyos kikötésekkel (WOC burkolt optikai kábelek) földkábelként is. Az optikai kábelek egy merevítőszálat vesznek körül, melyekre több csavart száltartót tekernek. A következő rétegekben vízzáró és mechanikai szilárdságot adó PVC- és aramidszigeteléseket visznek fel.

Power line kommunikáció

Kifejlesztését az energetikai ipar szorgalmazta, mivel maga a távvezetéki villamosenergia-elosztás is kábeleket használ az energiaellátásra. Így fölösleges egyéb kommunikációs kábelek kihúzása, ha a vezetékek már megvannak. Ezért születhetett meg a power line rendszer. A távvezetékre 30 kHz–500 kHz rádiófrekvenciás jelet ültetnek, ami így a hálózati frekvenciát nem zavarhatja. Elsősorban analóg és digitális PLC-k használják. Ez a típusú rendszer nem használható minden távvezetéktípuson; jellemzően a 220 és 110 kV-os hálózaton képes hatékony működésre. Ennél magasabb hálózati feszültségek esetén, mint pl. a 400 és a 750 kV-os hálózatoknál nehéz a jeleket regenerálni, mivel a kábeleket elsősorban nem kommunikációs célokkal telepítették. Igen magas csillapítással és zajszinttel rendelkeznek.

Műholdas kommunikáció

A műholdas kommunikáció néhány évvel ezelőtt terjedt el az energetikai ágazatban. A rendszert kiszolgáló műholdak geostacionárius pályán keringenek a Föld körül. Megfelelő lefedettséget nyújtanak még az erdős, hegyes területeken is. Egyszerre több szálon is képesek kapcsolódni a földi állomásokkal, mivel rajtuk több transzponder is található. Az állomások általában egy parabolikus tükörből, egy alacsony zajszintű rádió adóvevőből és egy alapsávi modulból állnak. Az adatok átvitelére a radarfrekvencia-sávokat a C 4–8 GHz-es és a Ku 12–18 GHz-es sávot használják. A Ku-sáv használata jelentős előnyökkel bír, a magasabb frekvenciasáv miatt kisebb méretű antennák alkalmazását teszi lehetővé, így a beruházási költségek is jóval kedvezőbbek.

Bérelt telefonvonalak

A bérelt telefonvonalak használata már az energetikai rendszerek hőskorában is fontos szerepet töltött be, napjainkra jelentősége csökkent, de nem tűnt el. Sok gyártó és szervezet támogatja a hagyományos készülékek által használt PSN-hálózatokat, elsősorban hang átvitelére. Így a SCADA-rendszer is nyújt egyfajta támogatást, elsősorban a telemetria részéről.

VHF-kommunikáció

Sávszélességét tekintve a hagyományosan használt 30–300 MHz-es tartományra korlátozódik. Ezt a sávot elsősorban mobil rádiók kommunikációjára használják. Mivel azonban több szervezet is használja ezt a sávot, az SCADA-rendszerek diszpécseri szolgálata csak

bizonyos frekvenciákon ad a torlódások elkerülésére. Némely gyártók csak a 136–155 MHz-es, illetve a 150–174 MHz-es sávra készítik fel eszközeiket. Ebből is látható, hogy az URH-sáv csak igen kis frekvenciasávját foglalják el a SCADA-eszközök.

UHF-kommunikáció

A VHF-sávval szomszédos 300 MHz – 3 GHz-es tartományt felölelő kommunikációs csatorna. Az SCADA-rendszerek a 928 MHz – 952 MHz-ig terjedő sávot használják, mely kifejezetten a közművek közötti információcserére lett kiadva. A rendszerek működhetnek pont–pont, pont–multipont, valamint szórt spektrumú kapcsolatban. A szórt spektrumú rendszer képezi alapját a 802.11 a/b/g vezeték nélküli hálózatoknak.

Mikrohullámú rendszerek

1 GHz felett üzemelő rádiófrekvenciás technológia. Nagy sávszélessége miatt magas csatornakapacitás jellemzi. Egy SCADA-rendszerben elsősorban hang, adat, tömörített video, telemetrikus információk küldésére és fogadására használják. Az előzőekhez hasonlóan alkalmas pont–pont, pont–multipont kapcsolatra. A többszörös kapcsolódásra FDMA, TDMA és CDMA módokat alkalmaz.

Az átviteli módszerek összehasonlítása

Az SCADA-rendszerek a híradástechnika szinte valamennyi területét igénybe veszik, rendkívül széles a felhasználási paletta. Emellett az eddig tárgyalt rendszerek biztonsági kockázattól függően bizonyos átfedéssel is működhetnek, tehát az adatok prioritásától függően az információ több útvonalon is eljuttatható a címzettnek. A lehető legjobb hatékonyság elérése érdekében kell a kommunikációs csatornákat megválasztani, ezért az eddig tárgyalt rendszerek előnyeit és hátrányait egy táblázatban hasonlítjuk össze.

Technológia	Előnyök	Hátrányok
Csavart érpár	Licenszmentes Rövid távolságokon gazdaságos Magas csatornakapacitás kis távolságokon	Sérülékeny Víz elleni védelem Kialakítása kevésbé rugalmas hálózatot eredményez Földkábelnek nem használható
Koaxiális kábel	Licenszmentes Rövid távolságokon gazdaságos Magas csatornakapacitás kis távolságokon Külső árnyékolás miatt zajvédett	Sérülékeny Víz elleni védelem Kialakítása kevésbé rugalmas hálózatot eredményez Földkábelnek nem használható
Optikai szálak	Elektromágneses sugárzásokkal szemben védett Földpotenciál-változással szemben védett Magas csatornakapacitás Alacsony beruházási költségek Licenszmentes	Drága eszközök szükségesek a telepítéshez Kialakítása kevésbé rugalmas hálózatot eredményez Sérülékeny Víz elleni védelem Új technológia lévén tanulást igényel
Power line kommunikáció	Az adatküldő és fogadó egység az adott helyen található A felhasználáshoz szükséges kábelek, illetve maga a rendszer ki van építve Digitális PLC esetén 3-4 csatorna használható egyszerre Analóg PLC esetén 2 csatorna használható egyszerre	Működése az elosztóhálózattól függ A vivőfrekvencia nem védett Jellegéből adódóan nem mindig áll rendelkezésre Magas csatornánkénti költségek Szakadt vezetéknél nem szolgáltat információt
Műholdas kommunikáció	Nehéz terepen is jó lefedettséget biztosít Könnyű hozzáférhetőség A költségek függetlenek a távolságtól Alacsony bit/hiba arány Könnyen alakítható hálózati rendszer	Magas az átviteli késleltetés Folyamatos bérleti költségek A Nap zavaró hatása befolyásolja működését Átvitel esetén nehézkes ellenőrzés
Bérelt telefonvonalak	Alacsony beruházási költségek Egyszerű karbantarthatóság Nem szükséges különösebb szakértelem a működtetéséhez	A javítást és a karbantartást a tulajdonos végzi Folyamatos bérleti költségek A rendszer nem minden esetben alkalmazható

Technológia	Előnyök	Hátrányok
VHF-kommunikáció	Nagyobb lefedettség, mint az UHF-sávban Független a távvezeték-hálózattól Gazdaságos üzemeltethetőség A jelterjedés során nem szükséges, hogy az adó és a vevő egymásra lásson Különböző frekvenciák is kijelölhetőek	Alacsony csatornakapacitás Alacsony digitális bit/rate Korlátozott átviteli technológia
UHF-kommunikáció	Alacsony beruházási költségek Független a távvezeték-hálózattól A jelterjedés során nem szükséges, hogy az adó és a vevő egymásra lásson Különböző frekvenciák is kijelölhetőek	Alacsony csatornakapacitás Alacsony digitális bit/rate Korlátozott átviteli technológia
Mikrohullámú rendszerek	Magas csatornakapacitás Magas átviteli sebesség Független a távvezeték-hálózattól Kevésbé érzékeny a fading jelenségekre Egyszerű telepíthetőség Jövőbeni fejlesztések	Adó és vevő között rálátás szükséges Üzemeltetéséhez drága eszközök szükségesek Frekvenciasávok kijelölése a városokban nehézkes Magas fejlesztési költségek

4. táblázat: Az átviteli technológiák összehasonlítása

Irodalomjegyzék

[1] *A kritikus infrastruktúra védelem fogalmi rendszere, hazai és nemzetközi szabályozása.* Katasztrófa Védelmi Tudományos Tanács Pályázata, Budapest, 2011.

[2] *Uniting and Strengthening America by Providing Appropriate Tools Required to Intercept and Obstruct Terrorism Act.* One Hundred Seventh Congress of the United States of America, Washintgton, 2001.

[3] *Zöld könyv.* Az Európai Közösségek Bizottsága, Brüsszel, 2005.

[4] *A létfontosságú infrastruktúrák védelmére vonatkozó európai programról.* Az Európai Közösségek Bizottsága, Brüsszel, 2006.

[5] *A létfontosságú infrastruktúrák figyelmeztető információs hálózatáról (CIWIN).* Az Európai Közösségek Bizottsága, Brüsszel, 2008.

The Issue of Interdependence in Energy Systems and Communications for Critical Infrastructure Protection

Vass Attila – Maros Dóra – Berek Lajos

Today security is defined differently than fifty years ago. The latest systems are more complex than ever before in history. The main threat that countries have to face is no longer posed by weather conditions or visible enemies but by terrorism. The vulnerability of critical infrastructures has increased due to the complex systems and cooperation between countries. Therefore different governments took different measures but with same objective: to prevent further attacks.

Keywords: CIP, CIWIN, Green Paper, SCADA, energy, communications, interdependence, EPCIP