

### A kiber-fizikai energia sebezhetősége és ellenálló képessége rendszerek: egy empirikus alapú tanulmány eredményei

Tapia, Mariela; Thier, Pablo; Gößling-Reisemann, Stefan

Publikációs verzió / Published Version Arbeitspapier /  
working paper

#### Empfohlene Zitierung / Javasolt idézet:

Tapia, M., Thier, P., & Gößling-Reisemann, S. (2020). *A kiber-fizikai energiarendszerek sebezhetősége és ellenálló képessége: egy empirikus alapú vizsgálat eredményei.* (artec-paper, 222). Bréma: Universität Bremen, Forschungszentrum Nachhaltigkeit (artec). <https://nbn-resolving.org/urn:nbn:de:0168-ssoar-73492-4>.

#### Nutzungsbedingungen:

*Dieser Text wird unter einer Deposit-Lizenz (Keine Weiterverbreitung - keine Bearbeitung) zur Verfügung gestellt. Gewährt wird ein nicht exklusives, nicht übertragbares, persönliches und beschränktes Recht auf Nutzung dieses Dokuments. Dieses Dokument ist ausschließlich für den persönlichen, nicht-kommerziellen Gebrauch bestimmt. Auf sämtlichen Kopien dieses Dokuments müssen alle Urheberrechtshinweise und sonstigen Hinweise auf gesetzlichen Schutz beibehalten werden. Sie dürfen dieses Dokument nicht in irgendeiner Weise abändern, noch dürfen Sie dieses Dokument für öffentliche oder kommerzielle Zwecke vervielfältigen, öffentlich ausstellen, aufführen, vertreiben oder anderweitig nutzen.*

*Mit der Verwendung dieses Dokuments erkennen Sie die Nutzungsbedingungen an.*

#### Használati feltételek:

*Ez a dokumentum letéti engedéllyel hozzáférhető (nincs újraelosztás - nincs módosítás). A dokumentum használatára nem kizárólagos, nem átruházható, egyedi és korlátozott jogot biztosítunk. Ez a dokumentum kizárólag az Ön személyes, nem kereskedelmi célú felhasználására szolgál. A dokumentum minden másolatának tartalmaznia kell a szerzői jogi és egyéb, a jogi védelemre vonatkozó információkat. Ön nem jogosult ezt a dokumentumot semmilyen módon megváltoztatni, nyilvános vagy kereskedelmi célokra másolni, a dokumentumot nyilvánosan kiállítani, előadni, terjeszteni vagy más módon nyilvánosan felhasználni.*

*A jelen dokumentum használatával Ön elfogadja a fenti felhasználási feltételeket.*

# A kiber- és számítógépes hálózatok sebezhetősége és ellenálló képessége. fizikai energiarendszerek

Egy empirikus alapú vizsgálat eredményei

Mariela Tapia, Pablo Thier, Stefan Gößling-Reisemann

artec-papír 222. sz.

április 2020

ISSN 1613-4907

Das artec Forschungszentrum Nachhaltigkeit ist ein interdisziplinäres Zentrum der Universität Bremen zur wissenschaftlichen Erforschung von Fragen der Nachhaltigkeit. Das Forschungszentrum Nachhaltigkeit gibt in seiner Schriftenreihe "artec-paper" in loser Folge Aufsätze und Vorträge von Mitarbeiter\*innen sowie ausgewählte Arbeitspapiere und Berichte von Forschungsprojekten heraus.

## Impresszum

### Herausadó: K:

Brémai Egyetem  
artec Forschungszentrum Nachhaltigkeit  
Postfach 33 04 40  
28334 Bréma  
Tel.: 0421 218 61801  
Fax: 0421 218 98 61801  
URL: [www.uni-bremen.de/artec](http://www.uni-bremen.de/artec)

### Kontakt:

Katja Hessenkämper  
E-mail: [hessenkaemper@uni-bremen.de](mailto:hessenkaemper@uni-bremen.de)

# A kiber-fizikai energiarendszerek sebezhetősége és ellenálló képessége

## Egy empirikus alapú vizsgálat eredményei

Mariela Tapia\*, Pablo Thier, Prof. Dr. Stefan Gößling-Reisemann (†)

*Brémai Egyetem, Rugalmas Energiarendszerek Kutatócsoport,  
Enrique-Schmidt-Str. 7, 28359 Bréma, Németország*

### Absztrakt

Az energiarendszerek mélyreható átalakuláson mennek keresztül a kiber-fizikai rendszerek irányába. Az energiarendszer átalakulása és az összekapcsolt rendszerek összetettsége miatt bekövetkező zavaró változások új, ismeretlen és kiszámíthatatlan kockázatoknak teszik ki a villamosenergia-rendszert. A kritikus pontok azonosítása érdekében sebezhetőségi vizsgálatot végeztek, amelyben az energiaágazat, valamint az információs és kommunikációs technológiák (IKT) szakértői vettek részt. A gyenge pontokat azonosították, például a szakpolitikák végrehajtásának hiányát, amelyet az érintett szereplők felkészületlensége súlyosbít. Az IKT összetett dinamikája miatt nem lehetséges a potenciális stresszorok teljes körű nyilvántartása a megfelelő felkészülési és megelőzési mechanizmusok meghatározása érdekében. Ezért javasoljuk, hogy a rendszer ellenálló képességének növelése érdekében alkalmazzunk rugalmassági menedzsment megközelítést. Ennek célja a hibák jobb átvészélése, ahelyett, hogy magasabb falakat építenénk. Arra a következtetésre jutunk, hogy a rugalmasság kiberfizikai energiarendszereknél való kiépítése megvalósítható, és segít a váratlan eseményekre való felkészülésben.

**Kulcsszavak:** kiber-fizikai energiarendszerek, ellenálló képesség kezelése, sebezhetőségi értékelés, vezérelv, ellenálló képességet fokozó intézkedések

**\*Korrespondáló** szerző. E-mail cím: mariela.tapia @ uni-bremen.de

## Köszönetnyilvánítás

Szeretnénk mély hálánkat kifejezni szeretett témavezetőnknek és barátunknak, Prof. Dr. Stefan Gößling-Reisemann-nak a *Strom-Resilienz* kutatási projekt fejlesztése során nyújtott rendkívül értékes meglátásaiért és hozzájárulásáért. Irányítását, lelkes bátorítását és konstruktív kritikáit mindig nagyra értékeltük.

Külön köszönetünket fejezzük ki Prof. em. Dr. Arnim von Gleichnek a sebezhetőséggel és ellenálló képességgel kapcsolatos témákról folytatott gyümölcsöző megbeszéléseiért.

Szeretnénk továbbá köszönetet mondani a *Strom-Resilienz* kutatási projekt keretében készített interjúkban és műhelytalálkozókban részt vevő szakértőknek értékes észrevételeikért és értő vitáikért.

Köszönet az *Ökológiai Gazdaságkutató Intézetnek* (Institut für ökologische Wirtschaftsforschung, *IÖW*) és a projektpartnereknek Astrid Aretznek, Mark Boostnak és Prof. Dr. Bernd Hirschlnek a *Strom-Resilienz* kutatási projekt aktív együttműködéséért és irányításáért.

Köszönjük Max Spengler támogatását az interjúk tartalomelemzésében, valamint Luis Rivera segítségét az interjúk átírásában és a műhelymunkák megszervezésében. Nagyra értékeljük továbbá Timseabasi Thomas és Cécile Pot d'or támogatását a dokumentum lektorálásában.

Ez a kézirat a *Strom-Resilienz* kutatási projekt eredményein alapul, amelyet a Német Szövetségi Oktatási és Kutatási Minisztérium az Innovációs és Technológiai Elemzés (ITA) program keretében, FKZ 16I1678 támogatással támogatott. A munka egy korábbi változata a projekt zárójelentésében jelent meg német nyelven (lásd (Hirschl et al., 2018)).

# A tartalomjegyzék

	<b>Absztrakt</b>	<b>3</b>
	<b>Köszönetnyilvánítás</b>	<b>4</b>
	<b>Tartalomjegyzék</b>	<b>5</b>
	<b>rövidítések jegyzéke</b>	<b>9</b>
	<b>Táblázatok listája</b>	<b>11</b>
	<b>Ábrák jegyzéke</b>	<b>12</b>
<b>A</b>		
	<b>összefoglaló</b>	<b>17</b>
	<b>Bevezetés</b>	<b>17</b>
	<b>Módszertan</b>	<b>18</b>
	megközelítése	18
	megközelítés	19
	<b>eredményei</b>	<b>20</b>
	Technológia	21
	irányelvek és eljárások	21
	tényező	22
	Szabályzat	23
	<b>stratégia</b>	<b>23</b>
	<b>Következtetések</b>	<b>25</b>
<b>1 Bevezetés</b>		
<b>2 Vezetői</b>		
A sebezhetőségi értékelés		
Rugalmassági menedzsment		
<b>A sebezhetőségi értékelés</b>		
Szervezeti biztonsági		
Az emberi		
<b>Rugalmassági menedzsment</b>		
<b>3 Módszertan</b>		
<b>3.1 Sebezhetőségi értékelési</b>	<b>módszertan</b>	<b>27</b>
3.1.1 A sebezhetőségi értékelés	minősítése	30
3.1.2 Referencia-architektúra	modell	32
3.1.3 Szakértői	műhelyek	35
3.1.3.1 Első szakértői	műhely	35
3.1.3.2 Második szakértői	munkaértekezletek	36
3.1.4 Szakértői	interjúk	36
3.1.5 Minőségi	tartomelemzés	37
<b>3.2 Rugalmassági menedzsment</b>	<b>megközelítés</b>	<b>37</b>
3.2.1 Felkészülés	és megelőzés	39
3.2.2 Robusztus és elővigyázatos	rendszertervezés megvalósítása	40

3.2.3	Kezelés és	helyreállítás	42
3.2.4	Tanuljunk a jövőre	nézve	42
<b>4</b>	<b>Sebezhetőségi értékelés eredményei</b>		<b>43</b>
	<b>4.1 Technológia</b>		<b>43</b>
	4.1.1 Bizonytalan kommunikáció		43
	4.1.1.1.1 Expozíció és érzékenység		44
	4.1.1.1.2 Atámadásmechanizmusok és stresszorok		49
	4.1.1.1.3 Potenciális hatások		54
	4.1.1.1.4 Potenciális hatások minősítése		56
	4.1.1.1.5 Adaptációs stratégiák és végrehajtás		56
	4.1.1.1.6 Adaptációs kapacitás minősítés		57
	4.1.1.1.7 Sérülékenységi besorolás		58
	4.1.2 Biztonságtalan végpontok		59
	4.1.2.1 Expozíció és érzékenység		59
	4.1.2.2.1 Atámadásmechanizmusok és stresszorok		61
	4.1.2.2.2 A rendszer szolgáltatásaira gyakorolt lehetséges hatások		62
	4.1.2.2.3 Potenciális hatásminősítés		64
	4.1.2.2.4 Adaptációs stratégiák és végrehajtás		64
	4.1.2.2.5 Adaptációs kapacitás minősítés		66
	4.1.2.2.6 Sérülékenységi besorolás		66
	4.1.3 Egyéb technológiával kapcsolatos feltételek		68
	<b>4.2 Szervezetibiztonsági irányelvek és eljárások</b>		<b>68</b>
	4.2.1 Az interdiszciplináris IT-OT ismeretek hiánya		68
	4.2.1.1 Expozíció és érzékenység		68
	4.2.1.2 Atámadásmechanizmusok és stresszorok		69
	4.2.1.3 Potenciális hatások		70
	4.2.1.4 Potenciális hatások minősítése		70
	4.2.1.5 Adaptációs stratégiák és végrehajtás		70
	4.2.1.6 Az alkalmazkodóképesség minősítése		71
	4.2.1.7 Sérülékenységi besorolás		71
	4.2.2 Tökéletesbiztonsági javítások kezelése		72
	4.2.2.1 Kitérő érzékenység		72
	4.2.2.2.1 Atámadásmechanizmus és stresszorok		73
	4.2.2.2.2 Potenciális hatások		73
	4.2.2.2.3 Potenciális hatások minősítése		73
	4.2.2.2.4 Adaptációs stratégiák és végrehajtás		73
	4.2.2.2.5 Adaptációs kapacitás minősítés		74
	4.2.2.2.6 Sérülékenységi besorolás		74
	<b>4.3 Az emberi tényező</b>		<b>75</b>

**4.3.1 A biztonságtudatosság hiánya vagy a biztonsági irányelvekre adott gyenge válasz a szervezeten belül**75

- 4.3.1.1 Expozíció és érzékenység75
- 4.3.1.2 Támadási mechanizmusok és stresszorok76
- 4.3.1.3 Potenciális hatások78
- 4.3.1.4 A lehetséges hatások értékelése78
- 4.3.1.5 Alkalmazkodási stratégiák és végrehajtás78
- 4.3.1.6 Alkalmazkodóképesség minősítés79
- 4.3.1.7 Sebezhetőségi besorolás79

**4.3.2 A fogyasztók biztonságtudatosságának**

hiánya80

- 4.3.2.1 Expozíció és érzékenység80
- 4.3.2.2 Támadási mechanizmusok és stresszorok81
- 4.3.2.3 Potenciális hatások81
- 4.3.2.4 Potenciális hatások értékelése81
- 4.3.2.5 Alkalmazkodóképesség minősítés82
- 4.3.2.6 Sebezhetőségi besorolás82

**4.4 Szabályzat**83

**4.4.1 A biztonsági előírások és rendeletek hatékony végrehajtásának**

hiánya83

- 4.4.1.1 Expozíció és érzékenység83
- 4.4.1.2 Támadási mechanizmus és stresszorok83
- 4.4.1.3 Potenciális hatások83
- 4.4.1.4 Potenciális hatások értékelése84
- 4.4.1.5 Alkalmazkodási stratégiák és végrehajtás84
- 4.4.1.6 Alkalmazkodóképesség minősítés84
- 4.4.1.7 Sebezhetőségi besorolás84

---

4.4.2	A	biztonságjavítására irányuló összehangolt erőfeszítések	hiánya85
4.5		<b>Az eseményalapú sebezhetőségi értékelés módszertanának szemléltetése87</b>	
4.6		<b>A sebezhetőségi értékelés összefoglalója90</b>	
5		<b>Rugalmassági menedzsment stratégia91</b>	
5.1		<b>Felkészülés és megelőzés91</b>	
5.1.1		Informatikai megelőzési mechanizmus93	
5.2		<b>Megbízható és elővigyázatos végrehajtása95</b>	tervezés
5.2.1		Észlelési mechanizmus97	
5.3		<b>Válságokkezelése és a válságbólvaló kilábalás98</b>	
5.4		<b>Tanuljon a jövőre</b>	nézve99
5.5		<b>A rugalmassági összefoglalása100</b>	stratégia
6		<b>Következtetések és kilátások104</b>	
7		<b>Referenciák107</b>	
A. függelék:		<b>Interjúelemzési módszertan114</b>	
		<b>Szakértői interjúk114</b>	
		<b>Kérdőív114</b>	
		<b>A tartalomelemzés módszertanának áttekintése115</b>	
		<b>tartalom kódolása118</b>	

## A rövidítések jegyzéke

	BDEWBundesverbandder Energie- und Wasserwirtschaft E.V
	BSIG GermanFederal Office for Information Security ( NémetSzövetségi Információbiztonsági Hivatal)
	CERTComputerEmergency Response Team for Federal Agencies
	CPPSCyber-physicalPower Systems ( kiber-fizikaienergiarendszerek )
	DAData hozzáférés
	DDoSDistributedDenial of Service ( elosztottszolgáltatásmegtagadás )
	DERDistributedEnergy Resources ( elosztottenergiaforrások )
DMSD	forgalomirányítási rendszerek
	DNP3Delosztotthálózati protokoll
	DOSDenial-of-Service
DSO	Delosztórendszer-üzemeltető
EMSE	Energiairányítási rendszerek
Ügynökség	ENISAEurópaiHálózat- és Információbiztonsági Ügynökség
	EVElektromosjármű
	GOOSEGenerikusobjektumorientált alállomásesemény
	HANHomeArea Network
	HMIHumanMachine Interface
	ICSIndustriálisvezérlőrendszerek
	ICTInformációsés kommunikációs technológiák
	IDHatolástészlelő rendszerek
	IECNemzetközielektrotechnikai bizottság
	IEDIntelligenselektronikus eszközök
	IoTInternetof Things
ISMS	Információbiztonsági irányítási rendszer
	ITInformációs technológia
	ICTInformációsés kommunikációs technológiák
	LMNLocalMetrológiai Hálózat
	MITMMan-In-The-Middle
	MSPCMultivariánsstatisztikai folyamatszabályozás
	NESCORNationalElectric Sector Cybersecurity Organization
Resource	NIDSNetwork-BasedIntrusion Detection System ( Hálózat

alapú behatolásérzékelő rendszer)

NIST Nemzeti Szabványügyi és Technológiai Intézet  
oK Open Konzequenze

OPCOLEa folyamatirányításhoz  
OTOműködési technológia  
PKIPublicKey Infrastructure  
PPPVédelmi profil  
PVFotovoltaikus  
RBACRole-alapú hozzáférés-szabályozás  
RMResilience Management  
RTURemoteterminál egység  
SAIDISrendszerátlagos megszakítási időtartam indexe  
SCADASfelügyeletivezérlés és adatgyűjtés  
SEPSmartEnergy profil  
SGAMSmartGrid architektúra modell  
SMGASmartMeter Gateway rendszergazda  
SMGWSmartMeter Gateway  
TNCTrustedNetwork Connect  
UPSEnergyellátás biztonsági mentések  
VAVsebezhetőségi értékelés  
VDEVerbandDer Elektrotechnik Elektronik Informationstechnik  
WANWideArea Network ( széleskörűhálózat )  
ZLLZigbeeLight Link

## A táblázatok listája

1. táblázat. A kiber-fizikai villamosenergia-rendszer rendszerszolgáltatásainak meghatározása, amely figyelembe veszi a villamosenergia-infrastruktúra és az IKT-infrastruktúra kritériumait. Forrás: A szerzők saját összeállítása (Gößling-Reisemann et al., 2013; von Gleich et al., 2010) alapján.

2. táblázat. A kiberfizikai energiarendszerek kritikus tulajdonságait, struktúráit és elemeit tükröző kategóriák és kategóriák

táblázat A kiber-fizikai energia kritikus tulajdonságait, struktúráit és elemeit tükröző kategóriák és alkategóriák, valamint a potenciális hatások, az alkalmazkodóképesség és a sebezhetőség megfelelő minősítései az L: alacsony, M: közepes, H: magas skálán

4. táblázat: Az ellenálló képességet fokozó intézkedések és elemek a technológia kategóriában a következő fázisok szerint: (1) Felkészülés és megelőzés, (2) Robusztus és elővigyázatos tervezés végrehajtása, (3) Kezelés és helyreállítás, valamint (4) Tanulás a jövőre nézve. Forrás: Saját ábrázolás.

..... 101

5. táblázat: Ellenálló képességet fokozó intézkedések és elemek a Szervezeti biztonsági politikák és eljárások kategóriában a következő fázisok szerint: (1) Felkészülés és megelőzés, (2) Robusztus és elővigyázatos tervezés végrehajtása, (3) Kezelés és helyreállítás, valamint (4) Tanulás a jövőre nézve. Forrás: A biztonság és a biztonság védelme: Saját

..... ábr

ázolás102

6. táblázat: Az emberi tényező kategória ellenálló képességet fokozó intézkedései és elemei a következő fázisok szerint: (1) Felkészülés és megelőzés, (2) Robusztus és elővigyázatos tervezés végrehajtása, (3) Kezelés és helyreállítás, valamint (4) Tanulás a jövőre nézve. Forrás: Az emberi tényező és az emberiség elleni küzdelem: Saját ábrázolás.

..... 103

7. táblázat: Az ellenálló képességet fokozó intézkedések és elemek a Rendeletek

kategóriában, majd az (1) Felkészülés és megelőzés, (2) Robusztus és elővigyázatos tervezés végrehajtása, (3) Kezelés és helyreállítás, valamint (4) Tanulás a jövőre nézve.

Source:

Saját

..... ábr

ácsolás103

táblázat                    A                    szakértői                    interjú                    és                    a  
..... műhelybe  
szélgetések alapján                    kialakított                    kezdeti  
..... kódrendszer

er120

táblázat Végleges kódrendszer, amely a megkérdezett szakértők által átadott tartalmakat rögzíti, és amelyet a sebezhetőségek értékeléséhez és az ellenálló képességet fokozó intézkedések levezetéséhez használtak fel.

..... 122

## A ábrák listája

1. ábra. Az eseményalapú sebezhetőségi értékelés (EVA) módszertanának vázlatos ábrázolása. Saját ábrázolás (Gößling-Reisemann et al., 2013; von Gleich et al., 2010)28
2. ábra. A strukturális sérülékenységvizsgálat (SVA) módszertanának vázlatos ábrázolása. Saját ábrázolás (Gößling-Reisemann et al., 2013; von Gleich et al., 2010) alapján 28
3. ábra A sebezhetőségi értékelési mátrix, amely figyelembe veszi a rendszer szolgáltatásaira és az alkalmazkodóképességre gyakorolt lehetséges hatások szintjét. (H: magas, M: közepes, L: alacsony). Forrás: A szerzők saját összeállítása (Gößling-Reisemann et al., 2013; von Gleich et al., 2010)31alapján. 20
4. ábra A sebezhetőségi vizsgálathoz használt referenciaarchitektúra-modell. Forrás: (IEC, 20)32
5. ábra Smart Grid sík. Forrás: (CEN-CENELEC-ETSI Intelligens Hálózat Koordinációs Csoport, 12)33
6. ábra Kategóriák a megkérdezettek szakterülete és a résztvevők száma szerint37
7. ábra A rendszer különböző stresszorokra való felkészültségéhez szükséges képességek hozzárendelése. A stresszorok a bekövetkezés ideje és a tudatosság mértéke szerint vannak megkülönböztetve. Forrás: (Gößling-Reisemann, 16)38
8. ábra A rugalmas irányítási megközelítés sémája, amely a négy fázist és az egyes fázisokhoz javasolt intézkedések meghatározásának forrásait mutatja. Forrás: Acatech et al., 2017; Goessling-Reisemann és Thier, 20

19)39 alapján készült saját ábrázolás.

9. ábra A rendszerek ellenálló képességét növelő elvek és elemek áttekintése. Forrás: (Goessling-Reisemann és Thier, ..... 20

19)42

10. ábra Smart Meter Gateway architektúra. Forrás: (BSI, ..... 2015a)4  
5

11. ábra A DER-eket tartalmazó energiarendszerek általános felépítése. Forrás: (Qi et al., 2016)  
47

12. ábra A "Crashoverride/Industroyer" komponensek egyszerűsített vázlata. Forrás (Cherepanov és Lipovsky, ..... 20

17)52

13. ábra A kiberfizikai energiarendszerek sebezhetőségének értékelése a nem biztonságos kommunikáció miatt. Az értékeléshez a villamosenergia-rendszer SGAM-tartományait három csoportba soroltuk: a) fogyasztás, b) elosztott energiaforrások (DER) és elosztás, c) termelés és átvitel. Forrás: A szerzők saját ábrázolása.....  
58

14. ábra A kiberfizikai energiarendszerek sebezhetőségének értékelése a nem biztonságos végpontok miatt. Az értékeléshez a villamosenergia-rendszer SGAM-tartományait három csoportba soroltuk: (a) fogyasztás, b) elosztott energiaforrások, c) termelés, átvitel és elosztás. Forrás: A szerzők saját ábrázolása .....  
67
15. ábra A kiber-fizikai energiarendszerek sebezhetőségének értékelése az interdiszciplináris IT-OT ismeretek hiánya miatt. Forrás: A szerzők saját ábrázolása .....  
72
16. ábra A kiberfizikai energiarendszerek sebezhetőségének értékelése a nem megfelelő biztonsági javítások kezelése miatt. Forrás: A szerzők saját ábrázolása.....  
74
17. ábra: A Stuxnet működése. Forrás (Kushner, ..... 2013)77
18. ábra A kiberfizikai energiarendszerek sebezhetőségének értékelésének összefoglalása a biztonságtudatosság hiánya vagy a szervezeten belüli biztonsági irányelvekre való gyenge reagálás miatt. Forrás: A szerzők saját ábrázolása .....  
80
19. ábra A kiberfizikai energiarendszerek sebezhetőségének értékelése a fogyasztók biztonságtudatosságának hiánya miatt. Forrás: A szerzők saját ábrázolása .....  
82
20. ábra A kiberfizikai energiarendszerek sebezhetőségének értékelése a biztonsági szabványok és előírások hatékony végrehajtásának hiánya miatt. Forrás: A szerzők saját ..... ábrázolása85
21. ábra A stresszorok referenciaarchitektúra-modelljének elhelyezkedése az eseményalapú VA alkalmazásának példaként. A stresszorok számozása a következő: (1) GPS-jel hamisítás, (2) a SCADA-rendszerek elleni belső fenyegetés, (3) az ICS firmware manipulálása az alállomásokon, és (4) a fejlett mérési infrastruktúra adatainak lehallgatása87
22. ábra A CPPS sebezhetőségének értékelése a stresszor (1) GPS-jel hamisítás miatt. Forrás: Saját ..... ábrázolás.88
23. ábra A CPPS sebezhetőségének értékelése a (2) stresszor (SCADA-rendszereken belüli

belső fenyegetés) miatt. Forrás: Saját

..... áb  
rázolás88

24. ábra A CPPS sebezhetőségének értékelése a stresszor (3) ICS firmware manipulálása miatt az alállomásokon. Forrás: Saját

..... áb  
rázolás89

ábra A CPPS sebezhetőségének értékelése a (4) stresszor (Advance Metering Infrastructure data eavesdropping) miatt. Forrás: Saját

..... áb  
rázolás89

# 1 Bevezetés

A villamosenergia-rendszerek az információs és kommunikációs technológiákkal (IKT) való egyre nagyobb mértékű konvergencia révén fejlődnek, ami komplex kiber-fizikai villamosenergia-rendszerekhez (CPPS) vezet. Ez lehetőséget teremtett a rendszerek teljesítményének fokozására, és megoldásokat kínál az elosztott és ingadozó megújuló energiaforrásokon alapuló energiaellátás kapcsolódó kihívásainak kezelésére. Ugyanakkor azonban a villamosenergia- és az IKT-infrastruktúrák közötti kiterjedt összekapcsolódás és kölcsönös függőség új, ismeretlen és kiszámíthatatlan kockázatoknak teszi ki a villamosenergia-rendszert.

Az energiarendszereket célzó kibertámadások száma és kifinomultsága az elmúlt években egyre nőtt. Az ukrán villamosenergia-hálózatot ért kibertámadás 2015 decemberében, amikor ismeretlen kiberszereplők megzavarták az energiahálózat működését, ami több mint 225 000 fogyasztó számára okozott áramkimaradást (Styzcynski és Beach-Westmoreland, 2017). Egy évvel később, 2016 decemberében egy ukrain átviteli szintű alállomást érintett egy "Crashoverride" néven azonosított rosszindulatú szoftver keretrendszer, ami meg nem határozott számú fogyasztó számára okozott kiesést (Dragos Inc., 2017). Ezek voltak az első bejelentett ilyen jellegű támadások, de az elmúlt években más esetekben is feltételeztek kibertámadásokat az energiarendszerek ellen. Például 2016 és 2018 között orosz hackerek hozzáférést szereztek az Egyesült Államok áramszolgáltatóinak vezérlőtermeihez, ami lehetővé tette számukra, hogy leállítsák a hálózatokat és áramkimaradásokat okozzanak (Cellan-Jones, 2018). Ebben az esetben a támadók a hozzáférést rosszindulatú szoftverek színrevitelével és spear phishing segítségével nyerték el (Department of Homeland Security, 2018). Bár a támadás és az amerikai elektromos hálózatban bekövetkezett tényleges áramkimaradások közötti kapcsolat nem volt egyértelmű, ez arra készítette a Belbiztonsági Minisztériumot és a Szövetségi Nyomozó Irodát, hogy felderítési és megelőzési irányelveket dolgozzon ki az ilyen tevékenységek ellen. Egy másik incidensről 2019. március 5-én számoltak be. Az Egyesült Államok nyugati részén az egyik elektromos közműszolgáltatóban szolgáltatásmegtagadási incidens miatt zavarok keletkeztek. Ez a támadás nem okozott áramkimaradást vagy kárt az energiatermelésben, és nem világos, hogy a nyugati átviteli hálózat szándékos célpont volt-e. De a közmű felügyeleti irányító és adatgyűjtő (SCADA) rendszerének bizonyos részei számára láthatóságvesztéshez vezetett, ezért az érintett kategóriába sorolták (Sobczak, 2019).

A sebezhetőség- és kockázatértékeléseket kulcsfontosságú intézkedésnek tekintik az energiarendszerek kiberbiztonsága szempontjából, lásd (Arghandeh et al., 2016; NIST,

2014; Rossebo et al., 2017; Teixeira et al., 2015), mivel az ismert sebezhetőségek és a rendszer biztonságára gyakorolt hatásuk azonosítása lehetővé teszi a sebezhetőségek kezelésére szolgáló módszerek kidolgozását. Ezekben a tanulmányokban a potenciális veszélyek listái és azok előfordulási valószínűsége alapján értékelték a lehetséges hatásokat és az enyhítési lehetőségeket.

Úgy véljük, hogy az IKT dinamikus jellege és a villamosenergia-infrastruktúrával való összetett kölcsönhatása miatt meglepetésekre kell számítanunk. Többé nem lesz lehetséges a potenciális veszélyek átfogó leltárát meghatározni, ahogyan az a klasszikus kockázatkezelésben történik. A megbízható áramellátás az élet szinte minden területe számára nagy jelentőséggel bír, ezért olyan stratégiákat kell kidolgozni, amelyek lehetővé teszik, hogy az energiarendszer felkészüljön a várható és váratlan stresszorokra. Más szóval, elengedhetetlen a rugalmassági menedzsment stratégia alkalmazása. A reziliencia számos definíciója létezik a tudományos közösségben (pl. (Jesse et al., 2019)). Jelen tanulmányban a rezilienciát úgy írjuk le, mint egy (társadalmi-technikai) rendszer azon képességét, hogy stressz és turbulens körülmények között is képes fenntartani szolgáltatásait (Brand et al., 2017; von Gleich et al., 2010). E definíció használatának előnye, hogy a rendszer szolgáltatásaira összpontosít, amelyeket az érintettekkel/felhasználókkal együtt kell felvázolni. Ily módon lehetővé válnak a rendszer változásai és fejlődései, amelyek az átmenetek központi szempontjai. A hangsúly az összekapcsoltság és az egymásrataltság összetett jellegén, valamint a rendszer azon képességén van, hogy szolgáltatásait fenntartsa.

Ez a kézirat a *Strom- Resilienz* kutatási projekt két munkacsomagjának (1) eredményeit mutatja be, amelyek a villamosenergia-rendszerek digitalizációjának sebezhetőségére és ellenálló képességére összpontosítottak. A projektet a Brémai Egyetem *Resilient Energy Systems* kutatócsoportja dolgozta ki az *Ökológiai Gazdaságkutató Intézettel* (Institut für ökologische Wirtschaftsforschung, *IÖW*) együttműködésben 2015 szeptembere és 2017 novembere között.

Az említett munkacsomagok fő célkitűzése az volt, hogy meghatározzák, milyen további sebezhetőségek merülhetnek fel a villamosenergia-rendszerek digitalizálásával, és milyen stratégiák szükségesek a villamosenergia-rendszerek ellenálló képességének növeléséhez, hogy a rendszer elsődleges funkciói még stresszhelyzetben is fennmaradjanak. A tanulmány két részből állt. Először egy sebezhetőségi vizsgálatot (VA) végeztünk, hogy azonosítsuk azokat a kritikus tulajdonságokat, struktúrákat és elemeket, amelyek a rendszert sebezhetővé teszik a kibertámadásokkal szemben. E célból interdiszciplináris megközelítést választottak, amelyben az energiaágazat érdekelt felei és az IKT-megoldások szolgáltatói interjúk és műhelybeszélgetések révén vettek részt. Másodsor, a rugalmas menedzsment megközelítés alkalmazásával ellenálló stratégiát dolgoztak ki annak meghatározására, hogy a kiber-fizikai rendszerek hogyan készülhetnek fel jobban bármilyen stresszorra.

A kézirat további része a következőképpen épül fel: a 2. fejezetben található összefoglaló kiemeli az alkalmazott módszerekkel és a főbb eredményekkel kapcsolatos fontos szempontokat. A 3. szakasz rövid elméleti háttérrel nyújt a sebezhetőség és az ellenálló

~~vizsgálati eredményei.~~  
képesség fogalmaival kapcsolatban, és részletesen ismerteti a sebezhetőség értékelésére alkalmazott módszereket és a

---

<sup>1</sup> 2. munkacsomag: A lehetséges zavaró események meghatározása és elemzése, valamint az ellenálló képesség kritériumainak konkretizálása, és 3. munkacsomag: A sebezhetőség minimalizálására és az ellenálló képesség maximalizálására irányuló lehetőségek meghatározása.

rugalmassági menedzsment stratégia. A 4. szakasz a sebezhetőségi értékelés eredményeit tárgyalja. Az 5. szakasz az ellenálló képesség kezelési stratégia eredményeit tárgyalja. A 6. szakasz a kéziratot következtetésekkel és kilátásokkal zárja.

## 2 Összefoglaló

*Megjegyzés: Ez a rész a TATuP Vol 29 No 1 (2020) című folyóiratban már megjelent munka (Tapia et al., 2020) preprint változata: Cybersecurity. Fenyegetés, sebezhetőség, értékek és károk. A végleges változatot lásd a <https://doi.org/10.14512/tatup.29.1.23> oldalon.*

### Bevezetés

A villamosenergia-rendszerek az információs és kommunikációs technológiákkal (IKT) való kiterjedt konvergencián keresztül fejlődnek, ami komplex kiber-fizikai villamosenergia-rendszerekhez (CPPS) vezet. Ez lehetőséget teremtett a rendszerek teljesítményének fokozására, és megoldásokat kínál az elosztott és ingadozó megújuló energiaforrásokon alapuló energiaellátás kapcsolódó kihívásainak kezelésére. Az utóbbi években azonban egyre több és kifinomultabb kibertámadás éri az energiarendszereket. Ilyen például az ukrán villamosenergia-hálózat elleni 2015-ös és 2016-os támadások, amelyek áramkimaradásokat eredményeztek (Dragos Inc., 2017). Az Egyesült Államokban 2019 márciusában újabb, egy közműszolgáltató ellen irányuló incidensről számoltak be (Sobczak, 2019). Az elmúlt években több kockázat- és sebezhetőségi értékelést is közzétettek az energiarendszerekre vonatkozóan, pl. (NIST, 2014; Rossebo et al., 2017). Ezekben a tanulmányokban a potenciális veszélyek listái és azok előfordulási valószínűsége alapján értékelték a potenciális hatásokat és az enyhítési lehetőségeket. Álláspontunk szerint az IKT dinamikus jellege és a villamosenergia-infrastruktúrával való összetett kölcsönös függősége miatt meglepetésekkel kell számolnunk. Többé nem lesz lehetséges a potenciális veszélyek átfogó jegyzékét meghatározni, ahogyan az a klasszikus kockázatkezelésben történik.

A megbízható áramellátás az élet szinte minden területén nagy jelentőséggel bír, ezért olyan stratégiákat kell kidolgozni, amelyek lehetővé teszik, hogy az energiarendszer felkészüljön a várható és váratlan stresszhatásokra. Más szóval, elengedhetetlen a rugalmassági menedzsment stratégia alkalmazása. A reziliencia számos definíciója létezik a tudományos közösségben, pl. (Jesse et al., 2019). Jelen tanulmányban a rezilienciát úgy írjuk le, mint *egy (társadalmi-technikai) rendszer azon képességét, hogy stressz és turbulens körülmények között is képes fenntartani szolgáltatásait* (Brand et al., 2017; von Gleich et al., 2010). E definíció használatának előnye, hogy a *rendszer szolgáltatásaira* összpontosít, amelyeket az érintettekkel/felhasználókkal együtt kell felvázolni. Ily módon lehetővé válnak a rendszer változásai és fejlődései, amelyek az átmenetek központi szempontjai. A hangsúly az összekapcsoltság és az egymásra utaltság összetett jellegén, valamint a rendszer azon képességén van, hogy *szolgáltatásait* fenntartsa.

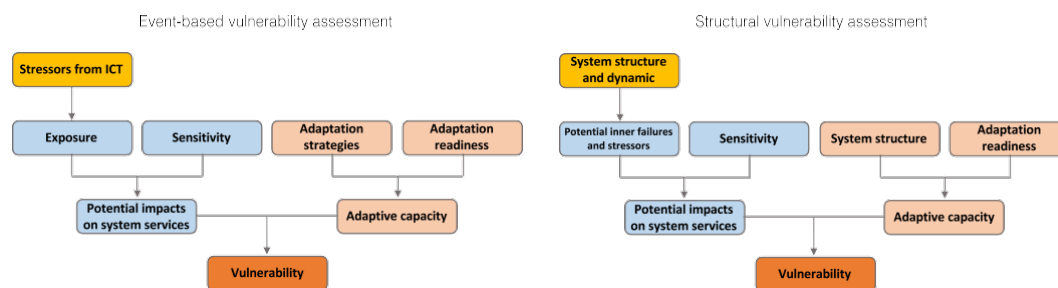
Ez a cikk egy empirikus és interdiszciplináris alapkutatás eredményeit mutatja be, amely az energia- és az IKT-ágazat szereplőinek bevonásával, interjúk és műhelybeszélgetések révén, jobb betekintést nyújt a következőkbe

a CPPS sebezhetőségét. A tanulmány két részből áll. Először is sebezhetőségi vizsgálatot végeztek az IKT-infrastruktúrából származó kritikus pontok azonosítására. Másodsor, a rugalmassági menedzsment megközelítés alkalmazásával ellenálló stratégiát dolgoztak ki annak meghatározására, hogy a CPPS hogyan tud jobban felkészülni bármilyen stresszorra.

## Módszertan

### Sebezhetőségi értékelés Megközelítés

A (Gößling-Reisemann et al., 2013; von Gleich et al., 2010) által végzett eseményalapú és strukturális VA módszereket (1. ábra) használtuk referenciaként ehhez a tanulmányhoz.



1. ábra A VA-módszertan vázlatos ábrázolása. Balra: eseményalapú VA. Jobbra: Strukturális VA. Forrás: A szerzők saját összeállítású a következők alapján (Gößling-Reisemann et al., 2013; von Gleich et al., 2010)

A lehetséges hatásokat a *rendszer szolgáltatásaira* gyakorolt hatásuk alapján értékelték, amelyeket ebben az esetben mind az elektromos, mind az IKT-infrastruktúra paraméterei alapján határoztak meg. Az elektromos infrastruktúra tekintetében a mennyiségi kritériumokat a rendszer azon képessége határozza meg, hogy képes-e ellátni a csatlakoztatott terhelést. A minőségi kritériumokat közvetlen műszaki paraméterek, például a teljesítményminőség vagy a megbízhatósági mutatók, valamint közvetett paraméterek, például a társadalmi-gazdasági és társadalmi-ökológiai hatások határozzák meg. Az IKT-infrastruktúra tekintetében a megközelítés figyelembe veszi a biztonsági követelményekre gyakorolt hatást, azaz az átmenő vagy nyugvó adatok (pl. vezérlőparancsok, firmware, szoftver stb.) titkosságát, integritását, rendelkezésre állását és letagadhatatlanságát.

A tanulmány a német és az európai villamosenergia-rendszerre összpontosított, amely a teljes elektromos energiaátalakítási láncot lefedte, és az IKT-infrastruktúrából származó stresszorok értékelésére korlátozódott. Referencia-architektúramodellként az intelligens hálózat architektúramodelljének (2) komponensrétegét használták. A 2016 júniusa és 2017 márciusa közötti időszakban két workshopot és 19 félig strukturált interjút végeztek az alábbi ágazatok szakértőivel: energia, ipari automatizálás, IKT és állami szervek. A szakértői nyilatkozatokat értékelték

---

<sup>2</sup> <http://smartgridstandardsmap.com/>

egy átfogó kvalitatív tartalomelemzési módszertan segítségével (Mayring, 2014).

A szakértők véleményét, a vonatkozó szakirodalmat és a saját megítélésünket ötvözve a lehetséges hatásokat minőségileg magas, közepes vagy alacsony szintre soroltuk a stresszorok és a strukturális gyengeségek által a rendszer szolgáltatásainak minőségi és mennyiségi kritériumaira gyakorolt hatások alapján. Az alkalmazkodóképesség meghatározásához figyelembe vettük a szakértők és a szakirodalom által adott információkat a meglévő vagy tervezett alkalmazkodási mechanizmusokról és az érintett szereplők hajlandóságáról azok végrehajtására. Ezeket minőségileg is magas, közepes vagy alacsony szintre értékelték. Következésképpen a sebezhetőségi szint a lehetséges hatások és az alkalmazkodóképesség kombinációjának eredménye volt a 2. ábrán látható mátrix szerint.

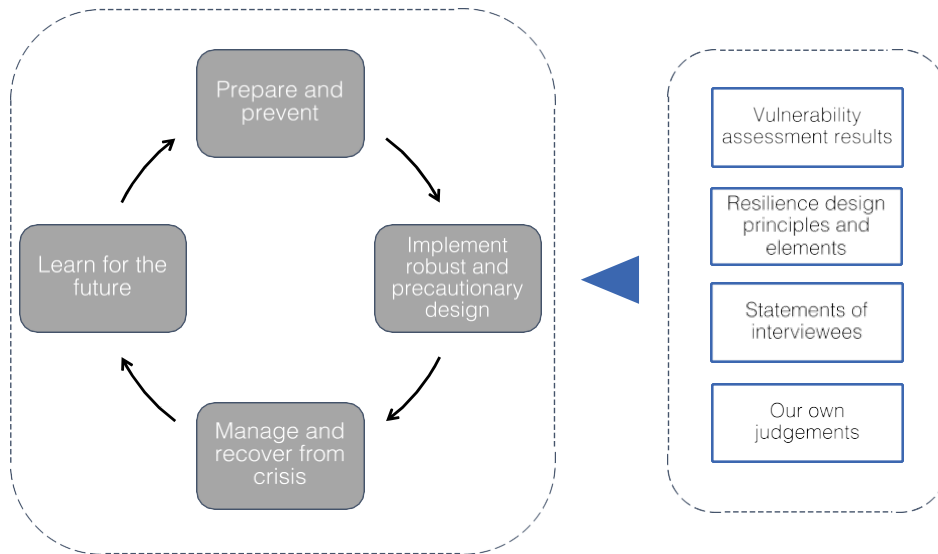
**Sebezhetőségi értékelési mátrix**

P o t e n c i á l i s h a t á s o k	Magas	H	H	M
	Közepes	H	M	L
	Alacsony	M	L	L
		Alacsony	Közepes	Magas
		Alkalmazkodóképesség		

**2. ábra:** A sebezhetőségi értékelési mátrix, amely figyelembe veszi a rendszer szolgáltatásaira és az alkalmazkodóképességre gyakorolt lehetséges hatások szintjét. (H: magas, M: közepes, L: alacsony). *Forrás: A szerzők saját összeállítása (Gößling-Reisemann et al., 2013; von Gleich et al., 2010) alapján.*

## Rugalmasági menedzsment Megközelítés

Az ellenálló CPPS-nek sokféle képességgel kell rendelkeznie, például ellenálló képességgel/robusztussággal, alkalmazkodással, innovációval és improvizációval az ismert és ismeretlen stresszorok leküzdésére. Ezek segítik a rendszereket a *rendszer szolgáltatások* fenntartásában (lásd a fenti meghatározást). Ebben a tanulmányban a (Acatech et al., 2017; Goessling-Reisemann és Thier, 2019) által leírt rezilienciamentedzsment megközelítést használták referenciaként. Ez egy négyfázisú megközelítést foglal magában: (1) Felkészülés és megelőzés, (2) Robusztus és elővigyázatos tervezés végrehajtása, (3) Válságok kezelése és a válságokból való felépülés, valamint (4) Tanulás a jövőre nézve. Az egyes lépésekhez javasolt intézkedéseket a következők alapján dolgoztuk ki: a VA eredményei, a (Brand et al., 2017; Goessling-Reisemann és Thier, 2019), a megkérdezett szakértők nyilatkozatai és saját megítélésünk alapján leírt rugalmasági tervezési elvek/elemek (3. ábra).



ábra: A rugalmas irányítási megközelítés négy szakasza és az egyes szakaszokhoz javasolt intézkedések meghatározásának forrásai.  
Forrás: A szerzők saját összeállítása (Acatech et al., 2017; Goessling-Reisemann és Thier, 2019) alapján.

## Sebezhetőségi értékelés Eredmények

Az Egyesült Királyság azonosította a CPPS sebezhetőségéhez hozzájáruló kritikus tulajdonságokat, szerkezeteket és elemeket. A kvalitatív tartalomelemzés eredményei alapján a megállapításokat a következő négy kategóriába sorolták: (a) technológia, b) szervezeti biztonsági politikák és eljárások, c) emberi tényező és d) szabályozások. Mindegyik kategória alkategóriákat tartalmazott, és ezeket külön-külön értékelték a fent leírt VA-módszerrel. Valamennyi alkategória *magas* sebezhetőségi minősítést eredményezett a *közepes vagy magas* potenciális hatások és a *közepes vagy alacsony* alkalmazkodóképesség kombinációjában (1. táblázat). A kategóriák és alkategóriák felsorolása nem tekinthető teljes körűnek. Azt tükrözi azonban, hogy a megkérdezetteket megkérdezték arról, hogy véleményük szerint melyek a kritikus pontok, ami a magas sebezhetőségek listáját eredményezte. A következő szakaszban röviden ismertetjük az egyes kategóriákra vonatkozó megállapításokat.

Kategória	Alkategória	Potenciális hatások	Alkalmazkodóképesség	Sebezhetőség
Technológia	Bizonytalan végpontok	M-H	M	H
	Bizonytalan kommunikáció	M-H	M	H
Szervezeti biztonsági politikák és eljárások	Helytelen javításkezelés	M-H	M	H
	Az interdiszciplináris IT-OT ismeretek hiánya	M-H	M	H
Az emberi tényező	A biztonságtudatosság hiánya a szervezetekben	M-H	M	H
	A fogyasztók biztonságtudatosságának hiánya	M-H	L	H
Szabályzat	A szabványok és rendeletek hatékony végrehajtásának hiánya	M-H	M	H
	A biztonság javítására irányuló összehangolt erőfeszítések hiánya	M-H	M	H

**Tab. 1:** A CPPS kritikus tulajdonságait, struktúráit és elemeit tükröző kategóriák és alkategóriák, valamint a potenciális hatások, az alkalmazkodóképesség és a sebezhetőség megfelelő minősítései az L: alacsony, M: közepes, H: magas skálán. *Forrás: A szerzők saját összeállítása*

## Technológia

A CPPS-ben részt vevő rendszerek, végpontok és szereplők megnövekedett száma nagyobb számú összeköttetést és kommunikációt eredményez. Ha ezek a kommunikációk titkosítatlan vagy gyengén titkosított hálózati protokollokat használnak, a hitelesítési kulcsok és az adattartalom kiszolgáltatottá válik (NIST 2014). A Man-in-the-Middle támadások segítségével a fenyegető ügynökök képesek lesznek lehallgatni, beadni vagy manipulálni a csomópontok közötti üzeneteket. Egyrészt az ipari vezérlőrendszerekben (ICS) a termelés, az átvitel és az elosztás területén használt hagyományos kommunikációs protokollok a szabadalmaztatott pont-pont kapcsolatokról és a külső hálózatoktól elszigeteltekben nyílt és szabványos protokollokká fejlődtek. A szakértők szerint ez nagy biztonsági problémát jelent. A "Crashoverride" rosszindulatú szoftver, amelyet a jelek szerint a 2016-os ukrain áramszünet során használtak, jól illusztrálja a fejlett rosszindulatú szoftvereket, amelyek kihasználják egyes ICS-protokollok gyengeségeit (Dragos Inc., 2017). A másik oldalról a szakértők azt is megállapították, hogy minél jobban elosztott és minél közelebb van a végfelhasználóhoz a kommunikáció, annál sebezhetőbbé válik. Ennek oka, hogy az ügyfél telephelyén található eszközöket (pl. Internet-of-Things eszközök) gyenge biztonsági jellemzőkkel telepítik, ráadásul nem is szabályozzák őket. Az esetek többségében nem rendelkeznek a biztonságos kulcskezelés, a hozzáférés-szabályozás vagy a javításkezelés képességeivel. Az intelligens otthoni eszközök biztonsági kihívásait és veszélyeit a (Lee et al., 2014) tárgyalja.

## **Szervezeti biztonsági irányelvek és eljárások**

A szakértők egyetértettek abban, hogy az informatikai és az üzemeltetési technológiák (OT) infrastruktúrái közötti növekvő összetettség és kölcsönös függőség miatt az új technológiák kezeléséhez szükséges tudás

kihívások megváltoztak. A legtöbb esetben az interdiszciplináris tudás hiányzik vagy korlátozott, ezért nehéz a teljes komplex rendszer megfelelő megértése, tervezése, megvalósítása és működtetése. Általában az OT-eszközöket inkább az ICS-üzemeltetők és mérnökök, mint a tapasztalt IT-szakemberek tartják karban, ami gyakori hibákat eredményezhet a karbantartás, a konfiguráció és a keményítés hiánya terén (Bodungen et al., 2017). Ráadásul a tipikus IT-rendszerek biztonsági intézkedései nem alkalmazhatók közvetlenül ICS-környezetekben, mert ez befolyásolhatja a folyamat stabilitását vagy rendelkezésre állását. Ezért speciális és testre szabott biztonsági intézkedésekre van szükség.

Mint a szakértők megállapították, az ICS rendszer általában elavult, vagy azért, mert a gyártók nem biztosítanak biztonsági javításokat, vagy azért, mert az adott rendszer időkritikus. Ennek következtében a támadók a még nem javított, ismert biztonsági rések kihasználásával hozzáférhetnek a különböző rendszerelemekhez. Mindazonáltal, még ha minden javítás és enyhítés naprakészen van is tartva, a támadások egyre kifinomultabbak, és a támadók ismeretlen nulladik napi kihasználásokat használnak (McLaughlin et al., 2015b).

## **A Emberi tényező**

A hatékony biztonsági képzések és tudatosságnövelő programok hiánya az energiaszektor szervezeteiben ahhoz vezethet, hogy a kiberbiztonsági szempontok tekintetében nem eléggé képzett vagy elkötelezett a személyzet (NIST, 2014). A social engineeringet alkalmazva a fenyegető ügynökök új támadási mechanizmusokat fedeznek fel, amelyek a szervezet különböző szintjeit célozzák meg. A szakértők szerint ez az egyik leggyorsabban növekvő biztonsági probléma. A 2015-ös ukrajnai áramszünet idején a támadók kifejlesztették a *Blackenergy 3* tool malware-t, és adathalászkampányt hajtottak végre az áramszolgáltató munkatársai ellen (Styrcynski és Beach-Westmoreland, 2017).

Az elégedetlenkedő alkalmazottak vagy volt alkalmazottak, akiket nem kezelnek megfelelően, amikor elhagyják a vállalatot, további potenciális fenyegetést jelenthetnek. Részletes ismeretekkel rendelkezhetnek a rendszerekről és hozzáférhetnek a kritikus adatokhoz, ami lehetővé teszi számukra, hogy azonosítsák a gyenge belső struktúrákat és a rendszerek kompromittálásának módszereit. Továbbá a rendszerkonfigurációra vonatkozó kritikus információk akár nyilvánosan is elérhetőek lehetnek a szállítók vagy az eszköztulajdonosok weboldalain, az alkalmazottak közösségi médiaoldalain stb. keresztül. A támadók ezeket az információkat felhasználhatják a támadás megtervezéséhez.

A szakértők emellett azt is megemlítették, hogy a végfelhasználók egy másik sebezhető pontot jelentenek, mivel nem ismerik vagy nem értik az okos eszközeik alacsony

biztonságának következményeit. Egy összetettebb probléma abból fakad, hogy a végfelhasználók prosumerek, akik nem feltétlenül rendelkeznek a megfelelő szakértői ismeretekkel az elosztott energiaforrások (DER) rendszereinek (pl. intelligens inverterek) megfelelő biztonsági intézkedéseinek végrehajtásához és karbantartásához.

## Szabályzat

A biztonsági előírások és rendeletek hatékony végrehajtásának hiánya egy másik kritikus pontot jelent a CPPS számára. A szakértők úgy vélték, hogy a kötelező érvényű szabályozások hiánya, amelyek rákényszerítenék az energiarendszer-üzemeltetőket a minimálisan szükséges biztonsági szabványok végrehajtására, illetve a gyártóknak arra, hogy termékeikben biztosítsák a szükséges biztonsági követelményeket, kiteszik a rendszert a lehetséges kibertámadásoknak, például az IEC 60870-5 protokollt futtató, nem korszerűsített ICS-rendszerek elleni man-in-the-middle támadásoknak (Maynard et al., 2014).

Különböző műszaki és szervezeti szabványokat dolgoztak ki az intelligens hálózatok kiberbiztonsági követelményeinek kezelésére (ENISA, 2012; NIST, 2014). Mindazonáltal, amint azt a szakértők megállapították, ezek az esetek többségében csak ajánlások, és a minimális biztonsági szintnek való megfelelést nem kényszerítik ki szabályozásokkal. A szakértők továbbá megemlítették, hogy a hálózatüzemeltetők számára nincsenek gazdasági ösztönzők a kiberbiztonsági fejlesztésekbe való beruházásra. A biztonsági intézkedések végrehajtása érdekében a régebbi ICS-ek korszerűsítésére vonatkozó döntés a következő tervezett életciklusú berendezéscseréig elhalasztható, nemcsak a folyamatok kritikussága miatt, hanem a kapcsolódó többletköltségek miatt is. Egy másik kritikus pont, amint azt a szakértők megjegyezték, a teljes rendszer biztonságának javítását célzó hatékony koordináció hiánya.

Az ebben a szakaszban tárgyalt kritikus pontok a fent említett valamennyi kategóriához kapcsolódnak. Az összefüggés az érintett szereplők meglévő alkalmazkodási stratégiák végrehajtására való felkészültségének hiányát látják. Így növelve magának az egyes kategóriáknak a sebezhetőségi szintjét.

## Rugalmassági menedzsment stratégia

A VA feltárta a kritikus sebezhető pontokat. A biztonsági intézkedések alkalmazása esetén nagy lehetőség van egyes sebezhetőségek csökkentésére. Ezek azonban elsősorban arra összpontosítanak, hogy a rosszindulatú támadókat a rendszeren kívül próbálják tartani. Ezért az egyik legnagyobb kihívás az, hogy megtaláljuk a módját annak, hogy az ismert és ismeretlen stresszorok kezelésében kiszélesítsük a horizontot azáltal, hogy a sikeres támadások utáni helyreállítási, alkalmazkodási és tanulási mechanizmust is bevonjuk, ahelyett, hogy csak a megelőzésre és a felderítésre összpontosítanánk. Ez a célja a tanulmány második részének. Fő szempontunk az, hogy hogyan növelhető a CPPS rugalmassága. Ehhez meg kell érteni, hogy a rugalmasság több mint az azonosított

sebezhetőségek kiküszöbölése. Az alkalmazott rugalmasságkezelési megközelítés négy fázisból áll (3. ábra).

Az **előkészítési és megelőzési szakaszban** azonosítják a CPPS gyenge pontjait, és hatékony megelőző intézkedéseket kell levezetni. A hangsúly itt az ismert stresszorokra helyeződik, így az IT-OT közötti holisztikus biztonsági megközelítés (IEC, 2016), valamint az energiaközpontú kockázatelemzés és a

kezelési stratégiákra van szükség (Fischer et al., 2018). A szakértők hangsúlyozzák továbbá a végpontokon alkalmazott skálázható és rendszeresen tesztelt biztonsági intézkedések (pl. titkosítás, hitelesítés, engedélyezés, behatolásérzékelő rendszerek), a javításkezelés, a hálózat szegmentálása, valamint a hatékonyabb és elkötelezettebb biztonsági képzések és tudatosságnövelő programok fontosságát. Technológiai szempontból hasznos az adattárolásra vonatkozó további intézkedések bevezetése és a fel nem használt erőforrások - működési lazaság - megőrzése a meglepetések jobb kezelése érdekében (Fischer és Lehnhoff, 2019).

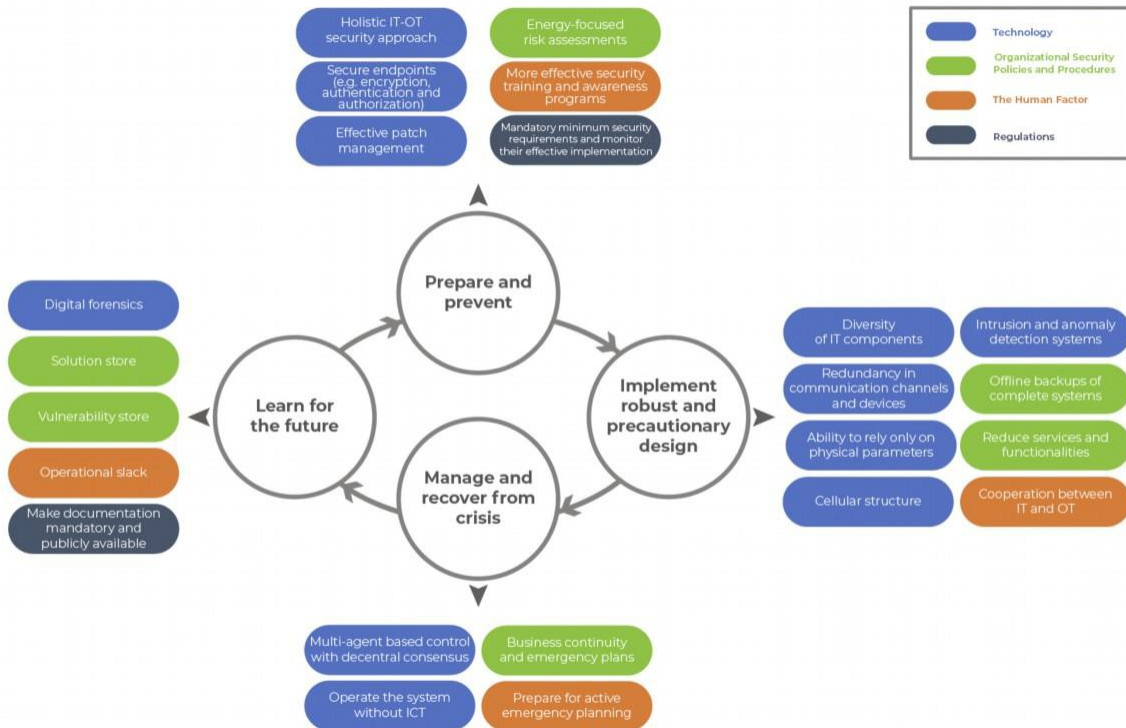
Az ellenálló képesség fokozása érdekében a kezdetektől fogva **szilárd és elővigyázatos rendszertervezést kell alkalmazni**. Ez képessé teszi a rendszert arra, hogy stressz vagy zavarok esetén is fenntartsa szolgáltatásait. A rendszernek az informatikai komponensek nagyfokú változatosságával, valamint a kommunikációs csatornák és eszközök redundanciájával kell rendelkeznie (BNetzA, 2019). A kizárólag fizikai paraméterekre való támaszkodás képességének fenntartása a működéshez, valamint a hardveralapú biztonság hasznos. Továbbá előnyösnek tűnik egy cellás struktúra megvalósítása a minimális és stabil áramellátás biztosítása érdekében a központi IKT-infrastruktúra meghibásodása esetén (VDE, 2015). A szakértők által támogatott további javaslatok a valós idejű felügyelet, a behatolás- és a rossz adatok észlelése (Iturbe et al., 2016; McCarthy et al., 2018), valamint az időszakos biztonsági mentések megvalósítása, továbbá a szolgáltatások és funkciók csökkentése az adatok, portok, könyvtárak stb. tekintetében. (Fischer és Lehnhoff, 2019).

Az ellenálló energiarendszer képes átvészelné a meghibásodásokat, hogy **kezelni tudja a válságokat és ki tudjon lábalni belőlük**. Míg a stabilitást és a biztonságot ebben a fázisban a decentralizált konszenzuskereséssel rendelkező, több ágensre épülő vezérléssel lehetne növelni (Lehnhoff és Krause, 2013), figyelmet kell fordítani arra is, hogy a rendszer IKT nélkül, azaz manuálisan is működjön, vagy legalábbis biztosítsuk a *puha leszállást*, ahogy azt a szakértők megállapították. Emellett kiemelt prioritást élvez az üzletmenet-folytonossági és vészhelyzeti tervek biztosítása regionális és helyi szinten, pl. legalább a közterületeken/épületekben és azok környékén lévő *ellátószigeteken* keresztül, valamint a reális kibertámadásokon alapuló aktív vészhelyzeti tervezésre és gyakorlatokra való felkészülés (Arghandeh et al., 2016).

A múltbeli és elkerült katasztrófákat a negyedik fázisban fel kell használni a **jövőre vonatkozó tanulságok levonására** a rendszer alkalmazkodóképességének javítása érdekében. Ebben az értelemben a digitális törvényszéki vizsgálat lehetővé tenné az incidensek és a majdnem incidensek alapos kivizsgálását és a tanulságok meghatározását. Ennek magában kellene foglalnia a kudarcokhoz vezető gyengeségek dokumentálását (*sebezhetőségi tár*) (Gößling-Reisemann, 2016). Ezenkívül a múltban a válságokat

elkerülhetővé tevő vagy a helyreállítást fokozó erősségeket is érdemes azonosítani, mivel ezek képezik a stratégiák és vészhelyzeti forgatókönyvek tervezésének alapját (*Solution store*) (Gößling-Reisemann, 2016). Ennek a dokumentációnak kötelezőnek és nyilvánosan hozzáférhetőnek kell lennie.

A 4. ábra az ellenálló képességet növelő intézkedések és elemek összefoglalóját mutatja az ellenálló képességet növelő megközelítés egyes szakaszaihoz.



4. ábra: Az ellenálló képességet fokozó intézkedések és elemek kiválasztása, kategóriák szerint rendezve: Technológia (kék), szervezeti biztonsági politikák és eljárások (zöld), emberi tényező (narancssárga) és szabályozások (szürke), a rugalmas irányítási megközelítés fázisai szerint. Forrás: Az Európai Bizottság a következő táblázatot állította össze A szerzők saját összeállítása

## Következtetések

Ebben a tanulmányban azonosították a CPPS sérülékenységéhez hozzájáruló kritikus tulajdonságokat, szerkezeteket és elemeket. Egyrészt a nem biztonságos kommunikáció vagy a nem biztonságos végpontok, különösen az ügyfél telephelyén, az eszközök gyenge biztonsági jellemzői miatt nagyfokú sebezhetőséget eredményeztek. Másrészt a social engineering gyorsan növekvő biztonsági probléma, amely lehetővé teszi a fenyegető ügynökök számára, hogy kihasználják a minden szervezetben jelen lévő egyik gyenge pontot: az emberi tényezőt. Annak ellenére, hogy léteznek olyan alkalmazkodási mechanizmusok, amelyek minimalizálhatják a hatást, kiderült, hogy ezek végrehajtását akadályozhatja a szabályok érvényesítésének hiánya vagy az érintett szereplők felkészületlensége ezen intézkedések végrehajtására. A kiberbiztonsági kihívások kezeléséhez a fizikai, kiber- és társadalmi szempontokat figyelembe vevő integrált értékelésre van szükség. A cél nem csupán az, hogy a támadókat a rendszeren kívül tartsuk, hanem az, hogy a rendszert úgy tervezzük meg, hogy az képes legyen átalakulni és

alkalmazkodni, hogy bármilyen stresszorzarral megbirkózzon. Más szóval, olyan ellenálló  
képesség-kezelési stratégiára van szükség, amely figyelembe veszi, hogy az ellenálló  
képesség több, mint az azonosított sebezhetőségek kiküszöbölése. Ez a cikk

az ellenálló képességet fokozó intézkedéseket a rugalmasságkezelési ciklus négy fázisához rendelték. Az egyik fontos intézkedés a megfelelő kiberbiztonsági szabályozási keret létrehozása és hatékony végrehajtásának nyomon követése. Ami a rendszerarchitektúrát illeti, a cellaszerkezet és a fizikai biztonsági mentés sikeres támadások esetén ellenálló képességet teremtene. Arra a következtetésre jutottunk, hogy a rugalmassági elvek/elemek bevezetése a rendszerbe és a rugalmassági menedzsment megközelítés alkalmazása megfelelő módja annak, hogy a rendszereket felkészítsük a váratlan eseményekre.

## 3 Metodológia

A *Strom-Resilienz* kutatási projekt fent említett munkacsomagjainak fő célkitűzése az volt, hogy azonosítsák, milyen további sebezhetőségek merülhetnek fel a villamosenergia-rendszerek digitalizálásával, és milyen stratégiák szükségesek a villamosenergia-rendszerek ellenálló képességének növeléséhez, hogy a rendszer elsődleges funkciói még stresszhelyzetben is fennmaradjanak.

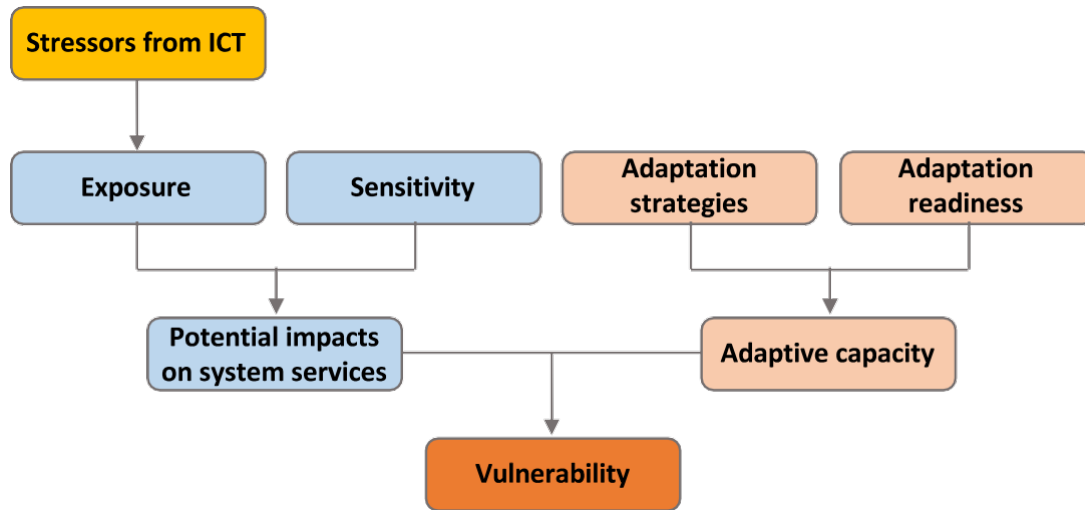
E kérdések megválaszolása érdekében a tanulmányt két részből állt. Először egy sebezhetőségi vizsgálatot végeztünk, hogy azonosítsuk azokat a kritikus tulajdonságokat, struktúrákat és elemeket, amelyek a rendszert sebezhetővé teszik a kibertámadásokkal szemben. E célból interdiszciplináris megközelítést választottak, amelyben az energiaágazat érdekelt felei és az IKT-megoldások szolgáltatói interjúk és műhelybeszélgetések révén vettek részt. Másodsor, a rugalmassági menedzsment megközelítés alkalmazásával ellenálló stratégiát dolgoztak ki annak meghatározására, hogy a kiber-fizikai rendszerek hogyan készülhetnek fel jobban bármilyen stresszorra. A 3.1. és a 3.2. szakasz az egyes részekben alkalmazott módszereket ismerteti.

### 3.1 Sebezhetőségi értékelés Módszertan

Ebben a tanulmányban két sérülékenységetértékelési módszert, nevezetesen az északnyugat-németországi energiarendszerek éghajlatváltozással kapcsolatos sérülékenysége vizsgálatán végzett eseményalapú sérülékenységetértékelést (EVA) és strukturális sérülékenységetértékelést (SVA) (Göbbling-Reisemann et al., 2013; von Gleich et al., 2010) használták referenciaként az értékeléshez. A kiválasztott módszertani keret a sebezhetőséget nemcsak a rendszer kitétségének, a rendszer külső/belső stresszorokkal szembeni érzékenységének és az energiarendszer szolgáltatásaira gyakorolt lehetséges hatásoknak a függvényeként veszi figyelembe, hanem a rendszer ezekkel való megbirkózási képességét is. Ez az alkalmazkodóképességként azonosított képesség a meglévő vagy tervezett alkalmazkodási stratégiákon és az érintett szereplők hajlandóságán alapul, hogy ezeket az intézkedéseket végrehajtsák (Göbbling-Reisemann et al., 2013). Az 1. és a 2. ábra az EVA és az SVA módszertanok sémáját mutatja be.

Érdemes megemlíteni, hogy az IT-biztonság területén a "sebezhetőség" kifejezés általában egy információs rendszer, a rendszerbiztonsági eljárások, a belső ellenőrzések vagy a végrehajtás olyan gyengeségére utal, amelyet egy fenyegetésforrás kihasználhat vagy kiválthat (NIST, 2014). Ez a meghatározás eltér a mi VA-módszereinkben használt meghatározástól, mivel csak a rendszer stresszornak való kitétségét jelenti, az alkalmazkodási intézkedések figyelembevétele nélkül.

## Event-based vulnerability assessment



1. ábra. Az eseményalapú sebezhetőségi értékelés (EVA) módszertanának vázlatos ábrázolása. Saját ábrázolás (Göbbling-Reisemann et al., 2013; von Gleich et al., 2010) alapján.

2. ábra. A strukturális sérülékenységvizsgálat (SVA) módszertanának vázlatos ábrázolása. Saját ábrázolás (Göbbling-Reisemann et al., 2013; von Gleich et al., 2010) alapján.

A potenciális hatásokat a rendszer szolgáltatásaira gyakorolt hatásuk alapján értékelték, amelyeket mind az energia-, mind az IKT-infrastruktúrára vonatkozó konkrét paraméterek alapján határoztak meg (lásd az 1. táblázatot).

1. táblázat. A kiber-fizikai villamosenergia-rendszer rendszerszolgáltatásainak meghatározása, amely figyelembe veszi a villamosenergia-infrastruktúra és az IKT-infrastruktúra kritériumait. Forrás: A szerzők saját összeállítása (Gößling-Reisemann et al., 2013; von Gleich et al., 2010) alapján.

Energetikai infrastruktúra	
<b>Mennyiségi kritériumok:</b>	
Energiaellátás	
<b>Minőségi kritériumok</b>	
<b><u>Közvetlen műszaki paraméterek</u></b>	<b><u>Közvetett paraméterek</u></b>
<ul style="list-style-type: none"> <li>• Energiaminőség:                             <ul style="list-style-type: none"> <li>▪ Feszültség szint (pl. 400 V +/-10%)</li> <li>▪ Frekvencia (pl. 50 +/- 0,2 Hz)</li> </ul> </li> <li>• Megbízhatósági mutatók: pl.,                             <ul style="list-style-type: none"> <li>▪ SAIDI (rendszer átlagos megszakítási időtartam indexe)</li> </ul> </li> </ul>	<ul style="list-style-type: none"> <li>• Környezeti hatások: pl,                             <ul style="list-style-type: none"> <li>▪ CO2-kibocsátás</li> <li>▪ Föld / erőforrások használata</li> <li>▪ Hulladéktermelés</li> </ul> </li> <li>• Gazdasági hatások: pl,                             <ul style="list-style-type: none"> <li>▪ Költségek/piaci árhatások</li> <li>▪ Versenyképesség</li> </ul> </li> <li>• Társadalmi hatások: pl,                             <ul style="list-style-type: none"> <li>▪ Az ügyfelek magánéletének veszélyeztetése</li> <li>▪ A technológia elfogadottságának veszélyeztetése</li> </ul> </li> </ul>
<b>Információs és kommunikációs infrastruktúra</b>	
Tranzit vagy nyugalmi állapotban lévő adatok, mint például: <ul style="list-style-type: none"> <li>• Ügyfél azonosító és helymeghatározó adatok</li> <li>• Mérőadatok</li> <li>• Vezérlőparancsok</li> <li>• Konfigurációs adatok</li> </ul>	<ul style="list-style-type: none"> <li>• Idő, óra beállítások</li> <li>• Hozzáférés-szabályozás</li> <li>• Firmware, szoftver és illesztőprogramok</li> <li>• Tarifális adatok</li> <li>• ...</li> </ul>
<b>Biztonsági követelmények</b>	
<ul style="list-style-type: none"> <li>• Bizalmasság</li> <li>• Integritás</li> </ul>	<ul style="list-style-type: none"> <li>• Elérhetőség</li> <li>• Visszautasíthatatlanság</li> </ul>

A villamosenergia-infrastruktúrát illetően a mennyiségi kritériumokat a rendszer azon képessége határozta meg, hogy képes-e ellátni a csatlakoztatott terhelést (Gößling-

*vizsgálat eredményei.*

Reisemann et al., 2013). A minőségi kritériumokat közvetlen műszaki paraméterek, mint például: a teljesítményminőség vagy a megbízhatósági mutatók, valamint közvetett paraméterek, mint például: környezeti hatások, gazdasági hatások (pl. az alábbiakra gyakorolt hatások

az energiapiac, számlázási pontatlanság) és társadalmi hatások (pl. a technológia elfogadottságának veszélyeztetése vagy az ügyfelek magánéletének megsértése).

Az IKT-infrastruktúra tekintetében a megközelítés figyelembe veszi a biztonsági követelményekre gyakorolt hatást, azaz az átmenő vagy nyugvó adatok (pl. vezérlőparancsok, konfigurációs adatok, firmware, szoftver, mérőadatok stb.) titkosságát, integritását, rendelkezésre állását és letagadhatatlanságát. Az alábbiakban a biztonsági követelmények rövid leírása következik (Cleveland, 2016):

- **Bizalmasság:** az információkhoz való jogosulatlan hozzáférés megakadályozása.
- **Integritás:** az információ jogosulatlan módosításának vagy ellopásának megakadályozása.
- **Elérhetőség:** a szolgáltatásmegtagadás megakadályozása és az információkhoz való engedélyezett hozzáférés biztosítása.
- **Tagadásmentesség:** egy megtörtént cselekmény tagadásának vagy egy meg nem történt cselekményre vonatkozó állításnak a megakadályozása.

### 3.1.1 Sebezhetőségi értékelés minősítés

A szakértők véleményét (lásd a 3.1.3. és 3.1.4. szakaszt), a vonatkozó szakirodalmat és saját megítélésünket ötvözve a rendszer szolgáltatásaira gyakorolt lehetséges hatásokat az alábbiakban felsoroltak szerint minősítettük, a stresszoroknak és a strukturális gyengeségeknek a rendszer szolgáltatásainak minőségi és mennyiségi kritériumaira gyakorolt hatása szerint:

- **Magas**, ha az energiaellátás mennyiségi kritériumait jelentősen befolyásolná,
- **Közepes**, ha a mennyiségi kritériumokat nem érinti lényegesen, de ha a veszélyeztetett biztonsági követelmény közvetlen hatással lehet a mennyiségi kritériumokra, vagy ha a minőségi kritérium legalább egy paraméterét lényegesen érinti,
- **Alacsony**, ha sem az energiaellátás mennyiségi, sem minőségi kritériumait nem érintené jelentősen, vagy ha a veszélyeztetett biztonsági követelmény csak közvetett hatással lehet a minőségi vagy mennyiségi kritériumokra.

Az alkalmazkodóképesség meghatározásához figyelembe vették a szakértők és a szakirodalom által adott információkat a meglévő vagy tervezett alkalmazkodási mechanizmusokról, valamint az érintett szereplők hajlandóságáról azok végrehajtására. Ezeket minőségileg is értékelték:

- **Magas**, ha mind a lehetséges hatások elkerülésére szolgáló alkalmazkodási mechanizmus, mind az alkalmazkodási hajlandóság adott.

- **Közepes**, ha vagy a lehetséges hatások elkerülésére szolgáló alkalmazkodási mechanizmus vagy az alkalmazkodási hajlandóság adott.

- **Alacsony**, ha sem a potenciális hatások elkerülésére szolgáló alkalmazkodási mechanizmus, sem az alkalmazkodási hajlandóság nem adott.

Következésképpen a sebezhetőségi szintet a lehetséges hatások és az alkalmazkodóképesség kombinációjának eredményeként értékelték a 3. ábrán látható mátrix szerint. A magas alkalmazkodóképesség megakadályozza vagy mérsékli a potenciális hatást, ami a potenciális hatás szintje alatt egy szinttel alacsonyabb sebezhetőségi szintet eredményez, kivéve azt az esetet, amikor a potenciális hatás már alacsony. A közepes alkalmazkodóképesség nem változtatja meg a potenciális hatást. Az alacsony alkalmazkodóképesség azonban egy szinttel a potenciális hatásszint fölé emeli a sebezhetőséget, azon hipotézisek alapján, hogy ilyen körülmények között a gyenge stresszorok hosszú ideig észrevétlenek (és megválaszolatlanok) maradhatnak, ami a rendszer szolgáltatására gyakorolt halmozódó hatásokhoz vezet (Gößling- Reisemann et al., 2013).

Az alkalmazkodóképesség javítását célzó intézkedések nagy lehetőséget rejtenek magukban nemcsak a sebezhetőség csökkentésére, hanem a rendszerek ellenálló képességének növelésére is. Ezért a sebezhetőségi értékelés eredményeit kiindulópontként használták az ellenálló képességi stratégia meghatározásához.

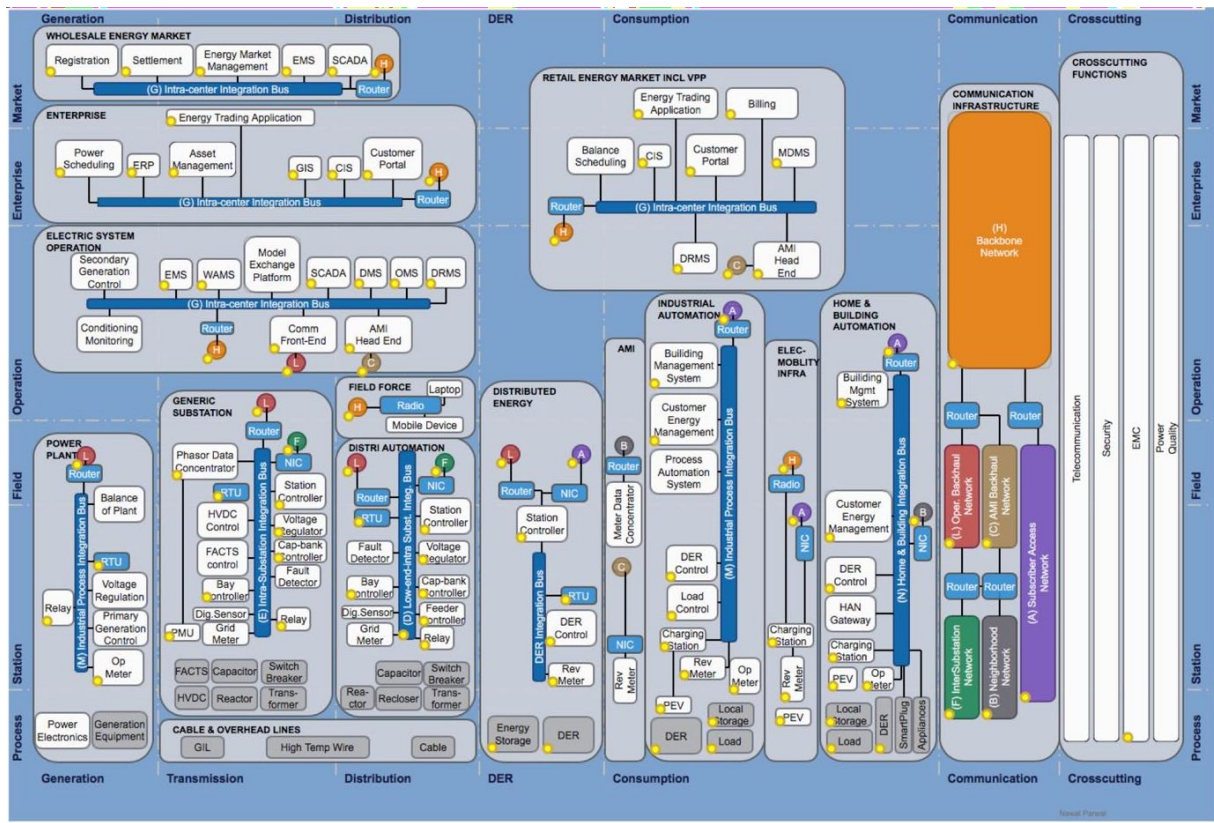
### Sebezhetőségi értékelési mátrix

P o t e n c i á l i s h a t á s o k	Magas	H	H	M
	Közepes	H	M	L
	Alacsony	M	L	L
		Alacsony	Közepes	Magas
		Alkalmazkodóképesség		

3. ábra A sebezhetőségi értékelési mátrix, amely figyelembe veszi a rendszer szolgáltatásaira és az alkalmazkodóképességre gyakorolt lehetséges hatások szintjét. (H: magas, M: közepes, L: alacsony). Forrás: A szerzők saját összeállítása (Gößling- Reisemann et al., 2013; von Gleich et al., 2010) alapján.

### 3.1.2 Referenciaarchitektúra modell

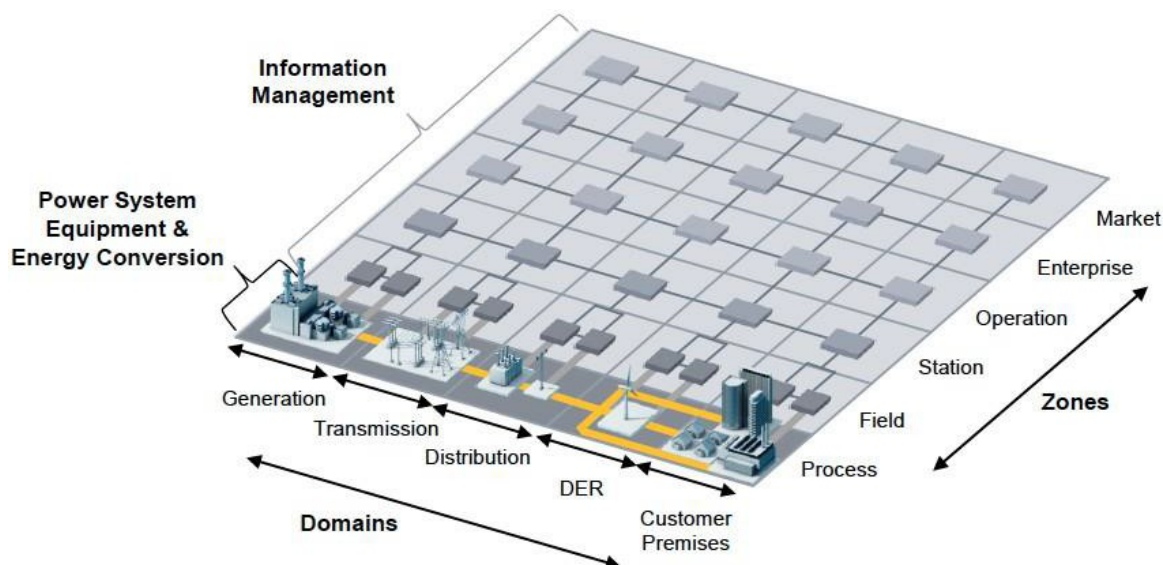
Ez a tanulmány a német és az európai villamosenergia-rendszerre összpontosított, és a teljes elektromos energiaátalakítási láncot lefedte. Referencia-architektúramodellként a Nemzetközi Elektrotechnikai Bizottság (IEC) által a Smart Grid Standards Mapping Toolban (IEC, 2020) használt Smart Grid Architecture Model (SGAM) (CEN-CENELEC-ETSI Smart Grid Coordination Group, 2012) komponensrétegét használták. A 4. ábra mutatja a VA-hoz használt referenciaarchitektúra-modell, az 5. ábra pedig az SGAM-sík egyszerűsített nézetét.



4. ábra A sebezhetőségi vizsgálatához használt referenciaarchitektúra-modell. Forrás: (IEC, 2020)

Az SGAM modell öt egységes rétegből áll, amelyek az üzleti célokat és folyamatokat, funkciókat, információs modelleket, kommunikációs protokollokat és komponenseket képviselik. Az egyes rétegek az intelligens hálózat síkját fedik le, amelyet az intelligens hálózati tartományok és zónák fednek le. Az SGAM-modell nemcsak az elektromos hálózat megvalósításainak jelenlegi állapotát mutatja be, hanem a jövőbeli intelligens hálózati forgatókönyvek felé történő fejlődést is, az egyetemesség, lokalizáció, konzisztencia, rugalmasság és interoperabilitás elveinek támogatásával (CEN- CENELEC-ETSI Smart Grid Coordination Group, 2012). Ezek a jellemzők lehetővé tették számunkra, hogy ezt a referenciaarchitektúra-modell használjuk a szakértői interjúk és a műhelytalálkozók anyagaként, hogy megvitassuk az energiarendszerek kiberbiztonságát az intelligens hálózat

funkcióinak teljes körű megvalósítását feltételezve.



5. ábra Smart Grid sík. Forrás: (CEN-CENELEC-ETSI Intelligens Hálózat Koordinációs Csoport, 2012)

Ez a tanulmány az SGAM architektúra szerint a különböző intelligens hálózati területekre terjedt ki: termelés, átvitel, elosztás, elosztott energiaforrások (DER), fogyasztói helyiségek, valamint az intelligens hálózati zónák: folyamat, mező, állomás, üzemeltetés, vállalkozás és piac (lásd az 5. ábrát). Az alábbiakban az egyes SGAM-tartományok, -zónák és -rétegek áttekintése következik (CEN-CENELEC-ETSI Smart Grid Coordination Group, 2012):

**SGAM tartományok:**

<b>Tömeges generálás</b>	A villamos energia nagy mennyiségben történő előállítása, például fosszilis, nukleáris és vízerőművek, tengeri szélenergiaerőművek, nagyméretű fotovoltaikus (PV) erőművek által - jellemzően az átviteli rendszerhez csatlakoztatva.
<b>Átvitel</b>	A villamos energiát nagy távolságokra szállító infrastruktúra és szervezet képviselője
<b>Forgalmazás</b>	A villamos energiát a fogyasztókhoz eljuttató infrastruktúra és szervezet képviselője
<b>DER</b>	A közüzemi elosztóhálózathoz közvetlenül csatlakozó , kisléptékű, elosztott elektromos erőforrásokat képviselő , kisléptékű, közvetlenül a közüzemi elosztóhálózathoz csatlakoztatott

**energiatermelési technológiák (jellemzően 3 kW-os  
tartományban)**

	10.000 kW-ig). Ezeket az elosztott elektromos erőforrásokat a DSO közvetlenül vezérelheti.
<b>Ügyfélei telephelyei</b>	Mindkettő - a villamos energia végfelhasználói és a villamosenergia-termelők - befogadása. A telephelyek közé tartoznak az ipari, kereskedelmi és otthoni létesítmények (pl. vegyi üzemek, repülőterek, kikötők, bevásárlóközpontok, otthonok). A termelés pl. fotovoltaiikus termelés, elektromos járművek tárolása, akkumulátorok, mikroturbinák formájában is megtalálható.

**SGAM-zónák:**

<b>Folyamat</b>	Beleértve mind a villamosenergia-rendszer elsődleges berendezéseit (pl. generátorok, transzformátorok, megszakítók, felsővezetékek, kábelek, elektromos fogyasztók...), mind a fizikai energiaátalakítást (villamos energia, napenergia, hő, víz, szél...).
<b>Terep</b>	Beleértve a villamosenergia-rendszer folyamatainak védelmére, vezérlésére és felügyeletére szolgáló berendezéseket, pl. védelmi relék, öblözetvezérlő, bármilyen intelligens elektronikus eszköz (IED), amelyek a villamosenergia-rendszerből származó feldolgozott adatokat veszik fel és használják fel.
<b>Állomás</b>	A mezők aggregációs szintjének megjelenítése, pl. az adatkoncentráció, az állomás-automatizálás...
<b>Művelet</b>	A villamosenergia-rendszerek vezérlési műveleteinek tárolása az adott területen, pl. elosztásirányítási rendszerek (DMS), energiagazdálkodási rendszerek (EMS) a termelési és átviteli rendszerekben, mikrohálózat-irányítási rendszerek, virtuális erőmű-irányítási rendszerek (több DER aggregálása), elektromos járműpark (EV) töltésirányítási rendszerek.

**Vállalat**

Magában foglalja a kereskedelmi és szervezeti folyamatokat, szolgáltatásokat és infrastruktúrákat a vállalkozások számára (közművek, szolgáltatók,

	energiakereskedők ...), pl. eszközgazdálkodás, személyzeti képzés, ügyfélkapcsolat-kezelés, számlázás és beszerzés.
<b>Piac</b>	Az energiaátalakítási lánc mentén lehetséges piaci műveletek tükrözése, pl. energiakereskedelem, tömegpiac, kiskereskedelmi piac...

### **SGAM rétegek**

<b>Üzleti</b>	Olyan üzleti eseteket képvisel, amelyek leírják és igazolják az érzékelt üzleti igényt.
<b>Funkció</b>	A fizikai megvalósításoktól független logikai funkciókat vagy szolgáltatásokat tartalmazó felhasználási eseteket képvisel.
<b>Információ</b>	Információs objektumok vagy adatmodellek, amelyek a funkciók teljesítéséhez és a kommunikáció révén történő cseréhez szükségesek.
<b>Kommunikáció</b>	A komponensek közötti információcsere protokolljait és mechanizmusait jelenti.
<b>Komponens</b>	A funkciókat, információkat és kommunikációs eszközöket befogadó fizikai alkatrészeket jelenti.

### 3.1.3 Szakértői műhelyek

2016 júniusában és 2017 márciusában két munkaértekezletet tartottak az IKT- és az energiaágazat szakértőinek részvételével, mind az ipar, mind a tudományos élet képviselői, hogy megvitassák a kiber-fizikai energiarendszerek sebezhetőségét és ellenálló képességét.

#### 3.1.3.1 Első szakértői workshop

Az első workshop során a fent leírt VA módszertani megközelítést alkalmazták egy korlátozott változatban. Ehhez a gyakorlathoz a kiberbiztonsági hibaforgatókönyvek egy sorát dolgozták ki, amelyeket a

A vita kiindulópontjaként az amerikai Nemzeti Villamosenergia-ipari Szektor Kiberbiztonsági Szervezetének (NESCOR) 1. technikai munkacsoportja (NESCOR, 2015) szolgált. A

Az említett dokumentum minden egyes hibaforgatókönyv esetében ismerteti a vonatkozó sebezhetőségeket<sup>3</sup>, a hatásokat és a csökkentési stratégiákat. A lehetséges hatások között szerepel az áramkimaradás, a berendezések károsodása, emberi áldozatok, bevételkiesés, az ügyfelek magánéletének megsértése és a közbizalom elvesztése.

A workshopon kis munkacsoportokat szerveztek a villamosenergia-ágazat különböző területei szerint. Minden csoport legalább egy NESCOR meghibásodási forgatókönyvet vitatott meg annak érdekében, hogy azonosítsák a stresszorokat, a kitétséget és a rendszer érzékenységét az előre leírt feltételek mellett. Megvitatták továbbá e feltételek gyakorlati megvalósíthatóságát is. A csoportok megvitatták továbbá a jelenlegi alkalmazkodási mechanizmusokat a forgatókönyvek bekövetkezésének megelőzésére és/vagy a szolgáltatás helyreállítására a meghibásodás után. Az elemzett NESCOR-forgatókönyvek a következők voltak:

- *"A hálózat instabilitásának fenyegető ügynöki okai a rendszerüzemeltetési központ és az üzem közötti dedikált adat- és hangvonalak ellenőrzésén keresztül (GEN.10)"*
- *"A kapcsolt kondenzátorbankok manipulálása a teljesítményminőség romlása érdekében (DGM.10)"*
- *"DER-rendszerek leállítása hamisított SCADA vezérlőparancsokkal (DER.14)"*
- *"Tömegmérő távkapcsolása jogosult személy által (AMI.1)"*
- *"A jogosulatlan árinformáció hatással van a közüzemi bevételekre (AMI.10)"*

A munkaértekezlet eredményei értékes betekintést nyújtottak a főbb kiberbiztonsági kihívásokról, amelyekkel a villamosenergia-rendszer különböző területein az IKT-rendszerek megnövekedett összetettsége miatt foglalkozni kell.

### 3.1.3.2 Második szakértői workshopok

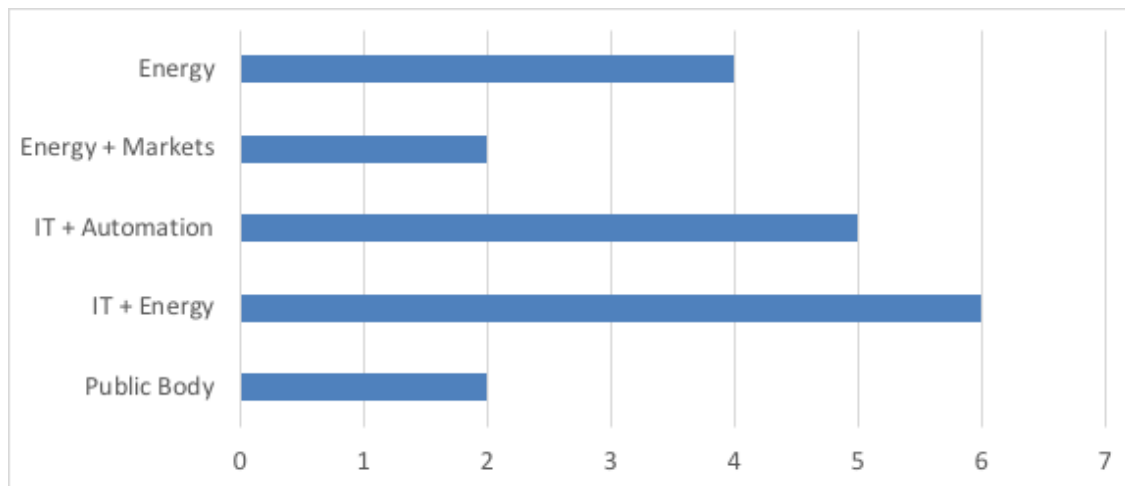
A második szakértői munkaértekezleten bemutatták a VA előzetes eredményeit, és megvitatták azokat a résztvevőkkel. A megbeszélések eredményei alapján konkretizálták a VA-t és az ellenálló képességi stratégiát. A fő hangsúlyt az energiarendszer szemcsézettségére helyezték, de a rugalmasságot növelő műszaki, szervezeti és szabályozási intézkedések is megvitatásra kerültek.

### 3.1.4 Szakértői interjúk

Annak érdekében, hogy a sebezhetőségi értékeléshez alaposabb ismeretekre tegyenek szert, a tanulmányhoz közel 100 IKT- és energiaügyi szakértővel vették fel a kapcsolatot, akik közül 19-en vettek részt személyes vagy telefonos félig strukturált interjúban 2016 októbertől és 2017 márciusa között. A megkérdezetteket szakterületük szerint öt kategóriába soroltuk a 6. ábrán felsoroltak szerint.

<sup>3</sup> A NESCOR-dokumentumban szereplő *sebezhetőség* fogalmát módszertanunkban *gyengeségként/kitettségként* értelmezzük.

Az interjúk során a szakértőket a jelenlegi és a tervezett villamosenergia-rendszerek kibersebezhetőségéről, a villamosenergia-rendszerek szolgáltatásaira gyakorolt lehetséges hatásokról, valamint az ezekkel való megbirkózásra, alkalmazkodásra vagy helyreállításra irányuló lehetséges alkalmazkodási stratégiákról kérdezték. Az interjúk során használt kérdések listája az A. függelékben található: Interjúelemzési módszertan.



6. ábra Kategóriák a megkérdezettek szakterülete és a résztvevők száma szerint

### 3.1.5 Minőségi tartalom elemzés

A szakértői műhelybeszélgetések és interjúk során elhangzott állításokat egy átfogó kvalitatív tartalomelemzési módszertan segítségével értékeltük (Mayring, 2014), és a VA számára bemeneti információként használtuk fel.

Mivel a megkérdezett szakértők közül néhányan névtelenséget kértek, az interjúk elemzése során úgy döntöttek, hogy az összes interjúalany esetében a "X interjúalany" jelzõt használják, ahol az X az interjú időpontjának megfelelő sorszámot jelenti. A következő szakaszokban ezt az azonosítót fogjuk használni az interjúalanyok nyilatkozataira való hivatkozáshoz.

A kvalitatív tartalomelemzés részletesebb információi az A. függelékben található: Interjúelemzési módszertan.

## 3.2 Rugalmassági menedzsment Megközelítés

Az elmúlt évtizedben a reziliencia fogalma egyre népszerűbbé vált, és a kutatói közösség többféle definíciót használ (lásd (Jesse et al., 2019)). Mi a rezilienciát úgy írjuk le, mint egy (társadalmi-technikai) rendszer azon képességét, hogy stressz és turbulens körülmények között is képes fenntartani szolgáltatásait (Brand et al., 2017; von Gleich et al., 2010). E definíció használatának előnye, hogy a rendszer szolgáltatásaira összpontosít, amelyeket az érintettekkel és/vagy felhasználókkal együtt kell felvázolni. Ily módon a rendszer változásai

## és fejlődése lehetséges, amelyek központi

az átmenetek szempontjai. A hangsúly az összekapcsoltság és az egymásrautaltság összetett jellegén, valamint a rendszer azon képességén van, hogy fenntartsa szolgáltatásait.

A reziliencia értelmezhető úgy is, mint a rendszer azon képessége, hogy felkészüljön, megbirkózzon és felépüljön bármilyen stresszorzal, miközben fenntartja a rendszer szolgáltatásait anélkül, hogy előzetesen feltétlenül ismernie kellene az esemény vagy a stresszor sajátosságait (Göbbling-Reisemann, 2016). Ezért meg kell különböztetni a stresszorok bizonyos jellemzőit és azokat a képességeket, amelyekkel egy rugalmas rendszernek rendelkeznie kell ahhoz, hogy kezelni tudja azokat. A stresszorokat dinamikájuk és a természetükre vonatkozó ismeretek állapota alapján az alábbiak szerint jellemezhetjük (Göbbling-Reisemann, 2016):

- **Ismert/várható:** olyan stresszorok, amelyeket a rendszer a múltban már megtapasztalt, és amelyek jövőbeli előfordulását előre jelzik.
- **Ismeretlen/váratlan:** olyan stresszorok, amelyeknek a rendszer még soha vagy csak nagyon ritkán volt kitéve, és amelyek jövőbeli előfordulására vonatkozóan nem léteznek előrejelzések.
- **Fokozatos/kúszó:** lassan és esetleg egy ideig észrevétlenül kialakuló stresszorok.
- **Hirtelen/ hirtelen:** hirtelen vagy hirtelen, figyelmeztetés nélkül kialakuló stresszorok.

Egy olyan rendszernek, amely képes felkészülni, megbirkózni a stresszorokkal, és a fent leírt jellemzők tetszőleges kombinációjával felépülni belőlük, a képességek változatos készletére van szüksége, amelyek robusztusság, alkalmazkodóképesség, innovációs képesség és improvizációs képesség néven foglalhatók össze (lásd a 7. ábrát).

Stresszor	Known / expected	Unknown / unexpected
Gradual / creeping	Adaptive Capacity	Innovation capacity
Abrupt / sudden	Robustness	Improvisation capacity

7. ábra A rendszer különböző stresszorokra való felkészültségéhez szükséges képességek hozzárendelése. A stresszorok a bekövetkezés ideje és a tudatosság mértéke szerint vannak megkülönböztetve. Forrás: (Göbbling-Reisemann, 2016)

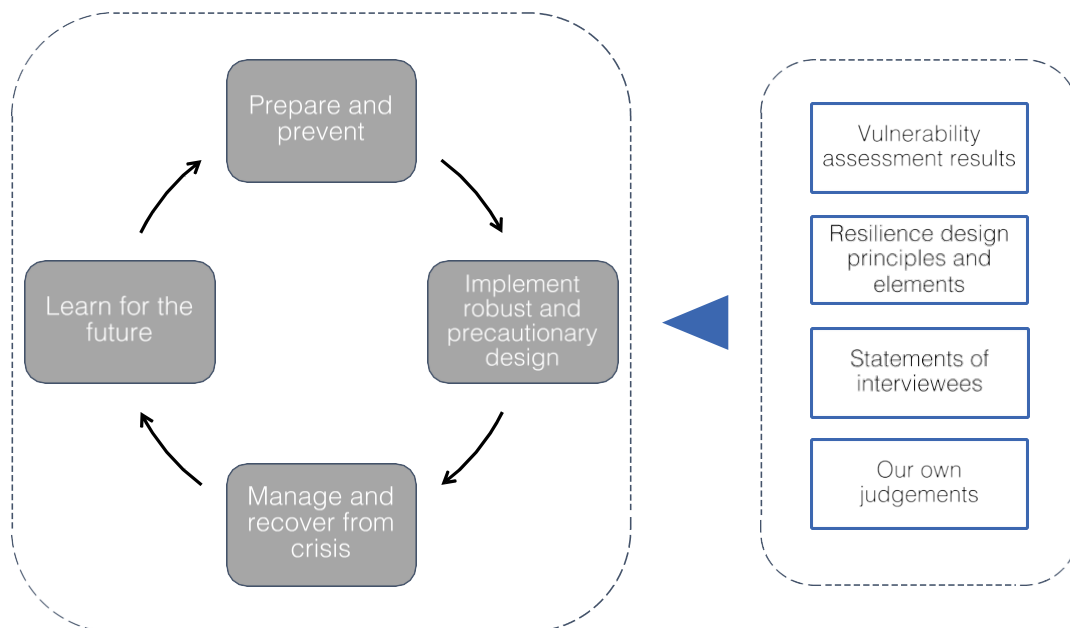
Ha a stresszorok fokozatosan alakulnak ki, és már ismertek a rendszer számára, vagy a közeljövőben várhatóan bekövetkeznek, akkor a meglévő struktúrák, összetevők és szervezetek kiigazítását lehet kezdeményezni annak érdekében, hogy jobban

megbirkózzanak a stresszorral, és jobban kiheverjék annak előfordulását. A másik véglet, amikor a stresszor ismeretlen és hirtelen alakul ki, a rendszer szereplői nem fognak

lesz idejük innovatív megoldásokat találni vagy ellenállást kialakítani, így improvizálniuk kell (Gößling-Reisemann, 2016).

A tanulmány második részének középpontjában az állt, hogy megvizsgálja, hogyan fejleszthető a rugalmasság a CPPS-en és a kapcsolódó szervezeteken belül. Ehhez a reziliencia fenti definícióját használtuk vezérelvként, és a (Acatech et al., 2017; Goessling-Reisemann és Thier, 2019) által leírt rezilienciamenedzsment megközelítést vettük alapul.

Ez a megközelítés négy fázisból áll: (1) Felkészülés és megelőzés, (2) Robusztus és elővigyázatos tervezés végrehajtása, (3) Válságkezelés és válságból való kilábalás, valamint (4) Tanulás a jövőre nézve, amelyeket a következő szakaszban röviden ismertetünk. Az egyes lépésekhez javasolt intézkedéseket a VA eredményei, a (Brand et al., 2017; Goessling-Reisemann és Thier, 2019), a megkérdezett szakértők nyilatkozatai és saját megítélésünk alapján dolgoztuk ki (8. ábra).



8. ábra A rugalmas irányítási megközelítés sémája, amely a négy fázist és az egyes fázisokhoz javasolt intézkedések meghatározásának forrásait mutatja. Forrás: Acatech et al., 2017; Goessling- Reisemann és Thier, 2019) alapján készült saját ábrázolás.

### 3.2.1 Felkészülés és Megelőzés

**Az előkészítési és megelőzési** szakaszban azonosítani kell a rendszer gyenge pontjait, és az eredményekből hatékony megelőző intézkedéseket és iránymutatásokat kell levezetni (Acatech et al., 2017). A korábbi válságokat és majdnem baleseteket átláthatóan dokumentálni és vizsgálni kell, hogy megismerjük az azokat kiváltó stresszorokat és azt a kontextust, amelyben bekövetkeztek, illetve amelyben elkerültek (Gößling-Reisemann, 2016). A további elemzésnek azokra a stresszorokra kell irányulnia, amelyek még nem fordultak elő, de valószínűleg előfordulhatnak a következőkben

a közeljövőben, pl. a trendek extrapolációjából ismert. Ezen túlmenően új veszélyek származhatnak társadalmi folyamatokból is, például: bizonyos technológiák növekvő elutasítása vagy az energetikai átmenetekkel kapcsolatos igazságtalan költség-haszon megoszlás, ami tiltakozásokhoz és a szükséges rendszerváltozások késedelméhez vagy leállításához vezet. Az újonnan kialakuló stresszorokat a sebezhetőségi értékelési módszerekkel lehet elemezni. Az értékelések eredményeit ezután az energiarendszer-elemek tervezési paramétereinek kiigazítására (technológiai szint), a kapcsolt infrastruktúrák tesztelési forgatókönyveinek és tervezési iránymutatásainak kidolgozására (rendszer szint), valamint a technológiai változásokra adott társadalmi hatások és válaszok nyomon követésére kell felhasználni, a kormányzási folyamatokra való visszacsatolással (kormányzási szint) (Gößling-Reisemann, 2016).

### 3.2.2 Robusztus és elővigyázatos rendszer megvalósítása tervezés

Az ellenálló képesség kiépítésének második szakasza a **robosztus és elővigyázatos rendszertervezés** megvalósítására összpontosít, hogy ellenálljon bármilyen stresszornak. Az ellenálló rendszerek fent részletezett jellemző képességeivel összhangban az ellenálló energiarendszerek központi tervezési elemei közé kell tartoznia a robusztusságnak, az alkalmazkodóképességnek, az innovációs képességnek és az improvizációs képességnek. A komponensek és rendszerek tervezési szintjén az ellenálló képességet növelő képességek először az azonosított sérülékeny elemek megerősítésével (lásd az előkészítés és megelőzés szakaszát), a redundancia, a pufferkapacitás és az energiatárolás növelésével érhetők el. Ez csökkenti a rendszer sebezhető elemeinek terhelését, és egyben elővigyázatossági intézkedésként is szolgál a további, még ismeretlen stresszorok ellen (Gößling- Reisemann, 2016). Az ismeretlen jövőbeli stresszorokra való felkészülés érdekében a rendszerben olyan elveket és elemeket kell bevezetni, amelyek növelik a rendszer ellenálló képességét.

A 9. ábrán összefoglalt elveket és elemeket olyan tervezési elvek és elemek kereséséből vezettük le, amelyek ismert rugalmasságnövelő tulajdonságokkal rendelkeznek, például az ökoszisztémák evolúciós folyamataira vonatkozó ismeretekből vagy az energiarendszerek, szervezetek és más alkalmazási területek társadalmi-technikai rugalmasságára vonatkozó ismeretekből. A kiválasztott elemek rövid leírása az alábbiakban olvasható, részletesebb elemzésük a (Brand et al., 2017) című könyvben található.

**A sokféleség** pozitívan járul hozzá ahhoz, hogy egy rendszer képes legyen reagálni a stresszorokra. Annak érdekében, hogy a sokféleség fogalmát működőképesebbé és potenciálisan mérhetőbbé tegyük, Stirling azt javasolja, hogy a sokféleséget az egyenlőtlenesség, a változatosság és az egyensúly fogalmaiban határozzuk meg (Stirling, 2007). A diszparitás alatt a rendszer elemei közötti különbségeket értjük. A változatosság az

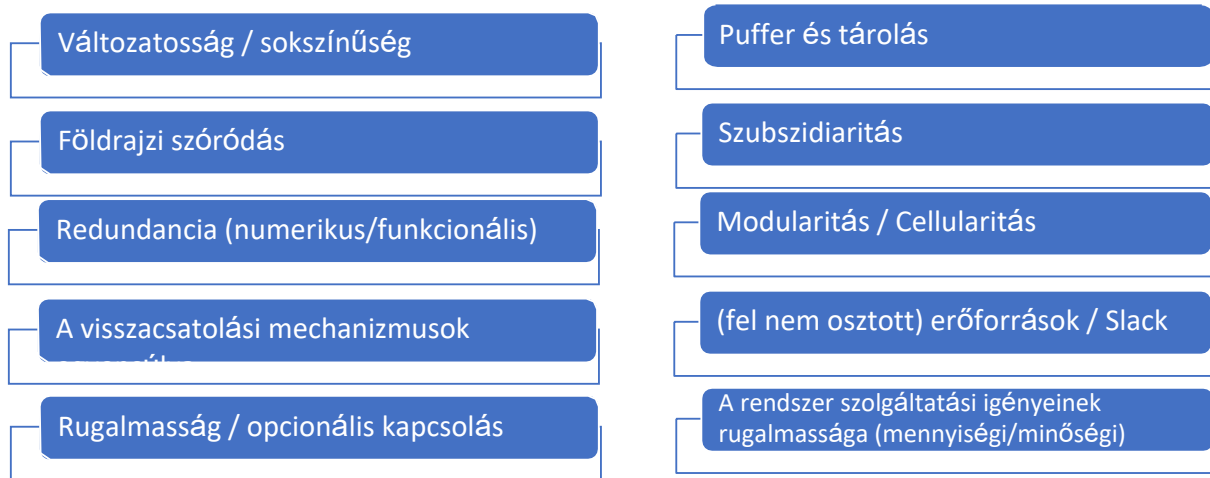
azonos funkciójú különböző elemek mennyiségét vagy számát jellemzi a rendszerben. Az egyensúlyt e különböző elemek eloszlása (keveréke) adja (Goessling-Reisemann és Thier, 2019). Célszerű az energiarendszerben meglévő technológiákat is megvizsgálni a sokféleséget növelő alternatív megoldások szempontjából.

**A redundancia** a rendszer elemeinek többszörös rendelkezésre állását írja le, akár számban, akár funkcionális egyenértékűségben. Ezekre a többszörös elemekre a normál működés során általában nincs szükség. A számszerű redundancia alatt az azonos funkcióval rendelkező, azonos számú azonos elem rendelkezésre állását értjük, míg a funkcionális redundancia arra a helyzetre utal, amikor ugyanazt a funkciót egymástól jelentősen eltérő elemek (pl. különböző technológiák, operációs rendszerek stb.) látják el (Goessling-Reisemann és Thier, 2019).

**A földrajzi szétszóródás** fontos szerepet játszik az ellenálló képesség szempontjából. A rendszerelemek földrajzi szétszóródásával minden lokális stresszornak, az időjárással kapcsolatos eseményektől a terrortámadásokig, viszonylag kisebb a támadási felülete (Goessling-Reisemann és Thier, 2019). A rendszerkritikus szolgáltatások szélesebb földrajzi tartományban történő elosztása így növeli a rezilienciát.

**A pufferek és tárolók** rendszerekben történő megvalósítása lehetővé teszi a rendszer számára, hogy belső vagy külső erőforrás-korlátozások esetén is fenntartsa szolgáltatásait. A pufferek és tárolók olyan extra kapacitásokat biztosítanak a rendszer számára, amelyek késleltetik a kritikus rendszerállapotokat az ellátás megszakadása után. Ezek az elemek tehát több olyan funkciót töltenek be, amelyek fokozzák a rendszer ellenálló képességét; leválasztják az alrendszereket vagy infrastruktúrákat egymásról, biztosítva a rendszer működését a kapcsolatok megszakadása után is, továbbá extra időt nyernek a rendszer helyreállításához, és önmagukban is megkönnyítik a helyreállítási folyamatot. Helyi megvalósítás esetén segíthetnek abban, hogy válság idején a rendszer nagyobb számú felhasználója számára minimális szolgáltatást tartsanak fenn (lásd (Lovins és Lovins, 2001) a villamosenergia-hálózatokra vonatkozó illusztrációkat) A tartalék energiaellátás akkumulátorokból történő szállítása az átviteli hálózatok megszakadása esetén egy példa erre (Goessling-Reisemann és Thier, 2019).

Egy olyan rendszert, amely felosztható és alszegmensekre bontható, **modulárisnak/cellulárisnak** nevezünk, ha az aggregált elemek teljes rendszerfunkciót biztosítanak az alszegmensekben (Goessling-Reisemann és Thier, 2019). A modularitás a műszaki rendszerek javíthatóságának és a kiesési idők csökkentésének tekinthető, de a sokféleség növelését is lehetővé teszi, ha a modulok jól definiált interfészekkel vannak ellátva, hogy megkönnyítsék a különböző technológiai megvalósítások cseréjét (Huang és Kusiak, 1998) idézi (Goessling-Reisemann és Thier, 2019).



9. ábra A rendszerek ellenálló képességét növelő elvek és elemek áttekintése. Forrás: (Goessling- Reisemann és Thier, 2019)

### 3.2.3 Kezelje és visszaállítani

Ha az energiarendszer meghibásodásai válságokhoz vezetnek, akkor azokat a lehető legkisebb területre vagy alrendszerre kell korlátozni, és a lehető leggyorsabban le kell küzdeni. Az ilyen válságok mértékének csökkentése érdekében regionális vagy helyi szinten vészhelyzeti tervezést és megfelelő intézkedéseket kell végrehajtani. A megújuló energiák növekvő részarányával együtt jár az energiarendszerek decentralizációjának tendenciája, ami a nagyobb ellenálló képesség érdekében kihasználható (Gößling- Reisemann, 2016).

### 3.2.4 Tanuljon a jövőre nézve

A múltbeli katasztrófákat és az elkerült katasztrófákat fel kell használni a **jövőre vonatkozó tanulságok levonására**, és ezáltal a rendszer alkalmazkodóképességének javítására. Ezt úgy lehet elérni, hogy dokumentáljuk és elemezzük ezeket a válságokat és eseményeket, ezáltal azonosítva azokat a gyengeségeket, amelyek bekövetkezésükhöz vezettek (sebezhetőségi tár), illetve azonosítjuk azokat az erősségeket, amelyek elkerülésükhöz vagy helyreállításukhoz vezettek (megoldási tár). A válságokra és a lehetséges megoldásokra vonatkozó ismereteket ezután szimulációk és üzleti játékok létrehozására kell felhasználni a rendszer szereplői számára minden szinten. Az improvizációs képesség növelhető azáltal, hogy a szereplőket ezekben a szimulációkban előre nem látható és valószínűtlen fejleményekkel, például kombinált külső fenyegetésekkel és a berendezések belső meghibásodásaival szembesítik (Gößling-Reisemann, 2016).

## 4 Sebezhetőségi értékelés eredményei

A VA az IKT-infrastruktúrából származó kritikus tulajdonságok, struktúrák és elemek széles körét azonosítja, amelyek hozzájárulnak a CPPS sebezhetőségéhez. A kvalitatív tartalomelemzés eredményei alapján a megállapításokat négy kategóriába és alkategóriába sorolták, amint azt a 2. táblázat mutatja.

2. táblázat. A kiberfizikai energiarendszerek kritikus tulajdonságait, struktúráit és elemeit tükröző kategóriák és alkategóriák

Kategória	Alkategória
Technológia	Bizonytalan végpontok
	Bizonytalan kommunikáció
Szervezeti biztonsági politikák és eljárások	Helytelen javításkezelés
	Az interdiszciplináris IT-OT ismeretek hiánya
Az emberi tényező	A biztonságtudatosság hiánya a szervezetekben
	A fogyasztók biztonságtudatosságának hiánya
Szabályzat	A szabványok és rendeletek hatékony végrehajtásának hiánya
	A biztonság javítására irányuló összehangolt erőfeszítések hiánya

Az egyes alkategóriák sebezhetőségét külön-külön értékeltük a 3.1. pontban ismertetett VA-módszerrel, és az eredményeket a következő szakaszokban ismertetjük.

### 4.1 Technológia

#### 4.1.1 Bizonytalan kommunikáció

A kiber-fizikai energiarendszerben részt vevő rendszerek, szolgáltatások és szereplők számának növekedése azt jelenti, hogy több összeköttetésre van szükség. Mivel az energiarendszerek szinte ugyanazt a TCP/IP alapú kommunikációs technológiát használják, mint az üzleti informatikai hálózatok, az ezzel kapcsolatos kiberbiztonsági problémák az energiarendszereket is érintik (Intervjú 1, személyes kommunikáció, 2016; Intervjú 6, személyes kommunikáció, 2016). Mindazonáltal,

a biztonsági követelmények nem azonosak az üzleti és ipari hálózatokkal. A titoktartás fontos szempont a hagyományos informatikában a vállalati információk titkossága miatt, de aligha élvez prioritást az ipari vezérlőrendszerekben (ICS), ahol az adatok integritása és rendelkezésre állása létfontosságú a rendszerek működésének fenntartásához (Marin Fernandes, 2012).

Ha a kommunikáció titkosítatlan vagy gyengén titkosított hálózati protollokat használ, a hitelesítési kulcsok és az adattartalom kiszolgáltatottá válik. A nyílt szövegű protollok használata lehetővé teszi a támadók számára a munkamenet eltérítését és a Man-in-the-Middle (MITM) támadásokat is, lehetővé téve a támadó számára az eszközök között továbbított adatok manipulálását (NIST, 2014). Bár egyes kapcsolatok biztonságosabbak lehetnek, mint mások, a kiber-fizikai energiarendszerek nagymértékben összekapcsolt jellege miatt a leggyengébb láncszem is támadási vektorként használható más tartományokba (Knapp, 2011).

A bizonytalan kommunikáció miatti sebezhetőség értékeléséhez az energiarendszer SGAM-tartományait (lásd a 4. ábrát) három csoportba soroltuk: (a) fogyasztás, b) elosztott energiaforrások és elosztás, c) termelés és átvitel.

#### 4.1.1.1 Expozíció és érzékenység

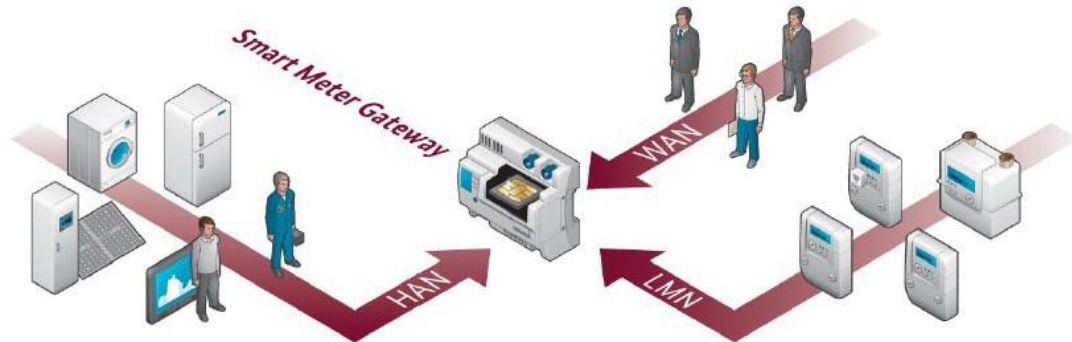
##### **a. Fogyasztás**

Az intelligens mérőinfrastruktúra esetében a szakértők többsége megemlítette, hogy Németországban erős titkosított kommunikációs rendszer működik, amely a német Szövetségi Információbiztonsági Hivatal (BSI) által az intelligens mérőportál védelmi profiljában (lásd (BSI, 2014)) meghatározott IT-biztonsági architektúrán és biztonsági követelményeken alapul.

A 10. ábrán bemutatott biztonsági architektúra szerint a központi kommunikációs komponens egy intelligens mérőátjáró (Smart Meter Gateway, SMGW), amely az ügyfél telephelyén található, és összekapcsolja a helyi mérőhálózatban (LMN) lévő elektronikus mérőberendezéseket, valamint az otthoni hálózatban (HAN) lévő bármely vezérelhető fogyasztási, tárolási vagy termelési eszközt a különböző piaci szereplőkkel (pl. a mérőhely-üzemeltető, az elosztórendszer-üzemeltető vagy az energiaszolgáltató nevében eljáró Smart Meter Gateway Administrator (SMGA)) a széleskörű hálózatban (WAN) (BSI, 2015a). Az SMGW összegyűjti, feldolgozza és tárolja a mérő(k)ről származó nyilvántartásokat, és biztosítja, hogy csak az arra jogosult felek férjenek hozzá. A releváns információkat küldés előtt aláírják és titkosítják, az SMGW szerves részeként beágyazott biztonsági modul kriptográfiai szolgáltatásainak felhasználásával. A védelmi profil (PP) meghatározza a biztonsági

célkitűzéseket és a megfelelő biztonsági követelményeket egy olyan biztonsági modulra vonatkozóan, amelyet az átjáró a kriptográfiai támogatáshoz használ (BSI, 2014)). Az intelligens mérési infrastruktúra különböző összetevői közötti átjárhatóság biztosítása érdekében a BSI

meghatározott műszaki végrehajtási iránymutatások, amelyek a TR-03109 műszaki iránymutatásban találhatóak, lásd (BSI, 2013).



10. ábra Smart Meter Gateway architektúra. Forrás: (BSI, 2015a)

Annak ellenére, hogy ez a kommunikációs rendszer az adatvédelem, az adatbiztonság és az interoperabilitás biztosítását célozza, egyes szakértők azt is megemlítették, hogy vannak hátrányai is. A rendszer már néhány éves, és a fő célja csak az SMGW és az SMGA közötti kommunikáció titkosítása. Az SMGW és más szereplők, azaz a külső piac közötti kommunikáció biztonsági követelményeit nem szabályozza az SMGA tanúsítási folyamata, ami potenciális biztonsági rést jelenthet, amely veszélyeztetheti az intelligens mérési adatok biztonsági követelményeit (8. interjúalany, személyes közlés, 2017; 19. interjúalany, személyes közlés, 2017). közlemény, 2017).

A PP és a kapcsolódó technikai végrehajtási iránymutatások értékelését von Oheimb, D. végezte el (von Oheimb, 2012), és számos hátrányra mutatott rá. Megemlítették, hogy a biztonsági rendszer csak az SMGW esetében igényel nehéz védelmi mechanizmust, ami nagy technikai többletköltséget, valamint magas végrehajtási, tanúsítási és használati költségeket jelent. Továbbá a titkosítási rendszerrel kapcsolatban a tanulmány megemlítette, hogy a klasszikus nyilvános kulcsú infrastruktúra (PKI) használata nagyon kritikus központi hibapontokat vezet be, ahol bármely gyenge pont kihasználása hatalmas károkat okozhat a teljes rendszerben. Ezt megerősítette egy informatikai biztonsági interjúalany is, aki megemlítette, hogy a nyilvános kulcsú kriptográfia alkalmazása az energiaágazatban, az energiarendszerek lényegében a nyilvános kulcsú kriptográfia azon problémáit örökítenék meg, amelyek jelenleg az online biztonságot, például a weboldalakat érintik. A problémák alapvetően a PKI fenntartásával járó többletköltségekben, nevezetesen a tanúsító hatóságokban és a kulcskezelésben rejlenek (13.

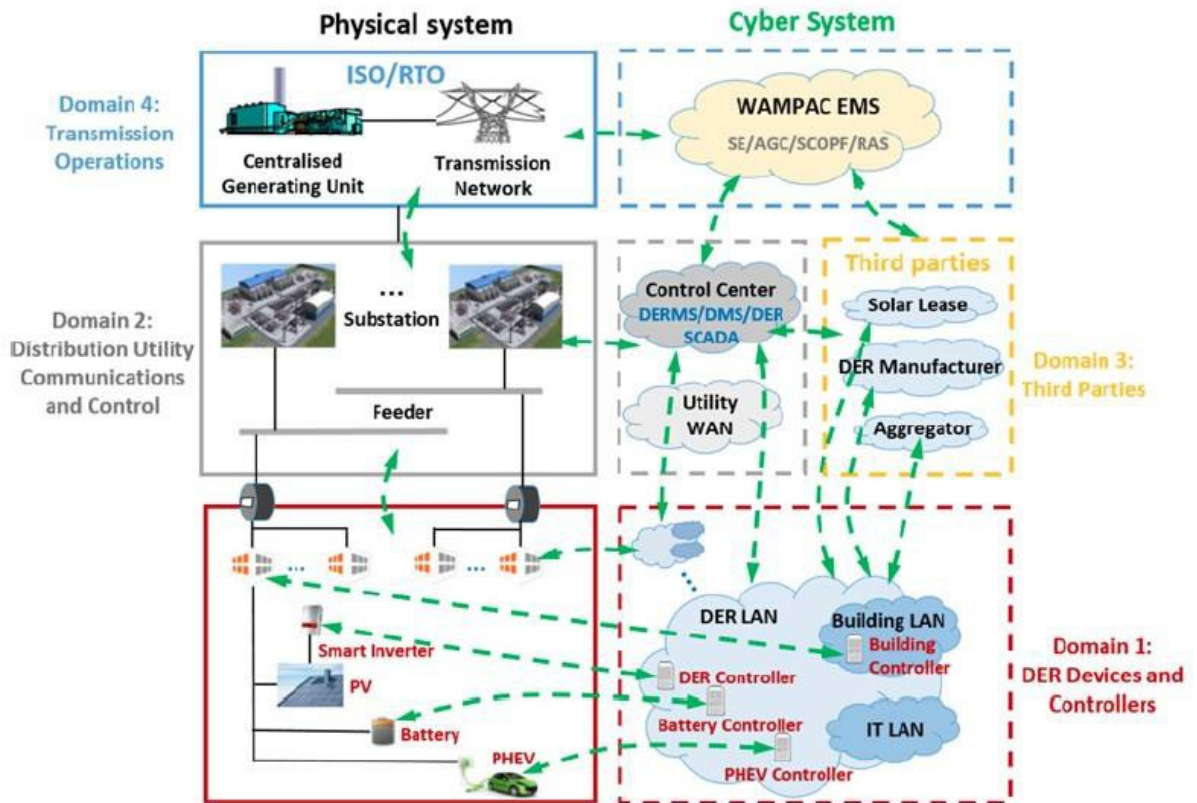
interjúalany, személyes közlés, 2017).

Az ügyfél helyiségein belül az otthoni vagy épületautomatizálási rendszerekben (pl. automatizált világítási rendszerek, felügyeleti rendszerek, intelligens készülékek és egyéb IoT-eszközök) használt kommunikációs protokollok egy másik belépési pontot jelenthetnek a potenciális adatbiztonság megsértéséhez, főként azért, mert e protokollok némelyike a tervezéskor nem biztonságos, és a jelenlegi szabályozás nem foglalkozik velük. Erre a gyengeségre példa a Morgner *et al.* által végzett munka (Morgner *et al.*, 2017). Ők a ZigBee Light Link (ZLL) hálózati protokoll biztonsági elemzését végezték el, amely a lakó-, kereskedelmi és ipari épületekbe szánt világítási rendszerek által használt egyik legnépszerűbb szabvány. Az elemzés a ZLL *touchlink* üzembe helyezési eljárására irányult, amelyet a ZLL-eszközök integrálására használnak a kriptográfiai hitelesítés helyett közvetlen közelségen keresztül. Az eredmények azt mutatták, hogy az *érintőkapcsolati* kommunikáció olyan kommunikációs keretekre támaszkodik, amelyek sem nem biztonságosak, sem nem hitelesítettek. Továbbá a hálózati kulcsnak a csatlakozó eszközhöz történő szállítása kizárólag egy globális mesterkulcs által védett, amely 2015 márciusában kiszivárgott, és a korábbi ZigBee Light Link termékekkel szembeni visszafelé kompatibilitási követelmények miatt nem újítható meg (Morgner *et al.*, 2017). A ZigBee egy népszerű szabvány a vezeték nélküli, alacsony fogyasztású kommunikációra, amelyet számos, a tárgyak internetét (IoT) használó eszközben valósítottak meg más alkalmazásokhoz, amelyek közé tartoznak az ajtózárok és a behatolásjelző rendszerek, további bizonytalan belépési pontokat adva hozzá, amelyek veszélyeztethetik a HAN-en belüli adatok biztonsági követelményeit.

#### **b. Elosztott energiaforrások (DER) és elosztás**

Az elosztott energiaforrások növekvő elterjedése dinamikusabbá és összetettebbé tette a hálózatot (Arghandeh *et al.*, 2016), jelentősen megnövelve a fogyasztók és harmadik felek tulajdonában és irányításában lévő eszközök (pl. intelligens inverterek, akkumulátorvezérlők) számát (Qi *et al.*, 2016).

Helyi szinten a DER-rendszerek a helyi feltételek, az előre meghatározott beállítások és a DER-tulajdonosok preferenciái alapján önállóan irányítják saját termelési és tárolási tevékenységeiket. A DER-rendszerek azonban aktív résztvevői a hálózati működésnek, és azokat össze kell hangolni más DER-rendszerekkel és az elosztóhálózati eszközökkel (IEC, 2016). A Qi, J. és társai által kidolgozott munkában (Qi *et al.*, 2016) egy négy tartományba csoportosított DER-rendszerarchitektúrát javasoltak, amely a DER és az intelligens inverterek kiberbiztonságának elemzéséhez használt különböző szereplőket és kölcsönhatásokat ábrázolja (lásd a 11. ábrát).



11. ábra A DER-eket tartalmazó energiarendszerek általános felépítése. Forrás: (Qi et al., 2016)

A következőkben a szerzők által említett néhány kritikus pontot említenek a bizonytalan kommunikációval kapcsolatban (Qi et al., 2016):

- **1. terület: DER-eszközök és -vezérlők:** A DER-tulajdonosok a DER-ről szóló információkat az intelligens inverterekkel való kommunikáció révén kapják meg, olyan bizonytalan vezeték nélküli kommunikációs protokollok segítségével, mint például a ZigBee.
- **2. terület: elosztó közművek kommunikációja és vezérlése:** A közművek az intelligens inverterekkel és vezérlőkkel olyan kommunikációs protokollok segítségével lépnek kapcsolatba, mint például az intelligens energiaprofil (SEP) 2.0, amelyet ellenőrizni kell a sebezhetőség szempontjából.
- **3. terület: Harmadik felek:** A legtöbb harmadik fél képes a DER állapotának nyomon követésére, és néhányan képesek közvetlenül is ellenőrizni a DER működését. Továbbá ezek a szervezetek nagyon sok DER-hez kapcsolódhatnak. Ezek az összeköttetések olyan központosított pontokat hoznak létre, amelyeket a támadók potenciálisan kihasználhatnak arra, hogy több elosztóhálózaton keresztül nagyszámú DER-t manipuláljanak és befolyásoljanak.
- **4. terület: Átviteli művelet:** A DER-üzemeltetést integrálni kell a nagy villamosenergia-hálózat üzemeltetésébe. Az erre a célra használt

kommunikációs protokollok közé tartozik az elosztott hálózati protokoll (DNP3) és az IEC 61850, amelyek eleve nem biztonságosak, és a biztonsági fejlesztések nem minden esetben valósíthatók meg.

végrehajtották (lásd a 4.4.1. szakaszt A biztonsági előírások és rendeletek hatékony végrehajtásának hiánya).

Amint azt az energia- és piaci ágazat egyik interjúalánya említette, a DER kommunikációs infrastruktúrája részben szabályozott, és a külső szereplők, mint például: a gyártók (pl. a PV-inverterek vagy a szélturbinák gyártói) vagy a közvetlen forgalmazók hozzáférhetnek az elosztott energiatermelő egységek vezérlőihez, hogy információkat kapjanak felügyeleti és ellenőrzési célokra. Problémák merülhetnek fel, mivel ezek a szereplők saját kommunikációs infrastruktúrával rendelkeznek a termelőegységekhez, amely nem biztonságos, és hátsó ajtót jelenthet a rendszerhez való hozzáféréshez (Interjúalany 2, személyes kommunikáció, 2016).

### **c. Termelés és átvitel**

Az ICS és a felügyeleti ellenőrző és adatgyűjtő (SCADA) rendszerek kommunikációs protokolljai az idők során a szabadalmaztatott pont-pont kapcsolatokról nyílt és szabványos protokollokká fejlődtek, amelyeket az elosztott rendszerekben használnak (McLaughlin et al., 2015). Kezdetben az energiarendszerek kommunikációs infrastruktúrája általában biztonságos volt, mivel el volt szigetelve a külső kommunikációs hálózatoktól (az úgynevezett "légrés"). Emellett egyedi, szabadalmaztatott hardveren és szoftveren alapultak, ami ésszerű "ismeretlenség általi biztonságot" biztosított számukra (Teixeira et al., 2015). Az IKT-hálózatokkal való kiterjedt konvergencia és a TCP/IP protokollokon alapuló domináns kommunikáció azonban nagy biztonsági problémát jelent az energiarendszerek számára (Interjúalany 2, személyes kommunikáció, 2016).

A hagyományos ICS kommunikációs protokollokat a kiberbiztonság szem előtt tartása nélkül tervezték, ezért nem rendelkeznek olyan informatikai biztonsági mechanizmusokkal, mint a titkosítás vagy a hitelesítés (15. interjúalany, személyes kommunikáció, 2017). A Modbus például egy egyszerű ügyfél-kiszolgáló protokoll, amelyet eredetileg az ICS-hálózatok alacsony sebességű soros kommunikációjára terveztek. Tekintettel arra, hogy a Modbus protokollt nem erősen biztonságkritikus környezetekre tervezték, a Modbus csomagokat titkosítatlanul küldik, ezért egy támadó könnyen csatlakozhat egy legitim hálózati csomóponthoz, és manipulálhatja az üzenetet, amelyet a vevő nem ismer fel (Interviewee 15, személyes kommunikáció, 2017; Mo et al., 2012), veszélyeztetve a mérési értékeket vagy a vezérlőparancsokat, ami a rendszer hibás működéséhez vezethet.

Továbbá az ipari vezérlőhálózatok egyes esetekben közvetlenül az internethez kapcsolódnak, megfelelő biztonsági intézkedések nélkül, így lehetővé téve a külső fenyegető tényezők számára a hozzáférést, akik vírusokkal vagy rosszindulatú

szoftverekkel fertőzhetik meg az ipari hálózatokat (1. interjúalany, személyes közlés, 2016; 15. interjúalany, személyes közlés, 2016).

közlemény, 2017). Az olyan keresőmotorok, mint a SHODAN<sup>4</sup>, segítségével könnyen megtalálhatók az internetre néző ICS-eszközök. Ezenkívül az interneten könnyen megtalálhatók az ICS protokollok jól ismert gyenge pontjainak kihasználására szolgáló nyílt forráskódú és kereskedelmi eszközök, amelyek még több ilyen rendszert tesznek ki potenciális támadásoknak.

Az SGAM-modell állomáshálózatában (lásd a 3.1.2. szakaszt) egyes érzékelők vagy intelligens elektronikus eszközök (IED) vezeték nélküli kommunikációt használnak, amelyek általában véve a gyenge protokollok, a titkosítási módszerek hiánya vagy a nem megfelelő eszközkonfiguráció miatt általában bizonytalanabbak. Ezen eszközök kompromittálásához azonban fizikai közelségre van szükség, ami az ipari környezetben belüli külső fenyegető tényezők esetében korlátozott lehet (15. interjúalany, személyes kommunikáció, 2017). Létezhet olyan támadási forgatókönyv, amelyben a behatolás kezdeti pontja az alállomáson található a vezeték nélküli eszközökön keresztül, és az elektromos rendszer működése felé terjed. Ha ezt nem veszik figyelembe, az komoly kockázatot jelenthet (18. interjúalany, személyes kommunikáció, 2017).

A legtöbb gyártó rendelkezik távszerviz-interfészekkel a nagyobb alkatrészek, például egy turbina ellenőrzésére és felügyeletére. A távoli hozzáférés a vezérlő szintjére vagy az emberi gépi interfész (HMI) szintjére is bejuthat a frissítések vagy javítások telepítése céljából. Ha a kapcsolat nincs megfelelően biztosítva, ez a távoli hozzáférés lehetővé teheti a rendszer eszközeihez való hozzáférést vagy további rosszindulatú célokat. A hálózatüzemeltetők a különböző eszközökhöz, például az alállomások berendezéseikhez is létrehozhatnak távoli kapcsolatokat a frissítések vagy javítások telepítése céljából. Erre a célra dedikált kommunikációs hálózatokat használhatnak, különösen a nagy üzemeltetők, de más kisebb üzemeltetők használhatják a távközlési szolgáltatók által bérelt hálózatokat vagy az interneten keresztül. Ez utóbbi esetekben, ha a kommunikációs infrastruktúrára vonatkozó biztonsági irányelveket nem megfelelően hajtják végre, az adatbiztonsági követelmények sérülhetnek (4. interjúalany, személyes kommunikáció, 2016; 17. interjúalany, személyes kommunikáció, 2017).

#### 4.1.1.2 Támadási mechanizmusok és stresszorok

A kommunikációs protokollok titkosításának és hitelesítésének hiánya lehetővé teszi a fenyegető ügynökök számára, hogy MITM-támadásokkal különböző műveleteket hajtsanak végre, mint például: a) a csomópontok közötti kommunikáció rögzítése és a csomagok újrarájátszása a rendszer valódi viselkedésének elrejtése érdekében a rendszer részletes ismerete nélkül, b) a munkamenetek eltérítése, amikor egy

## kommunikációs munkamenetet a támadó átvesz és jogosulatlanul használ

---

<sup>4</sup> <https://ics-radar.shodan.io>

az áldozattal való kommunikáció, vagy c) adatok befecskendezése vagy manipulálása a kommunikációs folyamatban lévő olvasás és parancsok valós idejű megváltoztatása érdekében (McLaughlin et al., 2015).

A következő szakaszban a különböző tartományi klaszterek kommunikációs infrastruktúrája elleni néhány támadási mechanizmust és stresszforrást ismertetünk:

### **a. Fogyasztás**

A szimatoló és lehallgató támadásokat a távoli vagy helyi fenyegető ügynökök használhatják a magánélet szempontjából fontos adatok vagy a számlázással kapcsolatos adatok titkosságának és sértetlenségének veszélyeztetésére. A WAN-ban található távoli támadók (lásd a 10. ábrát) megpróbálhatják kompromittálni a helyi infrastruktúra valamelyik komponensét, hogy kárt okozzanak magában a komponensben, vagy közvetlen hatást gyakoroljanak az elektromos hálózatra, például az intelligens inverterek adatmanipulációjával instabil hálózatot idézzenek elő. A helyi támadók, beleértve az átjáróhoz és/vagy a mérőeszközökhöz hozzáféréssel rendelkező prosumereket is, megpróbálhatnák jogosulatlanul kiolvasni vagy módosítani az eszközöket, miközben azokat az LMN-ben tárolják vagy továbbítják (lásd a 10. ábrát) (von Oheimb, 2012).

A HAN-on belüli hálózati eszközök elérhetőségét célzó szolgáltatásmegtagadási támadások a kommunikációs infrastruktúrát ért fizikai támadások révén valósulhatnak meg. A vezetékes kommunikációt a "vezetékek elvágásával" lehet befolyásolni, a vezeték nélküli kommunikációt pedig zavarni lehet (McLaughlin et al., 2015). A zavaró támadás a csatornák érzékeléséből áll, amíg a kommunikációt el nem fogják, majd a csatorna elárasztása jogtalan forgalommal az adatok elérhetőségének befolyásolására használható (Tazi és Abdi, 2015). Ezt a fajta támadást arra lehetne használni, hogy a vezeték nélküli médiumok zajjal való megtöltése révén megakadályozzák, hogy a mérőműszerek összekapcsolódjanak a közműszolgáltatóval. A csatornát a szolgáltatók mindig foglaltnak fogják látni, és az adatcsomagok fogadását megakadályozzák (Baig és Amoudi, 2013) idézi (Lopez et al., 2015).

Morgner és munkatársai (Morgner et al., 2017) valós támadást fejlesztettek ki az okosotthonok területén általánosan használt ZigBee eszközök vezeték nélküli kommunikációjára elleni lehallgatási és csomaginjekciós támadásokra. Az értékelés azt mutatta, hogy a protokoll biztonsági hiányosságai lehetővé teszik a fenyegető ágensek számára, hogy veszélyeztessék az eszközök elérhetőségét, és a hálózat összes csomópontja fölött irányítást szerezzenek.

## **b. Elosztott energiaforrások (DER) és elosztás**

A közműszolgáltatóknak, a DER-gyártóknak vagy harmadik fél aggregátoroknak távolról kell kommunikálniuk a DER-rel a működési pontok vezérlése és az eszközök állapotának figyelemmel kísérése érdekében, ami kritikus fontosságú az elosztóhálózat megbízhatóságának fenntartása szempontjából. Ha a kommunikáció nem titkosított vagy nem biztonságos hálózati protokollokat használ, ezek a gyenge pontok

lehetővé tehetik a fenyegető ügynökök számára, hogy MITM-támadásokat hajtsanak végre az üzenetek megtagadása, megzavarása vagy megváltoztatása érdekében. Ha ezek a támadások bekövetkeznek, akkor a támadó számára lehetővé tehetik, hogy nagyszámú DER-rendszert irányítson, ami komoly hatást gyakorolhat az elosztóhálózatra (Qi et al., 2016).

### c. Termelés és átvitel

A titkosítás és a hitelesítés hiánya számos ipari vezérlő protokoll esetében számos támadásnak teszi kiszolgáltatottá a rendszert. Például MITM-támadások révén egy fenyegető ügynök elfoghatja a kommunikációs kereteket, és összegyűjtheti a titkosítatlan plaintext kereteket, amelyek értékes információkkal szolgálhatnak, például: forrás- és célcímek, valamint vezérlési és beállítási információk (Mo et al., 2012). A támadó a kommunikációs folyamba valós időben adhat be vagy módosíthatja a leolvasásokat és parancsokat. Az összes csomag lehallgatása során egyes csomagok elhagyhatók, módosíthatók vagy tetszőleges kimenetelű új csomagok injektálhatók. Ez a támadás nagyon problematikus, ha tapasztalt felhasználó hajtja végre, mivel nehéz észlelni, és potenciálisan jelentős hatást érhet el. A támadó képes manipulálni a távoli helyekről származó mérési értékeket, valamint elnyomni vagy beadni a két kommunikáló csomópont közötti vezérlőparancsokat (McLaughlin et al., 2015).

A szakirodalomban protokollspecifikus támadásokat találunk. Például az olyan lehetséges támadásokat, mint az üzenet hamisítás, a visszajátszási támadások, a hálózat letapogatása és más, a Modbus biztonsági problémáival kapcsolatos lehetséges támadásokat részletesen ismerteti a (Mo et al., 2012). A Modbus-hálózatok elleni MITM-támadások végrehajtására szolgáló nyílt forráskódú vagy kereskedelmi eszközök szintén könnyen megtalálhatók az interneten.<sup>5</sup> (Bodungen et al., 2017). Az alállomások automatizálására használt protokollok tekintetében több szerző is foglalkozik az IEC 60870-5 protokollt futtató hálózatok elleni DoS-támadásokkal (Dondossola et al., 2008, 2009), mások pedig az IEC 60870-5-104 protokollra támaszkodó ICS elleni MITM-támadást mutatnak be (Maynard et al., 2014).

A "*Crashoverride*" (más néven "*Industroyer*") néven ismert rosszindulatú szoftver egy olyan fejlett és kifinomult rosszindulatú szoftver valós példája, amely több támadási mechanizmust kombinál, és kihasználja az alállomások automatizálásához használt bizonyos ipari protokollok gyengeségeit. Az 1. keretes írás részletes információkat közöl erről a kártevőről.

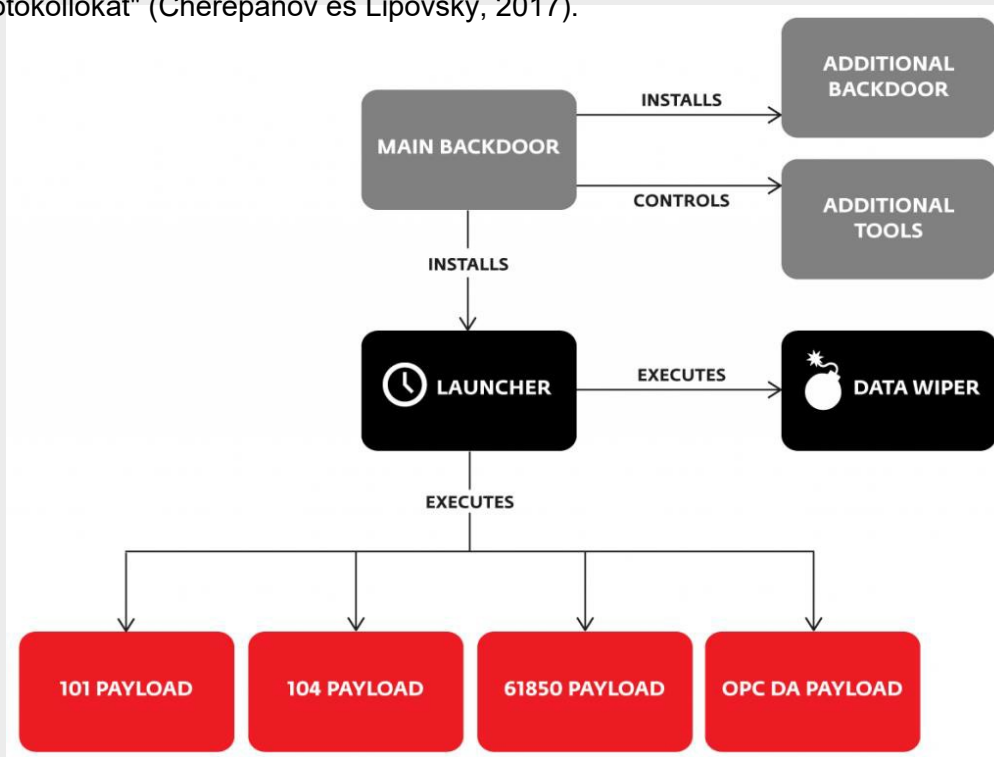
---

<sup>5</sup> A Modbus-VCR (lásd <https://github.com/reidmefirst/modbus-vcr>) egy példa egy szabadon elérhető eszközre, amely az Ettercap-pal együtt rögzíti a Modbus forgalmat, majd visszajátssza azt, így a rendszerek egy rögzített időszak alatt a szokásos módon működnek.

## 1. keretes írás: "Crashoverride" rosszindulatú program

2017 júniusában az ESET és a Dragos biztonsági kutatói részletes elemzést adtak ki erről a rosszindulatú szoftverről, amelyet ICS-összetevők ellen fejlesztettek ki. A szerzők szerint nagyon valószínű, hogy a "Crashoverride" segítségével 2016 decemberében Ukrajnában egy átviteli szintű alállomásra is hatással lehettek, ami áramkimaradásokat okozott (lásd: (Cherepanov, 2017; Dragos Inc., 2017)).

A "Crashoverride" kártevő mögött álló fenyegető szereplők mélyreható ismeretekkel rendelkeztek az energiarendszerekben használt ipari vezérlőrendszerekről, és olyan ipari kommunikációs protokollokat céloztak meg, amelyeket néhány évtizeddel ezelőtt a biztonság szem előtt tartása nélkül terveztek. Ezért a támadóknak "nem kellett protokollsebezhetőségeket keresniük; mindössze arra volt szükségük, hogy megtanítsák a rosszindulatú szoftvereket "beszélni" ezeket a protokollokat" (Cherepanov és Lipovsky, 2017).



12. ábra A "Crashoverride/Industroyer" komponensek egyszerűsített vázlata.

Forrás (Cherepanov és Lipovsky, 2017).

A "Crashoverride" rosszindulatú szoftver egy moduláris keretrendszer, amely képes az alállomások kapcsolóinak és megszakítóinak közvetlen vezérlésére. A 12. ábra mutatja a kártevő felépítését, amely egy fő hátsó ajtóból, egy további hátsó ajtóból, egy betöltő modulból, valamint több támogató és hasznos teher modulból áll. A hátsó ajtót a fenyegető ágensek a többi komponens telepítésére és vezérlésére

használják. Csatlakozik egy

távoli szerver (parancsnoki központ, C&C), hogy parancsokat kapjon és jelentsen a támadóknak. A kiegészítő hátsó ajtó (a Windows Notepad alkalmazás "trójai változata") egy alternatív fennmaradási mechanizmust biztosít, amely lehetővé teszi a támadók számára, hogy a fő hátsó ajtó észlelése és/vagy letiltása esetén újra hozzáférjenek a célzott hálózathoz. Az indítómodul, amely egy adott időpontot és dátumot tartalmaz, betölti a hasznos tehermodulokat, és elindít egy 1 vagy 2 órás visszaszámlálást az adattörlő komponens elindításához. A hasznos terhelési komponensek a következő szabványokban meghatározott bizonyos ipari kommunikációs protokollokat célozzák meg: IEC 60870-5-101, IEC 60870-5-104, IEC 61850 és OLE for Process Control Data Access (OPC DA). A törlőmodul a rendszer szempontjából fontos rendszerleíró kulcsok törlésére és fájlok felülírására szolgál, hogy a rendszer indíthatatlanná váljon és a helyreállítás megnehezüljön (Cherepanov, 2017; Cherepanov és Lipovsky, 2017; Dragos Inc., 2017).

A következőkben röviden ismertetjük az egyes hasznos modulok legfontosabb jellemzőit:

- A 101-es hasznos teher az IEC 60870-5-101 (más néven IEC 101) nemzetközi szabványról kapta a nevét, amely egy soros kommunikációs protokollt ír le a villamos energiarendszerek felügyeletére és vezérlésére, amelyet az ICS és a távoli végberendezések (RTU-k) közötti kommunikációra használnak. A 101-es hasznos teher részben megvalósítja az IEC 101-ben leírt protokollt, és képes konfigurációs fájl olvasására a hozzá csatlakoztatott összes RTU felsorolásához. E hasznos teher fő célja a mögöttes RTU be-/kikapcsolt állapotának megváltoztatása (Cherepanov, 2017; Virsec, 2017).
- A 104-es hasznos teher a fenti 101-es hasznos teher egy változata, amely TCP/IP hálózaton fut, és képes felderíteni a hálózatban lévő RTU-kat. Nevét az IEC 60870-5-104 (más néven IEC 104) nemzetközi szabványról kapta. A kártevő "megöli" az eredeti folyamatot, amely a normál 104-es hasznos teherfigyelési folyamatot végzi, és egy csaló folyamattal helyettesíti azt. Az 1. fázisban a csaló folyamat csatlakozik a cél RTU-khoz, és végigmegy azok állapotán. A 2. szakaszban a szélhámós folyamat folyamatosan felváltja a cél RTU-k be-/kikapcsolt állapotát, és naplózza a sikert, hogy az üzemeltetők ne kapjanak riasztást (Virsec, 2017).
- A 61850 hasznos teher az IEC 61850 szabvány után kapta a nevét, amely egy olyan protokollt ír le, amelyet a több gyártó közötti kommunikációra használnak az elektromos alállomások automatizálási rendszereinek védelmét, automatizálását, mérését, felügyeletét és vezérlését végző eszközök között. Végrehajtás után a modul egy konfigurációs fájlt használ a célpontok azonosításához, konfigurációs fájl nélkül pedig a helyi hálózatot sorolja fel a potenciális célpontok azonosításához.

Kommunikál a célpontokkal annak azonosítása érdekében, hogy az eszköz vezérel-

e megszakító kapcsolót. A hasznos teher felsorolja az adatokat, és naplót hoz létre gazdag

metaadatok az egyes célpontokról a C&C-be történő exportáláshoz (Cherepanov, 2017; Dragos Inc., 2017; Virsec, 2017).

- Az OPC DA payload komponens az OPC Data Access specifikációban leírt protokoll kliensét valósítja meg. Az OPC (OLE for Process Control) egy szoftverszabvány és specifikáció, amely a Microsoft technológiáin, például az OLE-n, a COM-on és a DCOM-on alapul. Az OPC specifikáció adathozzáférési (DA) része lehetővé teszi a kliens-szerver modellen alapuló, valós idejű adatcserét az elosztott komponensek között. Ez a hasznos teher lekérdezi az általa felfedezett különböző OPC szervereket, és olyan OPC szerverek által biztosított elemeket keres, amelyek az ABB megoldásaihoz tartoznak, mint például a MicroSCADA termékcsalád<sup>6</sup>. A végrehajtás után a modul egy 0x01-es állapotot küld ki, ami a célrendszerek esetében egy "Primary Variable Out of Limits" (Elsődleges változó a határértékeken kívül) állapotnak felel meg, ami az üzemeltetők számára a védőrelék állapotának félreértését eredményezi (Cherepanov, 2017; Dragos Inc., 2017; Virsec, 2017).

A további eszközök közé tartozik a Denial-Of-Service (DOS) eszköz, amely kihasználja a CVE-2015-5374<sup>7</sup> sebezhetőséget, ami a Siemens SIPROTEC digitális reléjének reagálatlan állapotba kerülését okozza, amíg manuálisan újra nem indítják (Cherepanov, 2017).

#### 4.1.1.3 Potenciális hatások

A nem biztonságos kommunikációs csatornák használata befolyásolja az adatbiztonsági követelményeket. A következő szakaszban az előző szakaszban értékelt egyes tartományi klaszterek lehetséges hatásait részletezzük:

##### a. Fogyasztás

Az adatok titkosságának MITM-támadások általi veszélyeztetése az intelligens mérési infrastruktúrában fontosabb biztonsági kérdésnek számít, mint a többi energiarendszer területén (1. interjúalany, személyes közlés, 2016). Az energiafogyasztási adatok elemzése jelentős betekintést nyújthat az ügyfelek magánéletébe (Greveler, 2016). Ha például egy fenyegető ügynök képes megfigyelni az energiafogyasztást, amely közvetlenül összefüggésbe hozható az ügyfél helyiségein belüli aktivitási mintákkal, ez kihatással lehet a háztartástulajdonosok biztonságára. A támadók kikövetkeztethetnék, hogy a tulajdonosok mikor tartózkodnak otthon, hogy bűncselekményeket hajtsanak végre (13. interjúalany, személyes közlés, 2017).

---

<sup>6</sup> Lásd: <http://new.abb.com/substation-automation/products/software/microscada-pro>

<sup>7</sup> Lásd: <https://ics-cert.us-cert.gov/advisories/ICSA-15-202-01>

A keresletre adott válaszrendszerek megvalósításának adatvédelmi vonatkozásai is lehetnek. A keresletre való reagáláshoz a fogyasztás és a termelés nagy gyakoriságú mérésére, valamint rugalmas terhelések rendelkezésre állására van szükség. Ha ezek a magánéletre érzékeny információk rossz kezekbe kerülnek, az ilyen információk titkosságának megsértése szintén magánéletre gyakorolt következményekkel járna (18. interjúalany, személyes közlés, 2017).

A németországi intelligens mérőberendezések biztonsági rendszerével kapcsolatos, a magánélet és az adatvédelem körüli vitáról részletes tájékoztatást nyújt (Greveler, 2016).

### **b. Elosztott energiaforrások és elosztás**

A DER-rendszerek kommunikációs kapcsolatainak megzavarása a támadó számára hozzáférést biztosíthat nagyszámú DER-eszközhöz. Ezek a hatások kisebbek lehetnek, ha a harmadik fél hozzáférése csak a DER állapotának megfigyelésére korlátozódik. Ha azonban a harmadik fél képes megváltoztatni az üzemi beállítási pontokat vagy a szoftverkonfigurációkat, akkor az e rendszerek elleni támadásoknak komoly hatásai lehetnek, amelyek túlmutathatnak egy elosztóhálózaton (Qi et al., 2016).

A NESCOR katalógusában (NESCOR, 2015) megtalálható néhány kapcsolódó hibaforgatókönyv. A DER.6. forgatókönyv például azt az esetet mutatja be, amikor egy fenyegető ágens veszélyezteti a DER-parancsok sorozatát, esetleg visszajátszási támadással, ami hálózati egyensúlyhiányt és áramkimaradásokat okoz. A DER.14. forgatókönyvben egy fenyegető ügynök meghamisítja a DER SCADA vezérlőparancsait, ami áramellátási instabilitást, többek között áramkimaradásokat és áramminőségi problémákat okoz.

### **c. Termelés és átvitel**

A SCADA-rendszer vagy intelligens elektronikus eszköz (IED) elleni adatinjekciós támadások rendszerzavarokat okozhatnak. A hamis protokollparancsok elküldhetők a szolgáltszervezők működésképtelen állapotba kényszerítésére, a szolgáltatások leállítására vagy a visszaállítások kikényszerítésére. Bizonyos parancsok egyszerre több eszköznek is továbbíthatók, így megállítva a hálózati forgalom áramlását, ami a szolgáltatás megtagadásához (DoS) vezethet. Ezen túlmenően rosszindulatú kódok felhasználhatók a diagnosztikai adatok törlésére (Lopez et al., 2015; Mo et al., 2012).

Az ipari kommunikációs protokollok gyengeségeit kihasználó "Crashoverride" rosszindulatú szoftver esetében a Dragos csapata legitim támadásokat és hatásforgatókönyveket írt le, amelyek a következőket foglalták magukban:

---

feszültségmentesített alállomások és kényszerített szigeteléses esemény (Dragos Inc., 2017). Az első forgatókönyvben a rosszindulatú vezérlőparancsokat ténylegesen végtelen hurokban az alállomások lezárt megszakítóinak kinyitására küldik. Ha egy rendszerüzemeltető megpróbál a HMI-jén (Human Machine Interface - ember-gép interfész) bezárási parancsot kiadni, a szekvenciahurok folytatja a megszakító újbóli kinyitását. Ez a nyitott megszakítókat fenntartó hurok gyakorlatilag

áramtalanítja az alállomás vezeték(ek)et, megakadályozva a rendszerüzemeltetőket a megszakítók kezelésében és a vezeték(ek) újbóli feszültség alá helyezésében. A vezeték vagy alállomás feszültségmentesítése a rendszer dinamikájától, a teljesítményáramlástól és más változóktól függ. Bizonyos körülmények között nem biztos, hogy azonnali hatása van, míg más esetekben áramkimaradásokat okozhat. Továbbá, mivel a központ elveszíti a megszakítók távvezérlését, a kézi működtetéshez szervizszemélyzetet kell küldeni az alállomásra. Ez néhány órás áramkimaradásokkal jár.

A második forgatókönyv szerint a fenyegető ügynökök egy vagy több RTU-t vesznek célba, és egy olyan vezérlőparancsot küldenek, amely a megszakító állapotát folyamatosan váltogatja a nyitott és a zárt állapot között. A megszakító állapotának megváltoztatása automatikus védelmi műveleteket indít el az alállomás elszigetelésére, ami hálózati instabilitást okozhat. Ha több alállomás összehangoltan sérül, a hatás kiterjedt áramkimaradásokhoz vezet.

#### 4.1.1.4 Potenciális hatások minősítése

A nem biztonságos kommunikációs csatornák használata veszélyezteti az integritást és a rendelkezésre állást, valamint a letagadásmertességi követelményeket, ami közvetlen hatással lehet az energiaellátásra. Az adatok titkosságának veszélyeztetése hatással lehet a közvetett paraméterekre, azaz az intelligens fogyasztásmérés társadalmi elfogadottságára. Ezért a VA módszertana szerint a lehetséges hatások a középestől a nagyig terjednek.

#### 4.1.1.5 Alkalmazkodási stratégiák és végrehajtás

A megkérdezettek szerint a villamosenergia-rendszer biztonságának megőrzése érdekében többszintű biztonsági mechanizmusokat kell egymásra építeni. Először is, az adatok és a kommunikációs csatornákon kriptográfiai módszereket kell alkalmazni az adatok integritásának biztosítása és az információk nem szándékos felfedésének megakadályozása érdekében. Ezen túlmenően a támadók tevékenységének hatékony átláthatósága érdekében behatolásérzékelő rendszerek (IDS) bevezetésére van szükség. (Interjúalany 1, személyes kommunikáció, 2016; Interjúalany 13, személyes kommunikáció, 2017). Az IDS-ek előnye, hogy képesek az ismert támadások felderítésére, rendelkezésre állnak a gyakori támadások mintáinak és szignatúráinak adatbázisai, amelyek letölthetők. Hátránya azonban, hogy az ilyen típusú rendszerek nem képesek az ismeretlen támadások észlelésére, ami más megközelítéseket igényel (Interviewee 1, személyes kommunikáció, 2016).

A titkosítás használata nem mindig megfelelő választás, és a szükségtelen titkosítás

---

előtt teljes mértékben meg kell ismerni a titkosítás használatával elvesző információkezelési képességeket (NIST, 2014). Amint azt az informatikai és automatizálási ágazat szakértői említették, az ipari vezérlőhálózatokon történő adattitkosítás a következőkkel járhat

növeli a késleltetést. Egyes gyártók megoldásokat kínálnak az ICS, pl. PLC előtt telepítendő titkosító eszközökre, amelyek titkosítják/dekódolják a kommunikációt. Más megoldások szállítói speciális eszközöket fejlesztenek ki az eszközeik közötti biztonságos kommunikáció biztosítására. A további megoldásoknak a közvetlenül az ipari vezérlőkön történő titkosítás irányába kell elmozdulniuk. A kvantumtitkosítás egy újszerű megoldás, amelyet kifejezetten a titkosság elérésére terveztek, de az ipari hálózatok esetében a legfontosabb kritérium a rendelkezésre állás, és ennek a megoldásnak bizonyítania kell, hogy nem növeli a késleltetést és nem befolyásolja a rendszer teljesítményét általában (15. interjúalany, személyes közlés, 2017). Abban az esetben, ha nem praktikus az összes mérés titkosítása, kritikus fontosságúvá válik a támadásnak kitett mérések felderítése és elkülönítése. A támadás hatékony elszigetelése lehetővé teszi a kárelhárítás (pl. a megtámadott mérések eltávolítása az állapotbecsléshez) időben történő elvégzését, mielőtt a támadás jelentős következményekkel járó incidenshez vezethetne (Teixeira et al., 2015).

A hagyományos ICS kommunikációs protokollok esetében már léteznek szabványok a biztonság növelésére. Az IEC 62351 szabványkészlet például biztonsági fejlesztéseket biztosít az olyan protokollok számára, mint az IEC 60870-5-104 és az IEC 60870-5-101. A gyártók azonban nem hajtják végre ezeket, és általában csak alapvető funkciókat biztosítanak, így az elosztóhálózati szolgáltatók nem lesznek képesek biztonságos környezetet létrehozni (1. interjúalany, személyes kommunikáció, 2016) (A biztonsági szabványok hatékony végrehajtásának hiányáról, mint sebezhetőségi feltételről bővebben lásd a 4.4.1. szakaszt).

Az informatikai és automatizálási ágazat szakértői emellett megemlítették, hogy tapasztalataik szerint az ipari ágazatban működő ügyfelek vagy vállalatok általában nem a legmodernebb technológiát, hanem már tesztelt és robusztus megoldásokat akarnak (15. interjúalany, személyes közlés, 2017).

Mivel a mai villamosenergia-hálózati berendezések nagy része régi, az adattitkosítás megvalósítása költséges lehet a berendezések megfelelő frissítése miatt. Ezért fontos meghatározni, hogy mely méréseket kell titkosítani a védelmi erőforrásokból származó előnyök maximalizálása érdekében (Teixeira et al., 2015).

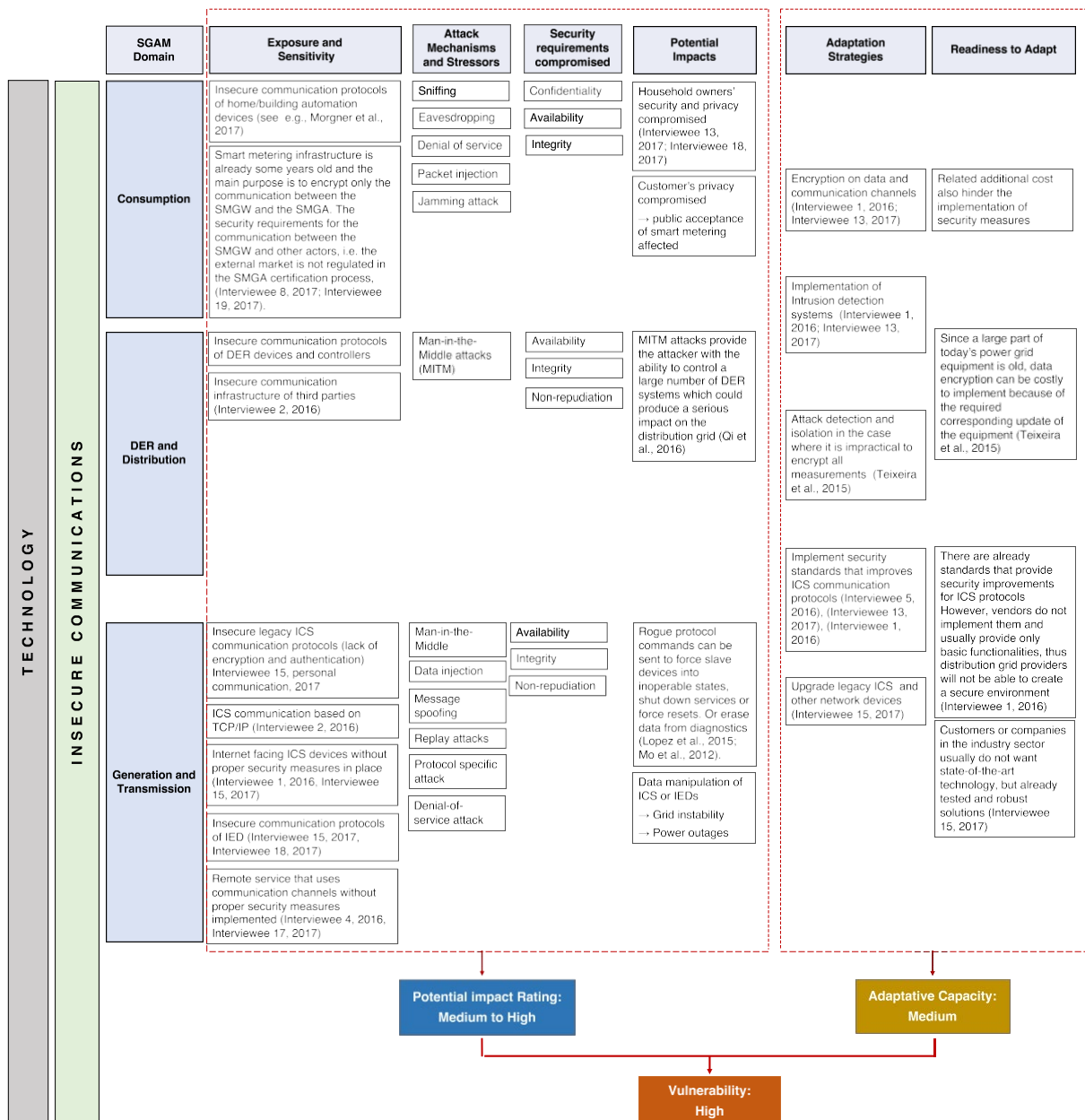
#### 4.1.1.6 Alkalmazkodóképesség minősítés

Az előző szakasz szerint léteznek olyan adaptációs mechanizmusok (pl. ICS biztonsági protokollok), amelyek javítják a kommunikáció biztonságát, azonban az ICS-tulajdonosok preferenciái vagy a kapcsolódó többletköltségek miatt korlátozott lehet a hajlandóság ezek alkalmazására. Ezért az alkalmazkodóképesség közepesnek minősül.

#### 4.1.1.7 Sebezhetőségi besorolás

A 4.1.1.1.4. szakaszban a potenciális hatások és a 4.1.1.1.6. szakaszban az alkalmazkodási képesség értékelése szerint a magas potenciális hatások és a közepes alkalmazkodási képesség a bizonytalan kommunikáció miatti magas sebezhetőséget eredményezi.

A 13. ábra összefoglalja a nem biztonságos kommunikáció miatti sebezhetőségi értékelést.



13. ábra A kiberfizikai energiarendszerek sebezhetőségének értékelése a nem biztonságos kommunikáció miatt. Az értékeléshez a villamosenergia-rendszer SGAM-tartományait három csoportba soroltuk: a) fogyasztás, b) elosztott energiaforrások (DER) és elosztás, c) termelés és átvitel. Forrás: A szerzők saját ábrázolása

#### 4.1.2 Bizonytalan végpontok

A hálózatbiztonságban a végpont minden olyan eszköz, amely hálózatra képes. A SGAM-tól eltérő zónákban és tartományokban lévő végpontok saját kihívásokat jelentenek. A nem biztonságos végpontok miatti sebezhetőség felmérése érdekében a villamosenergia-rendszer SGAM-tartományait (lásd a 4. ábrát) három csoportba soroltuk: (a) fogyasztás, (b) elosztott energiaforrások, (c) termelés, átvitel és elosztás.

##### 4.1.2.1 Expozíció és érzékenység

###### a. Fogyasztás

Az ügyfél telephelyén található végpontokat (lásd a 4. ábrát) (pl. otthoni automatizálási rendszer, IoT-eszközök, mobiltelefonok, laptopok) nem szabályozzák kiberbiztonsági intézkedések, és gyenge biztonsági jellemzőkkel telepítik őket. Ezért, ha ezen eszközök jól ismert sebezhetőségeit kihasználják, rosszindulatú behatolási pontokként használhatók fel az energetikai infrastruktúrát érő további támadások végrehajtásához. Ezek az eszközök nem rendelkeznek olyan biztonsági képességekkel, mint a biztonságos kulcskezelés és a hitelesítő adatok biztonságos tárolása. A hitelesítéssel is gond van, mivel sok esetben az eszközök nem rendelkeznek azonosítóval, és nem rendelkeznek megfelelő hitelesítő adatokkal a hitelesítéshez. Ezenfelül az eszközök nem rendelkeznek elegendő képességgel a javítások és a szoftverek kezelésére. A hálózathoz való ellenőrzési hozzáférés is korlátozott (5. interjúalany, személyes kommunikáció, 2016; 14. interjúalany, személyes kommunikáció, 2017; 18. interjúalany, személyes kommunikáció, 2017). közlemény, 2017).

Továbbá a szoftverintegritás-ellenőrzés vagy az aláírt szoftverek hiánya a tárgyak internete eszközökben megkönnyíti a rosszindulatú programok feltöltését ezekre az eszközökre, ahonnan támadást lehet indítani szolgáltatásmegtagadási támadások végrehajtására (5. interjúalany, személyes közlés, 2016). Az intelligens otthoni eszközökkel kapcsolatos biztonsági kihívásokat és fenyegetéseket bővebben tárgyalja (Lee et al., 2014).

Ha az eszközök jobban el vannak osztva, akkor a biztonsági intézkedések végrehajtásának skálázhatósága is problémát jelent a megfelelő biztosításuk érdekében, mivel nem csak néhány végpontot kell felügyelni, karbantartani és frissíteni, hanem több ezret (5. interjúalany, személyes közlés, 2016). Ebből a szempontból az elektromobilitás a jövőben nagy támadási felületet jelent majd az ügyféloldalon (Expertens-Workshop 2, 2017).

A német szabályozás szerint az intelligens fogyasztásmérőknek nagyon szigorú biztonsági feltételeknek kell megfelelniük, amelyek célja a fogyasztásmérő infrastruktúra biztonsági szintjének növelése. Vannak azonban más szolgáltatások vagy eszközök is, amelyek széleskörű

ellenőrzési lehetőségek (pl. okostelefonos alkalmazások), amelyek jelenleg nem szabályozottak (Expert-Workshop 2, 2017).

### **b. Elosztott energiaforrások**

Egy szakértő által említett összetettebb probléma abból adódik, hogy a végfelhasználók prosumerek, azaz energiatermelők, miközben egyszerre fogyasztják a saját maguk által termelt és a hálózat által szállított energiát. Korábban a klasszikus villamosenergia-rendszerben a termelési, átviteli és elosztási rendszereket vállalatok üzemeltették, és elszigetelt rendszerként kezelték őket. Az elosztott energiaforrások rendszereinek a hálózathoz való csatlakoztatása, amelyeket a végfelhasználók tartanak fenn és birtokolnak, azonban áthidalja azt a légrést, amely korábban lehetővé tette a kiberbiztonság bizonyos szintjének elérését. A probléma akkor merül fel, amikor ezek az elosztott rendszerek nem biztonságos hálózatokhoz vagy az internethez kapcsolódnak. Ennek következtében feltételezni kell, hogy a rendszer potenciálisan nem biztonságos végpontokhoz csatlakozik, ezért a hagyományos biztonsági intézkedések, például a hitelesítés vagy az engedélyezés nem lesznek elegendők (14. interjúalany, személyes közlés, 2017).

A kis méretű DER-rendszerek nem rendelkeznek kötelező előírásokkal e rendszerek biztosítására, ezért potenciális pontot jelentenek a rosszindulatú behatolások számára (Interjúalany 2, személyes kommunikáció, 2016).

### **c. Termelés, átvitel és elosztás**

Az állomás- és terepi zónák végpontjait (lásd a 4. ábrát) gyakran távoli telepítési helyszíneken telepítik, ahol nincs üzemeltető vagy karbantartó személyzet. Ezért, ha az ezeken a helyszíneken lévő végberendezések nem rendelkeznek megfelelő biztonsági intézkedésekkel, egy potenciális támadónak ideje lehet arra, hogy megpróbálja kompromittálni a nem biztonságos eszközöket (számítógépeket vagy hálózati eszközöket), bejutni a hálózatba, és onnan támadást indítani (5. interjúalany, személyes közlés, 2016).

Még az ipari létesítmények (pl. erőművek, átviteli alállomások) belsejében található végpontok is veszélybe kerülhetnek, amelyek általában zárt helyek. Az ipari automatizálás informatikai biztonságával foglalkozó szakértők megemlítették, hogy azok a pontok, ahol a felhasználók kapcsolatba léphetnek a rendszerrel, szintén gyenge pontokat jelentenek, mivel a felhasználó vagy a kezelők módosíthatják vagy manipulálhatják a konfigurációs paramétereket vagy a vezérlőparancsokat. Az RTU-k és a PLC-k hajlamosak az ilyen jellegű stresszforrásokra (15. interjúalany, személyes kommunikáció, 2017).

Továbbá a rendszerek vagy eszközök távoli hozzáférési képességei is jelenthetnek potenciális rosszindulatú behatolási pontokat. Amint azt az egyik interjúalany említette, a távoli hozzáférés önmagában nem jelent bizonytalanságot, mivel ha van egy biztonságos csatorna, megfelelő intézkedésekkel a

helyen lehetséges az olyan támadások felderítése, mint a lehallgatás vagy a "man-in-the-middle". Problémát jelenthet azonban, ha az egyik végpont potenciálisan nem biztonságos (14. interjúalany, személyes közlés, 2017). Ha például vírussal vagy rosszindulatú szoftverrel fertőzött laptopokat használnak távoli karbantartási célokra, vagy egyidejűleg nem biztonságos hálózatokhoz (pl. az internethez) csatlakoznak, ezek a végpontok veszélyeztethetik a rendszert (Expert-Workshop 1, 2016).

#### 4.1.2.2 Támadási mechanizmusok és stresszorok

Ha a végkészüléket kompromittálják, a támadónak nem kell feltörnie a titkosítást ahhoz, hogy az adatokat kiolvassa vagy manipulálja. A különböző SGAM-tartományokban különböző támadási mechanizmusok hajthatók végre:

##### **a. Fogyasztás**

A fenyegető ügynökök rosszindulatú kódokat vagy rosszindulatú szoftvereket tölthetnek fel az ügyfeleknél lévő, rosszul védett automatizálási eszközökre, hogy azokat irányítsák, és szolgáltatásmegtagadási támadásokat indíthassanak az energiarendszer vagy más infrastruktúrák, például banki rendszerek ellen (Interviewee 1, személyes közlés, 2016; Interviewee 5, személyes közlés, 2016).  
közlemény, 2016).

Az ügyfeleknél elhelyezett intelligens fogyasztásmérők fizikai manipulációs támadások célpontjai lehetnek, bár jelenleg ezek az eszközök ellenállóak. Ezek a támadások általában speciálisabbak, például az információk lehallgatására irányuló oldalcsatornás támadások (18. interjúalany, személyes közlés, 2017). A SPIDER kutatási projekt keretében elvégezték az intelligens mérőátjárók kiegészítő fenyegetéselemzését, ahol további fenyegetéseket fedeztek fel, amelyek többsége a manipulációs és szolgáltatásmegtagadási, az integritást és a rendelkezésre állást érintő biztonsági szempontok közé tartozik, lásd (Becker, 2013), idézi (Detken, Genzel, Hoffmann, Hoffmann, et al., 2014).

##### **b. Elosztott energiaforrások**

Egy másik lehetséges támadási mechanizmus lehet a DER rendszerelemek adatmanipulációja (2. interjúalany, személyes kommunikáció, 2016). A DER-hez sokféle digitális eszközre van szükség, hogy szabályozni lehessen a működésüket, és hogy a fogyasztók és a közműszolgáltatók információkat kapjanak a működésükről. A legtöbb DER intelligens invertereket és DER-vezérlőket tartalmaz; mások akkumulátorvezérlőket és akár elektromos járműveket (EV) vezérlőket is tartalmazhatnak. Ha a támadók közvetlenül hozzáférhetnek ezekhez a rendszerekhez, akkor képesek lesznek manipulálni bármelyik vezérlő funkciójukat,

vagy meghamisítani az állapotinformációkat a közműszolgáltatók vagy a tulajdonosok számára (Qi et al., 2016).

**c. Termelés, átvitel és elosztás**

A villamosenergia-hálózat állomás- és mezőzónáiban lévő ICS végpontok ellen fellépő egyes támadási mechanizmusokat többnyire emberi mulasztás vagy félrekonfigurálás okozza. Az üzemeltetési paraméterek szándékos manipulálása is előfordulhat. A vezeték nélküli interfésszel rendelkező eszközök egy másik támadási vektort jelenthetnek, amely a villamos rendszer működése felé terjedhet (18. interjúalany, személyes közlés, 2017).

A hálózatra csatlakoztatott USB flash meghajtók szintén felhasználhatók rosszindulatú programok telepítésének belépési pontjaként (1. interjúalany, személyes kommunikáció, 2016; 18. interjúalany, személyes kommunikáció, 2017). A (helyi vagy távoli) karbantartási szervizelés során a technikusok saját laptopon keresztül létesíthetnek kapcsolatot, amely vírusokkal vagy más rosszindulatú szoftverekkel fertőzött lehet, amelyek átterjedhetnek az ipari hálózatra (Expert-Workshop 1, 2016).

Az ügyfél telephelyén végrehajtott támadási forgatókönyvekhez hasonlóan a rosszul védett ipari vezérlőrendszerek, amelyek például egy internetre csatlakoztatott, de tűzfal nélküli vagy nem megfelelően konfigurált ipari vezérlőrendszerrel rendelkező alállomáson találhatók, veszélybe kerülhetnek, és egy botnet-kampány részévé válhatnak, ami szolgáltatásmegtagadási támadásokat okozhat. Egy másik támadási forgatókönyv szerint ezeket az ipari vezérlőrendszereket kriptográfiai kulcsok feltörésére vagy bitcoin bányászatra használhatják, akárcsak a hálózati nyomtatók esetében. Ezt a forgatókönyvet azonban néhány IT-biztonsági szakértő valószínűtlennek tartja (1. interjúalany, személyes közlés, 2016).

Az adatmanipulációt a felső zónákban is el lehet végezni a SGAM, pl. az üzemeltetés vagy a vállalat (lásd a 4. ábrát) adatbázis-kiszolgálókkal szemben (pl. SCADA historikus szerver), ahol az adatokat konszolidálják és jóváhagyják. A minőségi biteket vagy magát az adatot is lehetne manipulálni, és ennek következtében a HMI-n az irányítóközpontban megjelenített információk (pl. frekvencia) eltérnének attól, ami a terepen történik (4. interjúalany, személyes közlés, 2016).

#### 4.1.2.3 A rendszer szolgáltatásaira gyakorolt lehetséges hatások

##### **a. Fogyasztás**

A kompromittáló IoT-eszközök felhasználhatók a felhasználók elleni zsarolóvírus-támadásokhoz. Egy jövőbeli forgatókönyv szerint, ha valaki feltöri az intelligens otthoni környezetet, a támadó egy pénzüsszeget követelhetne a világítás, a fűtés, az autó akkumulátorának töltése stb. vezérlésének felszabadításáért. (18. interjúalany, személyes közlés, 2017). Továbbá, közvetett potenciális hatásként az új technológia

---

nyilvános elfogadottságát befolyásolhatja a tárgyak interneteivel kapcsolatos valamennyi, a fogyasztói világban felmerülő és a médiában megjelenő biztonsági probléma (5. interjúalany, személyes kommunikáció, 2016).

Az ügyfél telephelyén elhelyezett intelligens mérőkapuk manipulálhatók az energiafogyasztás csökkentése érdekében (1. interjúalany, személyes közlés, 2016; 6. interjúalany, személyes közlés, 2016; 18. interjúalany, személyes közlés, 2016). kommunikáció, 2017; 19. interjúalany, személyes kommunikáció, 2017). Ez azonban értelmetlen lenne, ha a támadó csak egyetlen átjárót tudna befolyásolni. Egy támadó számára érdekes lenne egyszerre több átjárót is kikapcsolni trójaiak vagy más rosszindulatú programok segítségével, hogy nagyobb hatást érjen el (Interviewee 19, 2017). Nagyobb hatást lehetne elérni, ha egy fenyegető ügynök képes lenne kompromittálni az intelligens mérőátjárók rendszergazdájának informatikai infrastruktúráját, hogy a biztonságos kommunikációs csatornát használja, és megtámadhassa az SMGA-hoz csatlakoztatható több millió átjárót (Interviewee 19, személyes közlés, 2017).

Ami az SMGW-nek a háztartást a villamos hálózatról leválasztó funkcióját illeti, Greveler, U., in (Greveler, 2016) megemlítette, hogy a szabályozható fogyasztókon kívül a kapu védelmi profilja nem biztosít olyan funkciót, amely leválasztja a háztartást a villamos hálózatról. Egy ilyen funkció különleges kockázatot hordoz, hiszen egy, az átjáró elleni sikeres támadás jelentős hatással lenne az egyes fogyasztókra (szinte valamennyi elektromos eszköz funkciójának elvesztése), valamint az elektromos hálózatra (sok háztartás hirtelen lekapcsolása esetén a hálózatok esetleges kaszkádszerű lekapcsolása).

## **b. Elosztás Energiaforrások**

Az intelligens inverterek feletti közvetlen irányítást biztosító támadások különösen veszélyesek lehetnek, mivel a támadás a hálózat állapota alapján intelligensen manipulálhatja az eszköz működését. Ez segíthet a támadónak a nemkívánatos hálózati állapotok felerősítésében (Qi et al., 2016). Egy szakértő spekulatív hibaforgatókönyvként említette, hogy abban az esetben, ha egy fenyegető ágens képes lenne elegendő decentralizált energiatermelőt, például PV-rendszereket manipulálni és egyszerre kikapcsolni, ez a hálózat instabilitásához és bizonyos potenciális áramkimaradásokhoz vezethetne, mivel maga a hálózat nem lenne képes kompenzálni a veszteséget (17. interjúalany, személyes közlés, 2017). Mint említettük, ez egy spekulatív hibaforgatókönyv, amely a potenciális hatás értékeléséhez több kvantitatív elemzést igényel.

## **c. Termelés, átvitel és elosztás**

Az állomáson és a mezőzónákban a végpontok a fentiek szerint potenciális veszélyeknek vannak kitéve. Azonban több erőfeszítést és elosztott támadást igényel ahhoz, hogy nagyobb hatást gyakoroljon a teljes rendszerre. Az irányítási rendszer

architektúrája szerint minél magasabb szintű az architektúra, annál kritikusabbá válik,  
mivel az információ

egy adott rétegre vonatkozó adatokat az összes alatta lévő rétegből gyűjtik össze. Ezért a legalacsonyabb szinten, azaz az állomás- és terepi zónákban (lásd a 4. ábrát) az ipari berendezések működési határérték-paramétereinek manipulálása nem járna nagy hatással a teljes rendszerre, de más hatásokhoz vezethet, például a berendezés fizikai integritására. Ha például a maximális munkaterhelés paraméterét módosítják, és így a készüléket a fizikai határértékek túllépésére kényszerítik, ez olyan fizikai károsodást eredményező meghibásodásokat eredményezhet, amelyek hatással lehetnek az adott rendszer teljesítményére (1. interjúalany, személyes közlés, 2016; 4. interjúalany, személyes közlés, 2016).

kommunikáció, 2016; 15. interjúalany, személyes kommunikáció, 2017).

Egy nagyobb támadási forgatókönyvben, ha egy alállomást megtámadnak és kikapcsolnak, akkor az alállomás által lefedett területen, például egy utcában vagy egy háztömbben áramkimaradás következik be. Emellett egy ilyen támadás hatással lehet a németországi energiaelosztás általános minőségére, ami közvetve érintheti a közmuvelőszolgáltatókat, mivel a referenciaértékek alapján kapnak fizetést, és ezek a kiesések gazdasági hatást jelenthetnek számukra (1. interjúalany, személyes közlés, 2016). Ahhoz, hogy nagyobb kiesés legyen, sok alállomásnak kellene egyszerre veszélybe kerülnie (Interjúalany 1, személyes közlés, 2016).

#### 4.1.2.4 Potenciális hatás értékelése

A fent említett lehetséges hatásoknak megfelelően a mennyiségi és minőségi kritériumokat különböző támadási mechanizmusok befolyásolhatják. A minőségi kritériumokra gyakorolt hatás nagyobb lesz, ha egyidejűleg elosztott támadásokat hajtanak végre. A nyilvános elfogadottságot is befolyásolná. Ezért a potenciális hatást közepesnek vagy magasnak kell értékelni.

#### 4.1.2.5 Alkalmazkodási stratégiák és végrehajtás

Általánosságban elmondható, hogy a végponttól végpontig tartó biztonság megvalósítása kihívást jelent. Ahogy egy IT-biztonsági szakértő megállapította: "Valószínűleg nem reális vagy naiv azt gondolni, hogy minden végpontot biztosítani tudunk. De biztosítanunk kell, hogy a biztonsági résről gyorsan tudomást szerezzünk." A biztonság javításának nagyon fontos követelménye a biztonsági képességek beépítése az eszközökbe a hitelesítés, a használat engedélyezése és az ellenőrzés tekintetében. Ezen felül fontos a javításkezelési folyamatok bevezetése, beleértve a tesztelést is, a szoftver és a hardver hibáinak kezelésére. A támadások megelőzése és elszigetelése érdekében hálózati szegmentációra és felügyeletre is szükség van (5. interjúalany, személyes kommunikáció, 2016).

Az egyes klaszterekre vonatkozó konkrét alkalmazkodási mechanizmusok a következők:

**a. Fogyasztás**

Ha a rendszer jobban elosztott, több biztonsági intézkedésre van szükség, továbbá iránymutatásokra és végrehajtási referenciákra, amelyek támogatják az eladókat az intézkedéseknek az ügyfelek telephelyén lévő eszközökön, pl. IoT-eszközökön történő végrehajtásában. Továbbá a nyílt szoftver lehetővé tenné a biztonsági közösség támogatását (5. interjúalany, személyes kommunikáció, 2016).

Azonban, mint már említettük, a 100%-os biztonságot nem lehet garantálni. Ezért ezeket az elosztott eszközöket nem megbízhatónak kell tekinteni, és ellenőrizni kell a bemeneteiket. Ezeket statisztikai eszközökkel kellene elemezni annak kimutatására, hogy ezek az eszközök manipulált vagy rosszindulatú információkat küldenek-e vagy sem. Szükség lehet például az ügyfeleknél telepített intelligens mérőórák méréseinek elemzésére annak biztosítása érdekében, hogy azok nem befolyásolják rosszindulatúan a hálózatot. Ez az elemzés azonban adatvédelmi szempontból is aggályos lehet. Vannak módszerek a mérési mérések aggregálására a háztartási szintek helyett a szomszédság szintjén, de ezek a technikák titokmegosztási sémákat vagy bármilyen más kriptográfiai protokollt vagy megoldást igényelhetnek. Ezért ezeket a technikákat be kell vetni, és meg kell találni az egyensúlyt a közműszolgáltató által érzékelt granularitás és az ügyfelek magánélete, valamint a rendszer általános biztonsága között (13. interjúalany, személyes közlés, 2017).

Az intelligens fogyasztásmérőkből érkező támadások megelőzése érdekében azok képességeit csak a leolvasási funkciókra kell korlátozni, de a vezérlési funkciókat nem szabad engedélyezni. Így kevésbé lesznek kitéve a támadásoknak (Expert-Workshop 2, 2017). Továbbá, mint fentebb említettük, a nagyobb hatás eléréséhez sok intelligens mérőórát vagy intelligens mérőátjárót kellene kompromittálni. Tekintettel arra, hogy egy SMGA körülbelül egymillió átjáróhoz csatlakozhat, nagymértékben megköveteli, hogy az SMGA-t hitelesíteni kell, ami Németországban jelenleg kötelező előírás (19. interjúalany, személyes közlés, 2017).

Az SMGA biztonságának növelése érdekében a Detken K. és munkatársai által kidolgozott munka (Detken, Genzel, Hoffmann, et al., 2014; Detken, Genzel, Rudolph, et al., 2014) a Trusted Computing megközelítés releváns aspektusainak használatát javasolja, mint például: az integritás mérése és ellenőrzése a Trusted Network Connect (TNC) segítségével. Ez a biztonsági koncepció egy bizalmi lánc létrehozásával felel meg a biztonsági követelményeknek. Az integritás ellenőrzése először a rendszerindításkor kerül alkalmazásra, a biztonságos rendszerindítás felhasználásával és a bizalmi lánc létrehozásával, beleértve a TNC szoftvert is. Az integritás ellenőrzése futásidőben is történik, a (bootoláskor) ellenőrzött TNC-szoftver felhasználásával. A hardver- és szoftverkomponensek mért értékeit a fájlrendszerben

hamisításbiztosan tárolják. EZ fejlett átjáróbiztonságot eredményez, amely minden szomszédos komponensre hatással van.

## **b. Elosztott energiaforrások**

Ami a DER-rendszerek biztonságának javítását illeti, a szakértők megemlítették, hogy a Németországban hamarosan bevezetésre kerülő intelligens mérési infrastruktúrát is fel lehetne használni e rendszerek biztosítására. Bár jelenleg nem ez a cél, és további szabályozások kidolgozására lenne szükség (17. interjúalany, személyes közlés, 2017).

## **c. Termelés, átvitel és elosztás**

Olyan megelőzési mechanizmusok, mint a rossz adatok felismerésére szolgáló rendszerek vagy adatszűrők használhatók. Az ellenőrző rendszereket általában úgy tervezik, hogy a terepről érkező adatok egy része hibás vagy téves lehet, ezért a szükséges adathalmazt túlbecsülik, ami lehetővé teszi a hibás adatok elvetését. Az említett, fizikai modelleken (pl. áram vagy feszültség, Ohm és Kirchhoff törvénye alapján) alapuló észlelési rendszerek alkalmazása lehetővé teszi a terepről érkező adatok további validálását (4. interjúalany, személyes közlés, 2016; 12. interjúalany, személyes közlés, 2016).

közlemény, 2017).

Ezen észlelési mechanizmusok megvalósítása a rendelkezésre álló adatok mennyiségére korlátozódna. A szakértők egyetértettek abban, hogy az átviteli szinten több adat áll rendelkezésre, mint az elosztási szinten, ahol jelenleg nem sok mérőeszköz van, ami kihívást jelent az ilyen észlelési rendszerek megvalósítása szempontjából (12. interjúalany, személyes közlés, 2017).

Továbbá az ipari útválasztók és kapcsolók jobb elemzési és észlelési képességeinek megvalósítása javítani fogja az ipari vezérlőrendszerek biztonságát, hogy képesek legyenek felismerni és megelőzni a terepi eszközökről érkező támadásokat. A jelenlegi ipari hálózatok azonban csak alapfunkciókkal rendelkeznek, ezért korszerűsítéseket vagy új hálózati eszközöket kell fontolóra venni (15. interjúalany, személyes közlés, 2017).

### **4.1.2.6 Alkalmazkodóképesség minősítés**

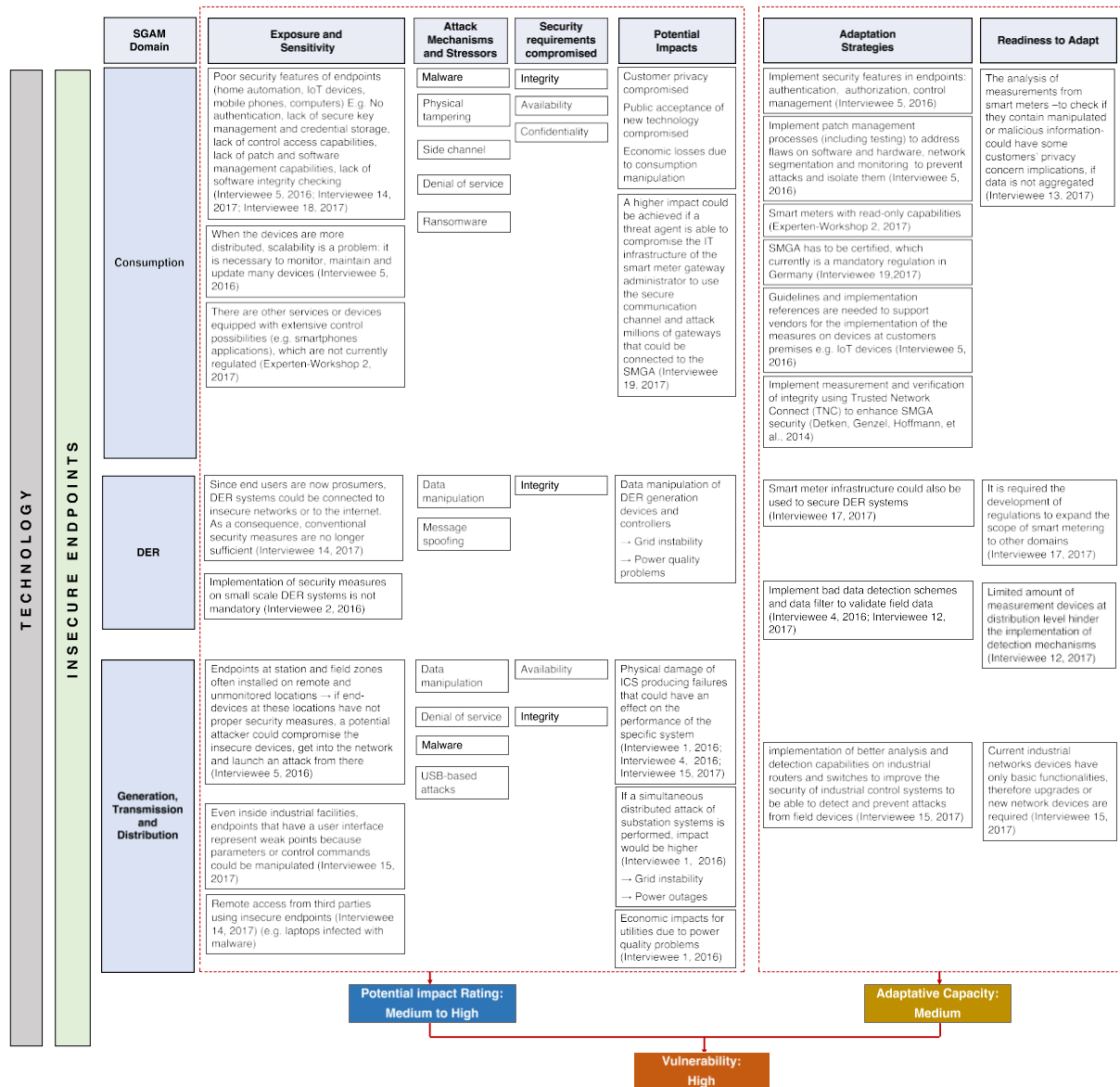
A megelőzésre néhány adaptációs stratégiát adtunk meg. Ezek végrehajtása azonban korlátozott lesz a további költségeket jelentő technikai követelmények vagy további szabályozási keretek kialakítása miatt. Ezért az alkalmazkodási képességet közepesre értékelték.

### **4.1.2.7 Sebezhetőségi besorolás**

Tekintettel a nagy potenciális hatás és a közepes alkalmazkodóképesség kombinációjára.

Ebben az esetben a sebezhetőségi besorolás magas.

A 14. ábra összefoglalja a nem biztonságos végpontok miatti sebezhetőségi értékelést.



14. ábra A kiberfizikai energiarendszerek sebezhetőségének értékelése a nem biztonságos végpontok miatt. Az értékeléshez a villamosenergia-rendszer SGAM-tartományait három csoportba soroltuk: (a) fogyasztás, b) elosztott energiaforrások, c) termelés, átvitel és elosztás. Forrás: A szerzők saját ábrázolása

### 4.1.3 Egyéb technológiával kapcsolatos feltételek

Az interjúk tartalomelemzése során a következő további, technológiával kapcsolatos feltételeket azonosítottuk. Az idő rövideje miatt azonban nem lehetett átfogó sebezhetőségi értékelést végezni.

- Bizonytalan interfész a különböző gyártóktól származó komponensek vagy különböző rendszerek között
- Engedélyezett, de nem engedélyezett szoftver- és firmware-módosítások
- Webszolgáltatásokban futó rendszerek, például virtuális erőművek

## 4.2 Szervezeti biztonsági irányelvek és eljárások

### 4.2.1 Az interdiszciplináris IT-OT ismeretek hiánya

#### 4.2.1.1 Expozíció és érzékenység

A villamosenergia-rendszerek IT és OT (üzemeltetési technológia) infrastruktúrája közötti összetettség és kölcsönös függőségek számának növekedésével az új kiber-fizikai rendszerek kezeléséhez szükséges tudás megváltozott. A két infrastruktúra közötti kapcsolatokat sajátos módon kell vizsgálni és védeni, ami nehéz a csak az egyik területen jártas szakértők számára. Az interdiszciplináris tudás a legtöbb esetben hiányzik, ezért nehéz az új rendszerek egészét megfelelően megérteni, megtervezni, megvalósítani és üzemeltetni (1. interjúalany, személyes közlés, 2016; 2. interjúalany, személyes közlés, 2016; 5. interjúalany, személyes közlés, 2016).

Az energiaágazatban különböző érdekelt felek vesznek részt, nevezetesen a hagyományos nagyméretű nyersanyagszolgáltatók, az elosztóhálózat-üzemeltetők, a tipikus fogyasztók, a feltörekvő kistermelők, a mérési szolgáltatók, az informatikai komponensek fejlesztői/szolgáltatói, valamint számos szabályozó és szabványosítási intézmény. E felek többsége nem rendelkezik komoly háttérrel az IT-biztonság terén (von Oheimb, 2013). Ráadásul a pályázati eljárások során a szakértelem hiánya mindkét infrastruktúrában hibákhoz vagy a biztonsági követelmények átfogó leírásának hiányához vezethet, ezért a megvalósított rendszerek nem tudnak megfelelni a minimális követelményeknek (18. interjúalany, személyes közlés, 2017).

Az egyik terület szakértői egyszerűen nem látják előre döntéseik következményeit és következményeit a rendszer más területeire és részeire nézve. Például egyrészt, ha az informatikai részleg az OT-üzemeltetéshez használt szervereket (pl. HMI, történész szerver) az IT-infrastruktúra részének tekinti, a szokásos IT-biztonsági intézkedések (pl. napi vírusirtó-frissítések) következményekkel járhatnak a rendszer üzemeltetési részére, ami kihat a rendszer rendelkezésre állására vagy teljesítményére (4. interjúalany,

személyes közlés, 2016). Másrészt

az OT-hálózat jelentős részét informatikai eszközök és rendszerek kötik össze, tartják fenn és működtetik. Általában ezeket az eszközöket inkább az ICS-üzemeltetők és mérnökök, mint tapasztalt IT-szakemberek tartják karban, ami gyakori hibákat eredményezhet a karbantartás, a konfiguráció és a keményítés hiánya terén (Bodungen et al., 2017).

Ezen túlmenően az IKT folyamatban lévő bevezetése a villamosenergia-üzemeltetési rendszerbe új kihívásokat jelent a rendszer működtetése szempontjából. Ahogy egyre több IKT-funkciót integrálnak a villamosenergia-rendszerekbe, az üzemeltetési személyzetnek több képzésre lenne szüksége ahhoz, hogy tudja, hogyan kell kezelni a kiber-fizikai eseményeket. A szakértők szerint ezekhez az új rendszerekhez képzett operátorokra van szükség, akiket kifejezetten arra képeznek ki, hogy ne csak a rendszer meglévő elektrotechnikai részeit, hanem az új informatikai biztonsági rendszereket, pl. a behatolást/anomáliákat észlelő rendszereket is kezelni tudják. Az üzemben lévő személyzetet nem lehet rövid időn belül átképezni informatikai szakértővé, hogy tudja, hogyan kell megfelelően reagálni az informatikai hibákra (Interjúalany 1, személyes közlés, 2016).

Egyrészt az üzemirányító központok általában nem integrálják az IKT-infrastruktúrából érkező hibákat vagy riasztásokat, ezért az üzemeltető nem tudja megkülönböztetni a hiba eredetét (1. interjúalany, személyes kommunikáció, 2016; 18. interjúalany, személyes kommunikáció, 2017). Másrészt, ha az informatikai részleg kezeli az anomália-érzékelő rendszereket és az IDS-eket, nem világos, hogy az informatikából származó bármilyen stresszor hogyan juthat el az üzemeltetési központba, hogy az reagáljon rá (18. interjúalany, személyes kommunikáció, 2017).

#### 4.2.1.2 Támadási mechanizmusok és stresszorok

Az informatikai és a szervezeti egységek szakértőinek hiánya számos lehetőséget nyit a támadók számára, hogy többféle módon is kárt tegyenek a rendszerben. Az ICS védelmének különböző megközelítései az IT és OT intézkedésekből biztonsági réseket hoznak létre, például: nem megfelelő hálózati szegmentáció, nem megfelelő változás- és konfigurációkezelés, gyenge helyi/távoli hozzáférés-ellenőrzés, a jelszavak gyenge generálása, használata és védelme stb.

Ha a rendszert nem megfelelően tervezték meg, mert nem ismerik a rendszer sérülékeny részeit, az újonnan hozzáadott szoftverek és firmware-ek nem megfelelő felülvizsgálata problémákat okozhat a rendszer stabilitásában. A nem megfelelő javításkezelés és az informatikai biztonsági intézkedések végrehajtása szintén károsíthatja a rendszert, mivel a rendszer általános kialakítása túlságosan összetetté válik, és a rendszereket sebezhetővé teszi a támadásokkal szemben. A biztonsági hiányosságokat vagy a

biztonsági intézkedések tervezésében és végrehajtásában elkövetett hibákat a támadók kihasználhatják a rendszer kompromittálására.

Egy támadási forgatókönyv kihasználhatja az üzemeltetők IT-OT-szakértelmének hiányát is, amikor a fenyegető ügynökök hibákkal és riasztási jelzésekkel árasztják el az irányítóközpontokat, hogy összezavarják a nem interdiszciplinárisan képzett üzemeltetőket, és a rendszer áttekinthetőségének elvesztéséhez vezetnek. A oldal provokálása.

kritikus hibák, vezérlési hibák és helytelen vezérlőparancsok, amelyek aztán a rendszer fizikai károsodásához vezethetnek (4. interjúalany, személyes közlés, 2016).

#### 4.2.1.3 Potenciális hatások

A kiberinfrastruktúra eszközeire vonatkozó nem megfelelő biztonsági intézkedések végrehajtása nem szándékolt következményekkel járhat a fizikai infrastruktúrára nézve, ami viszont hatással lehet a rendszer teljesítményére és stabilitására.

Az informatikai és OT-szakértelemmel rendelkező személyzet hiánya egyaránt hatással lesz a rendszer működésére. Amikor az OT-vel kapcsolatos informatikai incidensek vagy események történnek, nem lehet reagálni rájuk. A megfelelő képzéssel nem rendelkező üzemeltetők nem tudják megkülönböztetni a műszaki hibákból vagy természeti veszélyekből eredő, illetve a célzott támadásból eredő hibaüzeneteket. Ha nem tudják megfelelően és a valós problémának megfelelően kezelni a rendszert, akkor a rendszer teljesítménye is sérülhet (4. interjúalany, személyes közlés, 2016).

#### 4.2.1.4 A lehetséges hatások minősítése

Az interdiszciplináris ismeretek hiánya miatt nem megfelelő biztonsági intézkedések végrehajtása veszélyeztetheti az adatok hozzáférhetőségét, ami közvetlen hatással lehet a műszaki paraméterekre. A biztonsági hiányosságok kihasználása rendszerhibákhoz és áramkimaradásokhoz is vezethet. Ezért a VA módszertana szerint a lehetséges hatások a közepestől a nagyig terjednek.

#### 4.2.1.5 Alkalmazkodási stratégiák és végrehajtás

Alkalmazkodási stratégiaként a szakértők több szakértői tudás áthidalását követelik az IT és az OT között, hogy segítsék ezeket az ágazatokat egymás megértésében és a konfigurációs hibák vagy a nem megfelelő biztonsági intézkedések végrehajtásának elkerülésében (13. interjúalany, személyes közlés, 2017). A keresztmetszeti és interdiszciplináris területekre vonatkozó több szakértelem birtokában az iparágat saját komplexitásának jobb megértése és a rendszerarchitektúra holisztikus szemléletének kialakítása felé lehet nevelni (6. interjúalany, személyes kommunikáció, 2016; 17. interjúalany, személyes kommunikáció, 2017). Ez a szemlélet a különböző összetevők és területek közötti kapcsolatokra és kölcsönhatásokra összpontosítana.

Több keresztmetszeti együttműködéssel jobb biztonsági méréseket és rendszerterveket lehet kidolgozni, amelyek figyelembe veszik az IT és az OT közötti összetettséget és kölcsönös függőséget, és ami még fontosabb, a kritikus működési követelményeket, azaz az időzítést és a rendelkezésre állást. A biztonsági felelősségek meghatározása és értékelése a fejlesztési és üzemeltetési fázistól kezdve segít a konkrét követelmények

kezelésében (9. interjúalány, személyes közlés, 2017).

A meglévő iránymutatások egységesítése és megosztása a különböző területek között hasznos lehet az iránymutatások elkészítéséhez, hogy azokat szélesebb körben lehessen használni az érintett területeken és a rendszerben érintett különböző szereplők számára (18. interjúalany, személyes közlés, 2017).

Az üzemeltetéshez specifikusabb képzésre van szükség, csak a képzett és tapasztalt kezelők képesek megérteni a konkrét hibákat, és képesek felmérni azok hatását. Ennek megfelelően fognak reagálni, és hiba esetén is képesek működtetni a rendszert, míg a nem megfelelően képzett kezelők az alkatrészek károsodását kockáztathatják (4. interjúalany, személyes közlés, 2016). Továbbá IT- és OT-szakértőkből álló csapatokban kell dolgozniuk, hogy a rendszer bármilyen jellegű hibájára jobban tudjanak reagálni (19. interjúalany, személyes közlés, 2017).

A meglévő személyzet interdiszciplináris ismereteinek bővítését célzó képzési és oktatási programok vagy a szakemberek felvétele azonban a kapcsolódó költségek miatt akadályokba ütközhet (9. interjúalany, személyes közlés, 2017).

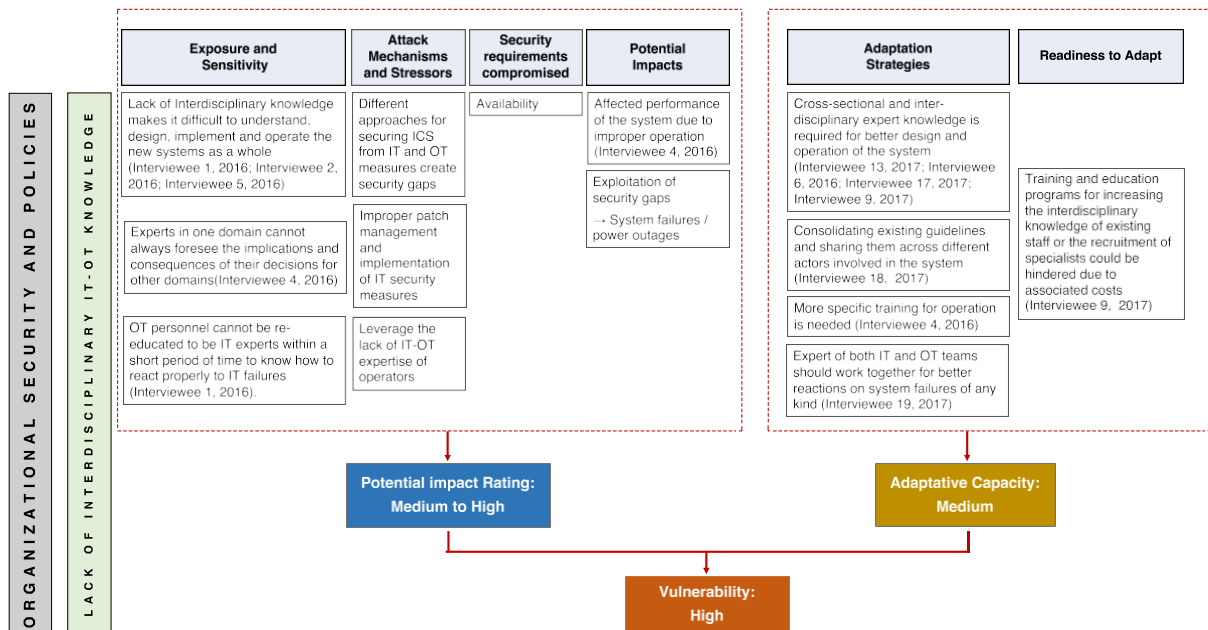
#### 4.2.1.6 Alkalmazkodóképesség minősítés

A szakértők említették az alkalmazkodási mechanizmusokat, azonban - ahogyan egyikük is említette - a meglévő személyzet interdiszciplináris ismereteinek bővítését célzó képzési programok végrehajtása vagy a szakemberek felvétele a kapcsolódó költségek miatt akadályokba ütközhet. Emiatt az alkalmazkodási képességet közepesre értékelték.

#### 4.2.1.7 Sebezhetőségi besorolás

Tekintettel a nagy potenciális hatásokra és a közepes alkalmazkodóképességre, ebben az esetben a bizonytalan kommunikáció miatti sebezhetőséget magasra kell értékelni.

A 15. ábra összefoglalja az interdiszciplináris IT-OT ismeretek hiánya miatti sebezhetőségi értékelést.



15. ábra A kiber-fizikai energiarendszerek sebezhetőségének értékelése az interdiszciplináris IT-OT ismeretek hiánya miatt. Forrás: A szerzők saját ábrázolása

## 4.2.2 Nem megfelelő biztonsági javítások kezelése

### 4.2.2.1 Expozíció és érzékenység

A szoftver/ firmware javításokat egyes esetekben nem ellenőrzik rendszeresen a frissítésük biztosítása érdekében. A nem megfelelő biztonsági javítások kezelésének következményei a szabványos IT-hálózatokban a legutóbbi globális kibertámadások, például a "WannaCry" során váltak nyilvánvalóvá. Ez a támadás elkerülhető vagy mérsékelhető lett volna, ha a vállalati és kormányzati informatikai osztályok megfelelő módon hajtották volna végre a rendelkezésre álló biztonsági javításokat, és több mint 10 éves operációs rendszereket frissítettek volna.

A szakértők egyetértettek abban, hogy az internetre csatlakozó rendszerek legalább heti, sőt napi szintű biztonsági javításokat igényelnek a biztonsági szint fenntartása érdekében. A szervezetek és a végfelhasználók azonban időnként nem látják be, hogy szükség van elavult operációs rendszereik és hálózati elemeik foltozására.

Az ipari vezérlőrendszerek esetében a szakértő azt állította, hogy ezek a rendszerek általában nem jól foltozottak, vagy azért, mert a gyártók nem biztosítanak biztonsági javításokat az eszközeikhez, vagy azért, mert az adott rendszer kritikus a működés szempontjából, és nem lehet kikapcsolni a biztonsági intézkedések alkalmazása érdekében. Ennek következtében a biztonsági réseket nem foltozzák megfelelően, és a rendszerek ki vannak téve a rosszindulatú behatolásoknak.

#### 4.2.2.2 Támadási mechanizmus és stresszorok

A fenyegető ágensek egy ismert, még nem javított biztonsági rést kihasználva férhetnek hozzá különböző rendszerelemekhez. A rosszindulatú programokat telepíteni lehet, és arra lehet használni, hogy helyettesítsenek vagy bármilyen funkciót hozzáadjanak egy eszközhöz vagy rendszerhez, például érzékeny információk küldésére vagy eszközök vezérlésére (Mo et al., 2012).

#### 4.2.2.3 Potenciális hatások

Attól függően, hogy milyen rendszerterületen sérült meg a javítatlan szoftver vagy firmware, a lehetséges hatások eltérőek lehetnek.

Például a NESCOR katalógusban szereplő AMI.25 hibaforgatókönyv leírja a mérőrendszerekben lévő, javítatlan tűzfalon keresztül történő támadás lehetséges hatásait. Ez az állapot lehetővé teszi a fenyegető ágens számára, hogy leállítsa az AMI fejtövet, ami kieséseket okozhat, mivel a közműszolgáltató nem képes csúcsidőben a keresletre való reagálást megvalósítani (NESCOR, 2015).

Ha a támadás az elosztó alállomások ipari vezérlő firmware-eit célozza meg, a fenyegető ágens képes lehet átvenni az alállomás irányítását, és lekapcsolni az elosztóhálózat áramkimaradásokat okozó szegmenseit. Az áramkimaradások mértéke a megtámadott alállomások számától függ (1. interjúalany, személyes közlés, 2016).

Továbbá a nem megfelelő javításkezelés vagy a javítási folyamat hibája a javítandó rendszerelemek rendelkezésre állását is befolyásolhatja, ami áramkimaradásokat okozhat. (lásd az AMI.28-as hibaforgatókönyvet a (NESCOR, 2015) című dokumentumban).

#### 4.2.2.4 A lehetséges hatások minősítése

A fenti részletes elemzés alapján a mennyiségi és minőségi kritériumok a támadási mechanizmusoktól és a támadás célterületétől függően változhatnak. A minőségi kritériumokra gyakorolt hatás nagyobb lesz, ha egyidejűleg elosztott támadásokat hajtanak végre. Ezért a rendszerre gyakorolt lehetséges hatások a közepestől a nagyig terjedő kategóriába sorolhatók.

#### 4.2.2.5 Alkalmazkodási stratégiák és végrehajtás

A szakértők megemlítették, hogy a megfelelő javítás-kezelés elengedhetetlen a technológiai fejlődéssel való lépéstartáshoz és az internet-hozzáféréssel rendelkező rendszerek biztosításához. A menedzsmentnek tartalmaznia kell a sebezhetőségek foltozásának súlyosságát és időkereteit (NESCOR, 2015).

Az ipari vezérlőrendszerek, különösen a SCADA rendszerek rendszeres foltozása azonban kihívást jelent, mivel ezek a rendszerek időkritikusak. Mivel nincs tesztkörnyezet, a foltozás új, ismeretlen sebezhetőségeket vezethet be, vagy végül tönkretelheti a rendszert (Cherdantseva et al., 2015). A szakértők a következők bevezetését javasolják

redundáns rendszerek a leállások elkerülése érdekében. Ennek az intézkedésnek az alkalmazása azonban a rendszer általános kialakításától függ, és a kapcsolódó többletköltségek akadályozhatják.

Még ha naprakészek is vagyunk az összes javítással és enyhítéssel, az ismeretlen nulladik napi kihasználások és a be nem jelentett sebezhetőségek széles körben elterjedtek (McLaughlin et al., 2015).

Egy másik megoldás, ahogyan azt néhány interjúalany említette, a kötelező előírások bevezetése lenne, hogy növeljék a tudatosságot és a hajlandóságot a megfelelő javítások és frissítések végrehajtására.

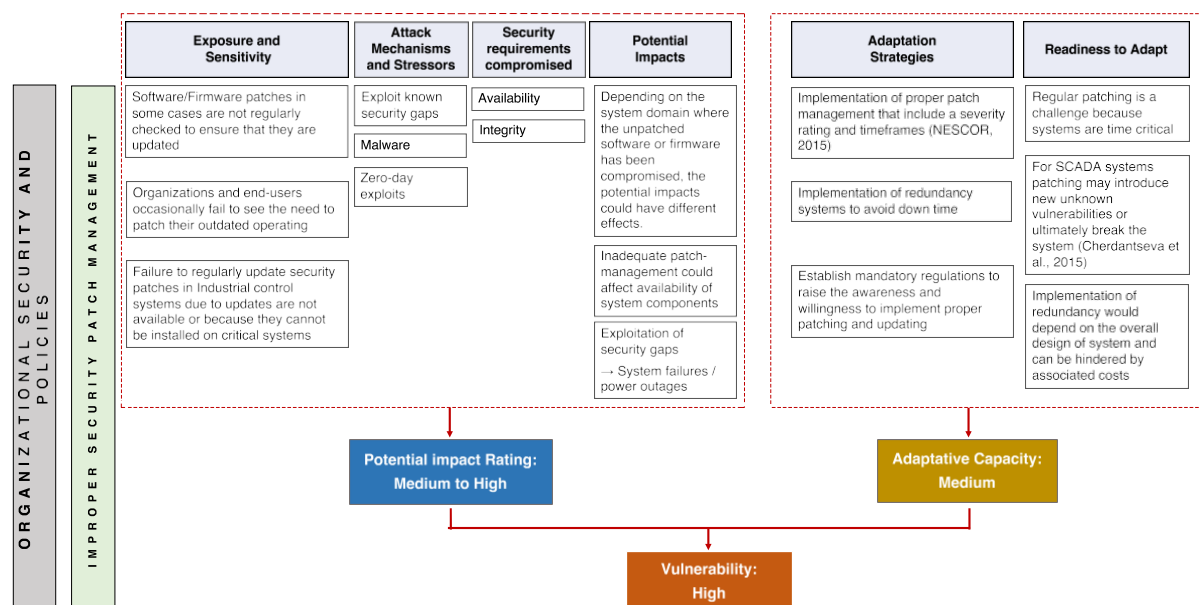
#### 4.2.2.6 Alkalmazkodóképesség minősítés

A fent leírt megfontolások alapján a VA szerint az alkalmazkodóképesség közepesnek minősül.

#### 4.2.2.7 Sebezhetőségi besorolás

Tekintettel a nagy potenciális hatásokra és a közepes alkalmazkodóképességre, a sebezhetőséget ebben az esetben magasnak kell minősíteni.

A 16. ábra összefoglalja a nem megfelelő biztonsági javítások kezelése miatti sebezhetőségi értékelést.



16. ábra A kiberfizikai energiarendszerek sebezhetőségének értékelése a nem megfelelő biztonsági javítások kezelése miatt. Forrás: A szerzők saját ábrázolása

## 4.3 Az emberi tényező

### 4.3.1 A biztonságtudatosság hiánya vagy a biztonsági irányelvekre való gyenge reagálás a szervezeten belül.

#### 4.3.1.1 Expozíció és érzékenység

A megfelelő biztonsági képzési és tudatossági programok hiánya egy energiaszektorbeli szervezetben, pl. a termelő erőművek, az elosztó és átviteli üzemeltetők stb. esetében nem megfelelően képzett személyzethez vezethet, amely véletlenül biztosíthatja a külső vagy belső stresszorok számára a láthatóságot, a tudást és a lehetőséget egy sikeres támadás végrehajtásához (NIST, 2014).

Egyrészt az informatikai szakértők szerint a social engineering az egyik leggyorsabban növekvő biztonsági probléma. Ez a támadási mechanizmus lehetővé teszi, hogy a fenyegető ügynök kihasználja a minden szervezetben jelen lévő egyik gyenge pontot: az emberi tényezőt. Ebben az esetben a személyzetet külső fenyegető ügynökök manipulálhatják, hogy segítsenek nekik hozzáférni a belső rendszerhez vagy támadást végrehajtani. A nem megfelelően képzett munkaerő nem lesz tisztában a szervezeti információk és berendezések védelméhez szükséges irányelvekkel és eljárásokkal, ami a gyenge pontok kihasználásának lehetőségét eredményezi, például: rosszindulatú USB-stickeket behelyezése a vállalati vagy operatív hálózatban lévő gépekbe, gyanús, gyakran nulladik napi exploitokat tartalmazó weboldalak böngészése, vagy az azonosító jelvényekkel való gondatlanság, amelyekkel részleges vagy teljes hozzáférést lehet szerezni a kritikus rendszerekhez (NIST, 2014). Továbbá a rendszerkonfigurációra vagy -architektúrára vonatkozó kritikus információk nyilvánosan hozzáférhetővé válhatnak a szállítók vagy eszközök, tulajdonosok weboldalán, az alkalmazottak közösségi médiaoldalain keresztül. A potenciális fenyegető ügynökök ezeket az információkat felhasználhatják a támadás megtervezéséhez.

Másrészt a további potenciális fenyegető tényezők közé tartoznak az elégedetlen, nagy bűnözési vagy rosszindulatú viselkedési potenciállal rendelkező alkalmazottak, illetve a volt alkalmazottak, akiket távozásukkor nem kezeltek megfelelően (4. interjúalany, személyes közlés, 2016). Ők magas szintű ismeretekkel rendelkeznek a rendszerekről és hozzáféréssel a kritikus funkciókhoz vagy érzékeny adatokhoz (pozíciójuktól függően), ezért képesek lehetnek azonosítani a lehetséges gyenge belső struktúrákat és módszereket, hogy támadást hajtsanak végre, súlyos károkat okozva a rendszerben.

A szervezet számos tanulságot szerzett a kiberfenyegetésekről a vállalati IKT-területén, és a személyzetet tudatosítják és kiképzik e fenyegetések felismerésére. Az ICS-üzemeltetők, mérnökök és más külső érintett szereplők azonban, mint például: ICS-

---

szállítók, rendszerintegrátorok, vállalkozók és karbantartó személyzet nem rendelkezik kiberbiztonsági képzéssel és oktatással (Luijff, 2016). Amint azt az informatikai biztonsági szakértők megállapították, az állomási zónában (lásd az intelligens hálózat architektúráját (IEC, 2020)) a legtöbb támadás vagy emberi

hiba, félrekonfigurálás vagy social engineering. Míg az üzemeltetési, vállalati és piaci zónák hálózatai általában tűzfalakkal, VPN-ekkel, IDS-ekkel és felügyeleti rendszerekkel vannak biztosítva, az állomás zóna rendkívül sebezhető az emberi tényezővel szemben (1. interjúalany, személyes közlés, 2016).

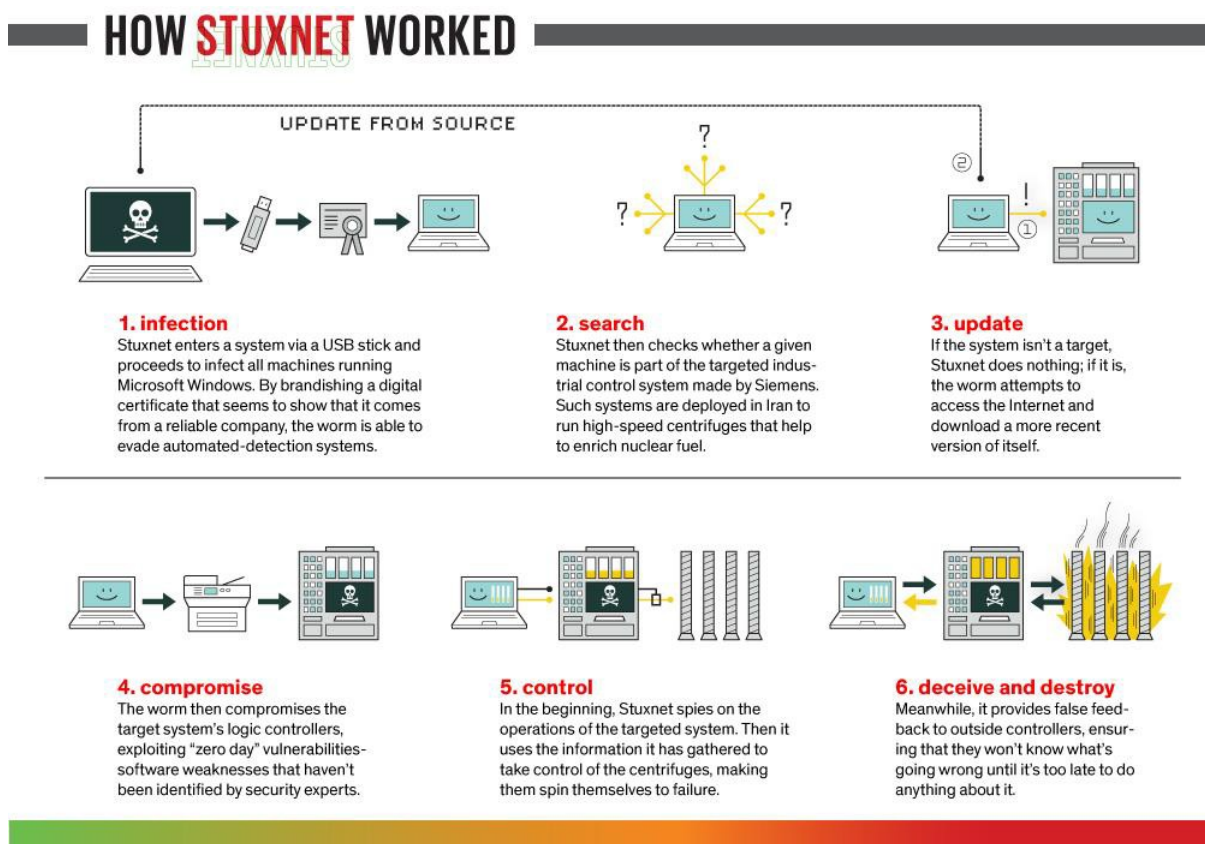
#### 4.3.1.2 Támadási mechanizmusok és stresszorok

A social engineering segítségével a fenyegető ügynökök új támadási mechanizmusokat fedeznek fel, amelyek a szervezet különböző szintjeit célozzák meg. A "spear phishing" például az egyik támadási mechanizmus, amikor külső fenyegető ügynökök rejtett rosszindulatú kódot tartalmazó e-maileket küldenek az alkalmazottnak, hogy megfertőzzék a létesítmény hálózatát. A 2015-ös ukrainai esetben a fenyegető ügynökök kifejlesztettek egy rosszindulatú programot ("*Blackenergy 3*"), és fegyverré alakított dokumentumokat készítettek, hogy a rosszindulatú programot e-mailben juttassák el. A rosszindulatú dokumentumokat csatolmányként tartalmazó e-maileket egy adathalászkampány keretében küldték el a szervezeten belüli embereknek. A fenyegető szereplők sikeresen telepítették a rosszindulatú programot, miután az alkalmazottak megnyitották a fegyveresített e-mail mellékleteket. A rosszindulatú program tartalmazott beépülő szoftvert a rendszer hozzáférési hitelesítő adatok gyűjtéséhez és a belső hálózaton történő felderítő tevékenység végzéséhez. Az ellopott hitelesítő adatok felhasználásával a fenyegető ügynökök hozzáfértek az ipari vezérlőkörnyezethez, és összetett műveletsort hajtottak végre (Styczynski és Beach- Westmoreland, 2017).

Egy másik módja a periméter áttörésének az USB-alapú támadások. Az USB-perifériák vonzó eszközzé váltak a kibertámadások indításához, ahol a fenyegető ügynökök kihasználják a felhasználókat, akik hajlamosak ezeket a perifériákat lazán használni, feltételezve, hogy biztonságosak, holott valójában beágyazott rosszindulatú hasznos terhet hordozhatnak, amelyet támadások indítására lehet használni (Nissim et al., 2017). Az USB-eszközök felhasználhatók bizonyos ICS-célpontok, például PLC-k (programozható logikai vezérlők) megtámadására is, amint azt a híres "Stuxnet" rosszindulatú szoftver is bizonyította az iráni urándúsító létesítmény Natanz külvárosában lévő centrifugái ellen. Ebben az esetben a fenyegető ügynökök közvetett módon, fertőzött mobil eszközökön és USB-stickeken keresztül szivárogtak be olyan vállalkozóktól, akik törvényes hozzáféréssel rendelkeztek a létesítmény legkritikusabb rendszeréhez (Langner, 2013). A Stuxnet féreg egy példátlanul összetett kód volt, amely három szakaszban támadott. (1) Először a Microsoft Windows gépeket és hálózatokat vette célba, többszörösen replikálva magát. Kompromittált digitális tanúsítványok segítségével a Stuxnet képes volt megkerülni a tűzfalakat, miközben tovább terjedt a SCADA-rendszer helyi kommunikációs hálózataiban. A Stuxnet peer-to-peer kommunikációs képességei

lehetővé tették a kártevő számára, hogy frissítse magát, még akkor is, ha a fertőzött eszköz nem rendelkezett közvetlen hozzáféréssel az internethez. (2) Ezután megkereste a Siemens Step7 szoftverét, amely szintén Windows-alapú, és amelyet PLC-k programozására használnak. (3) Végül, miután a célzott PLC-t megfertőzte, a Stuxnet megváltoztatta a működési módját. A PLC rootkit segítségével a rosszindulatú program módosította a PLC kódját, hogy közzétételi támadást hajtson végre, és rögzítse a kapott adatokat. Miután az adatok rögzítése néhány

a Stuxnet a fizikai rendszer megzavarásával szabotálni kezdte a rendszert. Miközben a Stuxnet megváltoztatta az aktuátorokhoz küldött vezérlőjelet, az üzemben okozott károkat úgy rejtette el, hogy a korábban rögzített adatokat a SCADA felügyeleti rendszereibe táplálta (Knapp, 2011; Kushner, 2013; New Jersey Cybersecurity & Communications Integration Cell, 2017). A 17. ábra a Stuxnet támadási forgatókönyvét szemlélteti.



17. ábra: A Stuxnet működése. Forrás (Kushner, 2013)

A bennfentes fenyegetések által végrehajtott támadásra példa a máltai intelligens fogyasztásmérők manipulálása. Az állami tulajdonú Enemalta energiaszolgáltató munkatársai kenőpénz ellenében mintegy 1000 intelligens mérőórát manipuláltak, és azokat a magas áramfogyasztású ügyfeleknél helyezték el. Az okosmérőket úgy konfigurálták, hogy akár 75 százalékkal kevesebb energiafogyasztást rögzítsenek, mint amennyit valójában fogyasztottak. A mérőórát a plombák vagy védőmechanizmusok feltörése nélkül manipulálták. Bizonyíték volt arra, hogy a mérőket más ügyfelek úgy manipulálták, hogy nagyobb áramfogyasztást mérjenek, hogy egy körzet teljes fogyasztását állandó értéken tartsák, és a csalást leplezzék (BSI, 2015b).

#### 4.3.1.3 Potenciális hatások

A veszélyeztetett adatok relevanciájától vagy a célzott felhasználó jogosultságaitól függően a lehetséges hatások különböző mértékűek lehetnek. Az információk kiszivárgása révén egy fenyegető ügynök jogos hitelesítő adatokat szerezhet a kritikus rendszerekhez való hozzáféréshez. Ha egy támadó áthatol egy rendszeren, akkor lehetséges lenne a SCADA-rendszer infrastruktúrájának (pl. az adattörténész szerverének) veszélyeztetése. Ha a helyzetet súlyosbítja a vállalati és az ipari vezérlőhálózat nem megfelelő elkülönítése, a fenyegető ügynök átveheti az ellenőrzést a terepi eszközök felett, és helytelen vagy káros üzemirányítási műveleteket hajthat végre, amelyek ismeretlen időtartamú kieséseket vagy az ICS-eszközök közvetlen fizikai károsodását okozzák. Továbbá a támadás nemcsak az áramelosztást zavarná meg, hanem az informatikai rendszereket is tönkretenné, elárasztaná a hívásközpontokat és gátolná az incidensek elhárítását, mint a 2015-ös ukrainai támadás esetében (Styrcynski és Beach- Westmoreland, 2017).

Az intelligens mérőinfrastruktúra esetében az intelligens mérőátjáró-adminisztrációs (SMGA) létesítmények informatikai infrastruktúrájának veszélyeztetése lehetővé tenné a fenyegető ügynök számára, hogy a biztonságos kommunikációs csatornán keresztül közel egymillió intelligens mérőátjárót támadjon meg, például kikapcsolva azokat, ami a hálózat instabilitását és esetleges áramkimaradásokat okozna (19. interjúalany, személyes közlés, 2017).

A NESCOR katalógus (NESCOR, 2015) további lehetséges társadalmi tervezésből eredő hatásokat mutat be a következő területeken: mérési infrastruktúra (lásd AMI.3, AMI.9), átvitel (lásd WAMPAC.4), elosztás (lásd DGM.10) és termelés (lásd GEN.4, GEN.9).

#### 4.3.1.4 Potenciális hatások minősítés

Figyelembe véve a minőségi és mennyiségi kritériumokat egyaránt érintő lehetséges hatások körét, ebben az esetben a rendszerre gyakorolt lehetséges hatások közepes és magas közötti értéket kapnak.

#### 4.3.1.5 Alkalmazkodási stratégiák és végrehajtás

A szakértők szigorúbb kötelező biztonsági intézkedéseket javasolnak a különböző szervezeti szinteken a social engineering elleni küzdelem érdekében. Az üzemeltetőket és az adminisztratív személyzetet ki kell képezni, hogy tisztában legyenek a rendszert veszélyeztető körülményekkel. (pl. rossz jelszókezelés, nem megfelelő levélmelléletek kezelése, azonosítatlan USB-meghajtók stb.) A dolgozókat be lehetne vonni a social engineering gyakorlatokba, ahol a vállalat által generált adathalász leveleket kapnak, vagy elhelyezett hamis USB-meghajtókat találnak, hogy megtanulják, hogyan kell

*vizsgálat eredményei*  
megfelelően reagálni a szociál engineering támadások veszélyére. A biztonsági képzéseket és a biztonságtudatosági programokat a munkatársak minden egyes tagjához a beosztásuknak megfelelően kell igazítani. A programnak tartalmaznia kell egy meghatározott időszakon át tartó folyamatos átképzési erőfeszítést, hogy tükrözze az új

eljárások, új technológiák, valamint a kiberbiztonsági program fontosságának megerősítése (ENISA, 2012; NIST, 2014). Emellett az új alkalmazottak személyes háttérellenőrzését is javítani kell, hogy az ICS-hez operatív vagy adminisztratív hozzáféréssel rendelkező valamennyi alkalmazottat megfelelően átvilágítsák (ENISA, 2016).

Nagyobb tudatosságra és hajlandóságra lenne szükség a humán erőforrás, a vezetés, az informatikai osztály és a szabályozó hatóságok összehangolt erőfeszítéseikhez, hogy a szervezetek szigorú biztonsági politikáiban állapotodjanak meg. Mindazonáltal a biztonsági politikák és a képzési programok végrehajtási költségei akadályozhatják a jóváhagyást, és korlátozhatják a bevezetett biztonsági szintet, amint azt egy szakértő megállapította. A biztonsági intézkedések alkalmazását a munkavállalók elkötelezettségi szintje is korlátozhatja.

#### 4.3.1.6 Alkalmazkodóképesség minősítés

Tekintettel arra, hogy az alkalmazkodási stratégiák adottak, de alkalmazásuk az érintett szereplők hajlandóságától függ, az alkalmazkodási képességek közepesnek minősülnek.

#### 4.3.1.7 Sebezhetőség minősítés

A VA módszertana szerint a nagy potenciális hatás és a közepes alkalmazkodóképesség kombinációja magas sebezhetőségi besorolást eredményez.

A 18. ábra összefoglalja a biztonsági tudatosság hiánya vagy a szervezeten belüli biztonsági irányelvekre való gyenge reagálás miatti sebezhetőségi értékelést.

18. ábra A kiberfizikai energiarendszerek sebezhetőségének értékelésének összefoglalása a biztonságtudatosság hiánya vagy a szervezeten belüli biztonsági irányelvekre való gyenge reagálás miatt. Forrás: A szerzők saját ábrázolása

## 4.3.2 A biztonságtudatosság hiánya a fogyasztók körében

### 4.3.2.1 Expozíció és érzékenység

A végfelhasználók a rendszer egy másik sebezhető pontját jelentik. A fogyasztók részéről a tudatosság hiánya vagy az alacsony biztonság következményeinek nem megfelelő megértése veszélyeztetheti az energiarendszert. A szakértők megerősítik, hogy a végfelhasználók többsége nem rendelkezik szakértői ismeretekkel az otthoni automatizálási rendszerekről és a tárgyak internetét (IoT) használó eszközökről, így nem tudják, hogyan kell megfelelően biztosítani és karbantartani az intelligens eszközeiket.

A szakértők megemlítették, hogy egyrészt az IoT és az otthoni automatizálási eszközök, különösen a polcra beszerezhető termékek jól ismert biztonsági résekkel rendelkeznek, amelyeket a támadók kihasználhatnak. Másrészt a nem megfelelően foltozott vagy karbantartott végfelhasználói eszközök csatlakozhatnak az otthoni hálózathoz, ami a rendszer sebezhetőségét növeli azáltal, hogy további bizonytalan belépési pontokat ad hozzá.

Egy szakértő által említett összetettebb probléma abból adódik, hogy a végfelhasználók prosumerek, de nem rendelkeznek a megfelelő szakértői ismeretekkel a DER-rendszerek megfelelő biztonsági intézkedéseinek végrehajtásához és fenntartásához.

#### 4.3.2.2 Támadási mechanizmusok és stresszorok

Egy fenyegető ügynök lehallgatással hozzáférhet az ügyfelek adataihoz, és ellophatja a személyes adatokat, beleértve a villamosenergia-felhasználást is, egy olyan tűzfalon keresztül, amely szándékosan vagy akaratlanul közvetlen hozzáférést tesz lehetővé más hálózatokból. A lehallgatáson kívül a fenyegető ügynökök hozzáférhetnek az intelligens fogyasztásmérő eszközökhöz, hogy manipulálják a mérési adatokat, vagy manipulálják az elosztott energiaforrások rendszerparamétereire vonatkozó adatokat. A tárgyak interneteinek eszközeit kompromittálhatják és felhasználhatják elosztott szolgáltatásmegtagadási (DDoS) támadás végrehajtására.

#### 4.3.2.3 Potenciális hatások

A támadási mechanizmustól függően az ügyfél magánéletét felfedhetik, vagy a kommunikációs csatornákat felhasználhatják az adatok manipulálására és helytelen vezérlőparancsok küldésére, ami az energiarendszer instabilitásához és kiesésekhez vezethet.

A DER.2 hibaforgatókönyv a NESCOR katalógusból (NESCOR, 2015) (NESCOR, 2015) azt az esetet szemlélteti, amikor egy nagy DER-rendszer tévesen csatlakozik egy vezeték nélküli vállalati hálózathoz, és így a DER-rendszer ki van téve az internetnek. A fenyegető ágens megszerezheti az irányítást és megváltoztathatja a DER funkcióinak működését. Következésképpen a hálózaton káros fordított energiaáramlást vagy az alállomási transzformátorok túlterhelését tapasztalhatja.

Az AMI nem biztonságos hálózatai vagy néha még a védett hálózatok is lehetőséget kínálnak arra, hogy egy esetleges jogsértés veszélyeztesse az ügyfelek magánéletét, ami az ügyfelek AMI iránti bizalmának elvesztéséhez vezethet.

#### 4.3.2.4 Potenciális hatások minősítés

Tekintettel arra, hogy a biztonsági követelmények: az integritás és a bizalmasság veszélybe kerülhetnek, és ez hatással lehet a minőségi kritériumokra, valamint az energiaellátásra, a fogyasztók biztonságtudatosságának hiánya miatti lehetséges hatások a közepes és a magas közötti értéket képviselik.

#### **Alkalmazkodási stratégiák és végrehajtás**

A potenciálisan nagy következményekkel járó jogsértések megelőzése érdekében az interjúpartnerek azt javasolták, hogy a végfelhasználói oldalon a kiberbiztonsággal kapcsolatos oktatásra van szükség a magasabb biztonsági szint eléréséhez. A saját intelligens rendszereik jobb ismerete növeli a végfelhasználók tudatosságát. Ez lehetővé teszi továbbá a végfelhasználók számára, hogy megfelelően üzemeltessék és

---

karbantartsák a rendszerüket, így saját maguk is képesek lennének bizonyos fokú biztonságot biztosítani. Az otthoni eszközökre és karbantartásukra vonatkozó kötelező biztonsági mérések segítenék az otthoni automatizálási rendszerek minimális biztonságának elérését. Ezek a stratégiák azonban még nem léteznek, és alkalmazásukhoz nem létezik irányelvek érvényesítése.

A magasabb biztonsági szint elérése ellentétes lesz a rövid távú gazdasági logikával, amint azt a szakértők említették. Ezért a legtöbb esetben a magasabb szintű biztonsági intézkedések végrehajtását az ügyfél vagy a fogyasztó oldalán a biztonságért való fizetési hajlandóság fogja korlátozni.

A szakértők szerint továbbá a jelenleg alkalmazott biztonsági intézkedések többsége a rosszindulatú támadókat a rendszeren kívül próbálja tartani, ezért az egyik legnagyobb kihívás az, hogy a kibertámadások megelőzésétől vagy észlelésétől a sikeres támadást követő helyreállítási mechanizmusok felé haladjunk. A jobb megfigyelő és észlelő rendszerekkel együtt ez jobb lehetőségeket kínálna a támadásokra és a manipulált adatokra való reagálásra. Fontos azonban, hogy a több felügyeleti rendszer alkalmazásakor ügyelni kell az ügyfelek magánéletének védelmére.

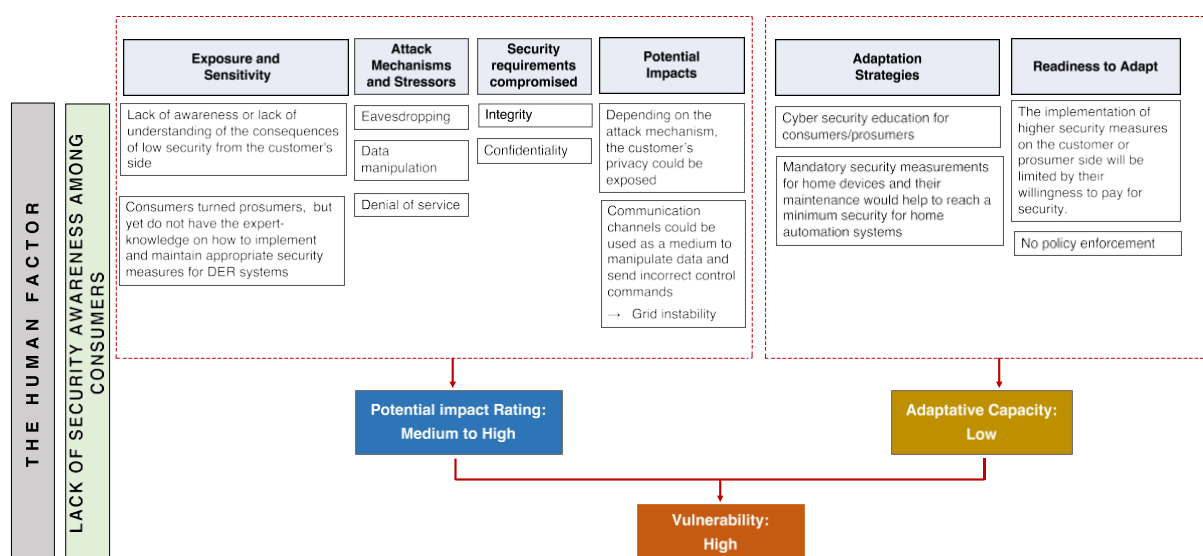
#### 4.3.2.5 Alkalmazkodóképesség minősítés

Tekintettel arra, hogy az említett alkalmazkodási stratégiák még nem kerültek bevezetésre, és hogy a fogyasztók alkalmazkodási hajlandósága korlátozott, a jelenlegi alkalmazkodási kapacitás ebben a kategóriában alacsony.

#### 4.3.2.6 Sebezhetőség minősítés

A VA módszertan szerint a közepes vagy magas potenciális hatások alacsony alkalmazkodóképességgel kombinálva magas általános sebezhetőséget eredményeznek az ügyfél részéről a biztonságtudatosság hiánya miatt.

A 19. ábra összefoglalja a kiberfizikai energiarendszerek sebezhetőségének értékelését a fogyasztók biztonságtudatosságának hiánya miatt.



19. ábra A kiberfizikai energiarendszerek sebezhetőségének értékelése a fogyasztók biztonságtudatosságának hiánya miatt. Forrás: A szerzők saját ábrázolása

## 4.4 Szabályzat

### 4.4.1 A biztonsági szabványok és a szabályozás hatékony végrehajtásának hiánya.

#### 4.4.1.1 Expozíció és érzékenység

Különböző műszaki és szervezeti szabványokat dolgoztak ki az intelligens hálózatok kiberbiztonsági követelményeinek kezelésére. A szakértők szerint azonban ezek az esetek többségében csak ajánlások, és alkalmazásuk nem kötelező.

Az IEC 62351 szabványkészletet például az alállomás-infrastruktúra biztonságára dolgozták ki, és keretet biztosít a szoftveralkalmazások közötti kommunikáció végponttól végpontig tartó biztonságához. Nagymértékben támaszkodik a TLS használatára az energiarendszer különböző támadási mechanizmusok elleni védelme érdekében (International Electrotechnical Commission (IEC), 2007).

Annak ellenére, hogy ez a szabvány biztonsági fejlesztéseket biztosít az olyan protokollok számára, mint például: IEC 61850 (GOOSE, SV és MMS), IEC 60870-5-104 és DNP3, valamint IEC 60870-5-101.

és soros DNP3, a gyakorlatban nem mindig alkalmazzák (Basagiannis et al., 2015; McLaughlin et al., 2015), és a szakértők megemlítették, hogy a gyártók gyakran nem hajtják végre a termékeikben az ajánlott biztonsági intézkedéseket. Az informatikai szakértők úgy vélték, hogy az energiarendszer-üzemeltetőket az előírt minimális biztonsági szabványok végrehajtására kényszerítő kötelező előírások, illetve a szállítóknak a szükséges biztonsági követelmények termékeikben való biztosítására vonatkozó előírások hiánya miatt a rendszer ki van téve a lehetséges kibertámadásoknak.

#### 4.4.1.2 Támadási mechanizmus és stresszorok

Egy fenyegető ügynök kihasználhatja a hitelesítés vagy titkosítás hiánya miatt ismert gyengeségeket bizonyos szabványos protokollokban, jogosulatlanul hozzáférhet a rendszerhez, manipulálhatja és kompromittálhatja a kommunikációs munkameneteket.

A lehetséges stresszorokra találhatunk néhány példát a szakirodalomban a támadásokkal kapcsolatban, mint például: DoS-támadások (Dondossola et al., 2008, 2009) vagy man-in-the-middle (Maynard et al., 2014) az IEC 60870-5 protokollt futtató hálózatok ellen. A (Kush et al., 2014) munkája gyakorlati támadást is bemutatott, a GOOSE (Generic Object Oriented Substation Event) hitelesítés és titkosítás gyengeségeit kihasználva hamisított üzenetekkel, az egyes érvényes üzenetek között helytelen adatokkal.

#### 4.4.1.3 Potenciális hatások

A támadási mechanizmustól függően a hatások eltérőek lehetnek. Például, ha egy

fenyegető ügynök olyan titkosítatlan, egyszerű szöveges SCADA-kereteket (például Distributed Network Protocol 3.0, DNP3) fog el, amelyek értékes információkat, például vezérlési és beállítási információkat tartalmaznak.

intelligens berendezések (IED) esetében a fenyegető ágens képes lehet leállítani az eszköz szolgáltatásait, helytelen parancsokat küldeni és zavarokat okozni (Kush et al., 2014).

#### 4.4.1.4 Potenciális hatások minősítés

Tekintettel az informatikai biztonsági követelményekre, a kompromittálódás az energiarendszer instabilitásához és kiesésekhez vezethet. A VA módszertana szerint a rendszerre gyakorolt lehetséges hatások a középestől a nagyig terjedő kategóriába sorolhatók.

#### 4.4.1.5 Alkalmazkodási stratégiák és végrehajtás

Vannak olyan helyes gyakorlatra vonatkozó iránymutatások, amelyek magasabb szintű biztonsági szabványok alkalmazását javasolják az eszközök kommunikációjának biztosítására, az üzenetek védelmére és az integritás biztosítására az energiarendszerek irányításában és az alállomások automatizálásában. A szakértők szerint azonban ezek nem kötelezőek, és a minimális biztonsági szinteknek való megfelelést a jogszabályok nem kényszerítik ki.

Ezen túlmenően a biztonsági intézkedések végrehajtása érdekében a régebbi rendszerek korszerűsítésére vonatkozó döntés különböző tényezők miatt a következő tervezett életciklusú berendezéscseréig elhúzódhat. A folyamat kritikus szintje vagy a szervezet gazdasági korlátai akadályozhatják az alkalmazást. Következésképpen a jelenleg telepített, örökölt protokollokat használó örökölt eszközök biztosítják, hogy számos sebezhető rendszer marad a területen, és várja, hogy kihasználják őket (Knapp és Samani, 2013).

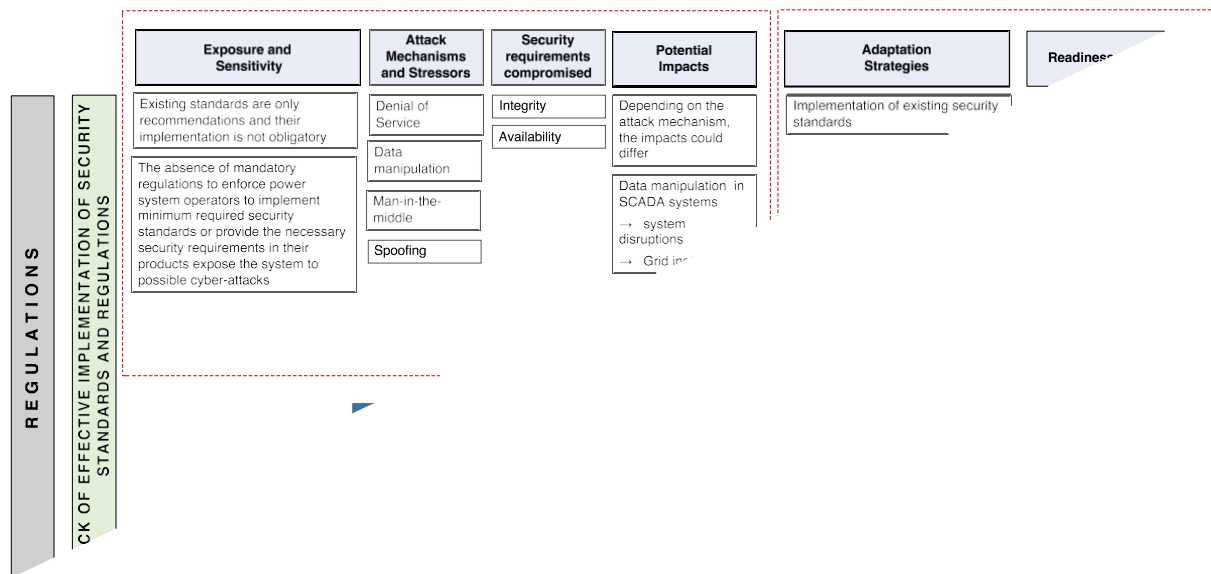
#### 4.4.1.6 Alkalmazkodóképesség minősítés

Tekintettel arra, hogy az intelligens hálózatok biztonságának javítására már léteznek alkalmazkodási mechanizmusok, de az alkalmazásra való hajlandóság korlátozott lehet, az alkalmazkodási képesség közepesnek minősül.

#### 4.4.1.7 Sebezhetőség minősítés

Tekintettel a nagy potenciális hatásokra és a közepes alkalmazkodóképességre, ebben az esetben a sebezhetőséget magasnak kell minősíteni.

A 20. ábra összefoglalja a biztonsági előírások és rendeletek hatékony végrehajtásának hiánya miatti sebezhetőségi értékelést.



20. ábra A kiberfizikai energiarendszerek sebezhetőségének értékelése a biztonsági szabványok és előírások hatékony végrehajtásának hiánya miatt. Forrás: A szerzők saját ábrázolása

#### 4.4.2 A biztonság javítására irányuló összehangolt erőfeszítések hiánya

E kategória esetében az idő rövidege miatt nem került sor a VA-módszertannak megfelelő átfogó értékelésre. Az interjúk elemzésének főbb megállapításait azonban az alábbiakban ismertetjük.

Németország esetében a biztonsági előírások főként az intelligens fogyasztásmérésre és a kritikus infrastruktúrára összpontosítanak. A szakértők azonban megemlítették, hogy hiányzik a hatékony koordináció a teljes rendszer biztonságának javítása érdekében. A német jogszabályok szerint a villamosenergia-hálózat-üzemeltetőknek az IEC/ISO 27001 szabványon alapuló információbiztonsági irányítási rendszert (ISMS) kell létrehozniuk és tanúsítaniuk. Jelenleg azonban<sup>8</sup> nincsenek kötelező előírások a kisméretű DER-rendszerek biztosítására (2. interjúalany, személyes közlés, 2016), amelyek a 4.1. és 4.3.2. szakaszban végzett VA szerint olyan kritikus pontokkal rendelkeznek, amelyeket a fenyegető tényezők kihasználhatnak, jelentős hatást gyakorolva az energiarendszerre.

Hasonlóképpen, az intelligens mérési infrastruktúra esetében a védelmi profilokon (PP) és a műszaki iránymutatásokon (TR-03109) alapuló biztonsági intézkedések nem tartalmaznak előírásokat az egyéb, széleskörű vezérlési lehetőségekkel felszerelt, az otthoni automatizálási hálózathoz csatlakoztatható szolgáltatásokra vagy eszközökre vonatkozóan.

Ezen túlmenően a biztonság javítása az energiatermelés és a hálózatüzemeltetők részéről további gazdasági beruházásokat jelentene, és ezt a fogyasztókra lehetne átruházni a következőkön keresztül

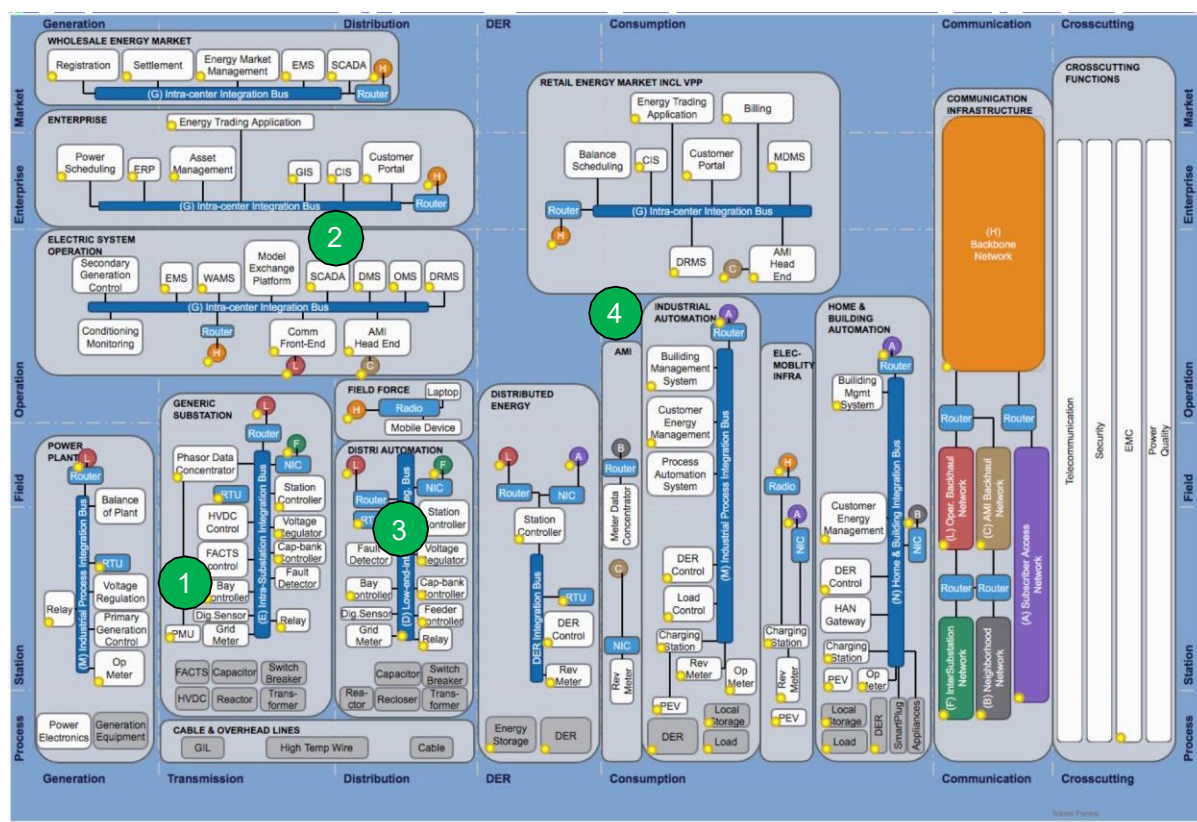
<sup>8</sup> Az interjúk időpontjáig, azaz 2016-ig és 2017-ig.

villanyszámlák. Az energiaágazat egyik szakértője megemlítette, hogy a fogyasztók nem hajlandók magasabb árat fizetni a nagyobb biztonságért. Inkább a legalacsonyabb ár alapján választanak áramszolgáltatót, ezért nem fogadnak el egy olyan új villamosenergia-rendszert, amely nem kínál jelentős közvetlen előnyöket a régi rendszerhez képest (6. interjúalany, személyes közlés, 2016). Az informatikai biztonsággal foglalkozó szakértők kijelentették, hogy az ügyfeleket nem kérdezték meg és nem vonták be az energiaátalakítás folyamatába, és ez a digitalizációs átalakulás esetében is így lehet. Ezért az új technológiák és a kapcsolódó biztonság fontosságával kapcsolatos tudatosság hiánya az ügyfelek részéről akadályozhatja a biztonságosabb energetikai megoldásokba való beruházási hajlandóságot, mivel az ügyfelek nem ismerik a biztonságos energetikai rendszerből származó számos előnyt (Intervjúe 1, személyes kommunikáció, 2016).

## 4.5 Az eseményalapú sebezhetőségi értékelés szemléltetése módszertan

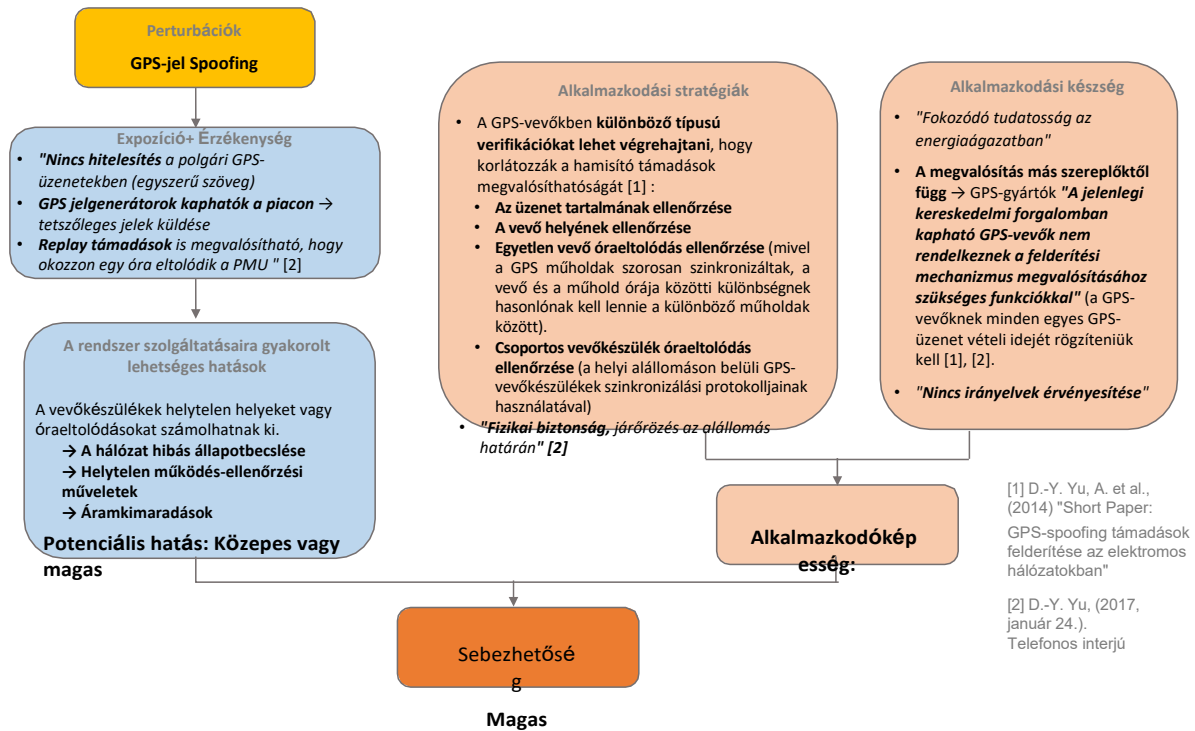
Ez a szakasz példákat mutat be, amelyek az eseményalapú sebezhetőségi értékeléshez használt módszertan alkalmazását szemléltetik. Itt a sebezhetőségi szintet az IKT négy konkrét stresszorára vonatkozóan határozták meg: (1) GPS-jelek meghamisítása, (2) SCADA-rendszerek elleni belső fenyegetés, (3) ICS firmware manipulálása az alállomásokon, és (4) fejlett mérési infrastruktúra adatainak lehallgatása. Ezeket a stresszorokat a szakértők az interjúk során említették, és a tartalomelemzés módszerével azonosították.

Minden egyes stresszor aszerint került kategorizálásra, hogy a villamosenergia-rendszer mely területén és mely rétegében fordulhat elő. A 21. ábra mutatja az egyes stresszorok elhelyezkedését a referenciaarchitektúra-modellen.

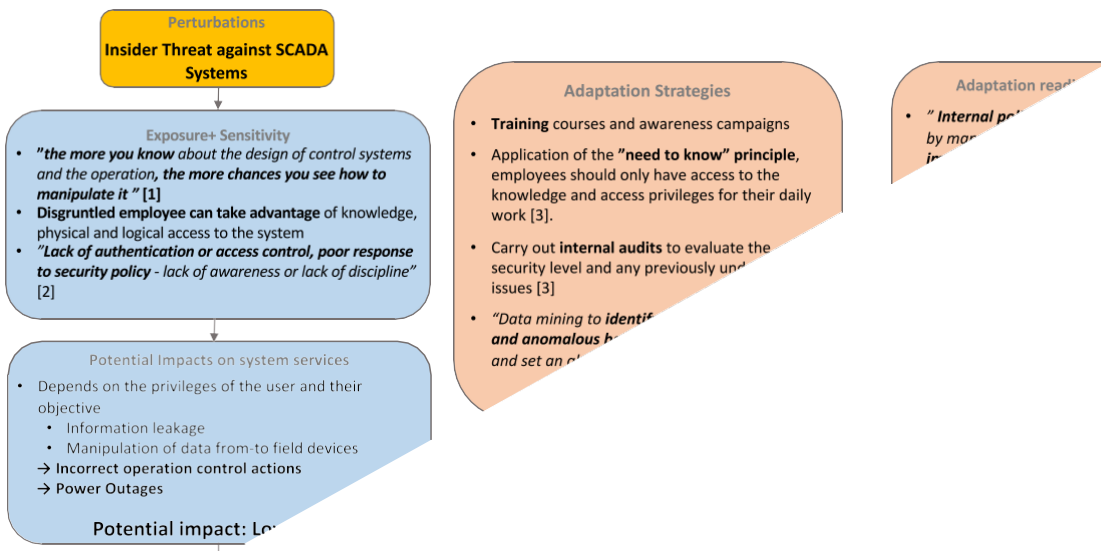


21. ábra A stresszorok referenciaarchitektúra-modelljének elhelyezkedése az eseményalapú VA alkalmazásának példájaként. A stresszorok számozása a következő: (1) GPS-jelek meghamisítása, (2) SCADA-rendszerek elleni belső fenyegetés, (3) ICS firmware manipulálása az alállomásokon, és (4) fejlett mérési infrastruktúra adatainak lehallgatása.

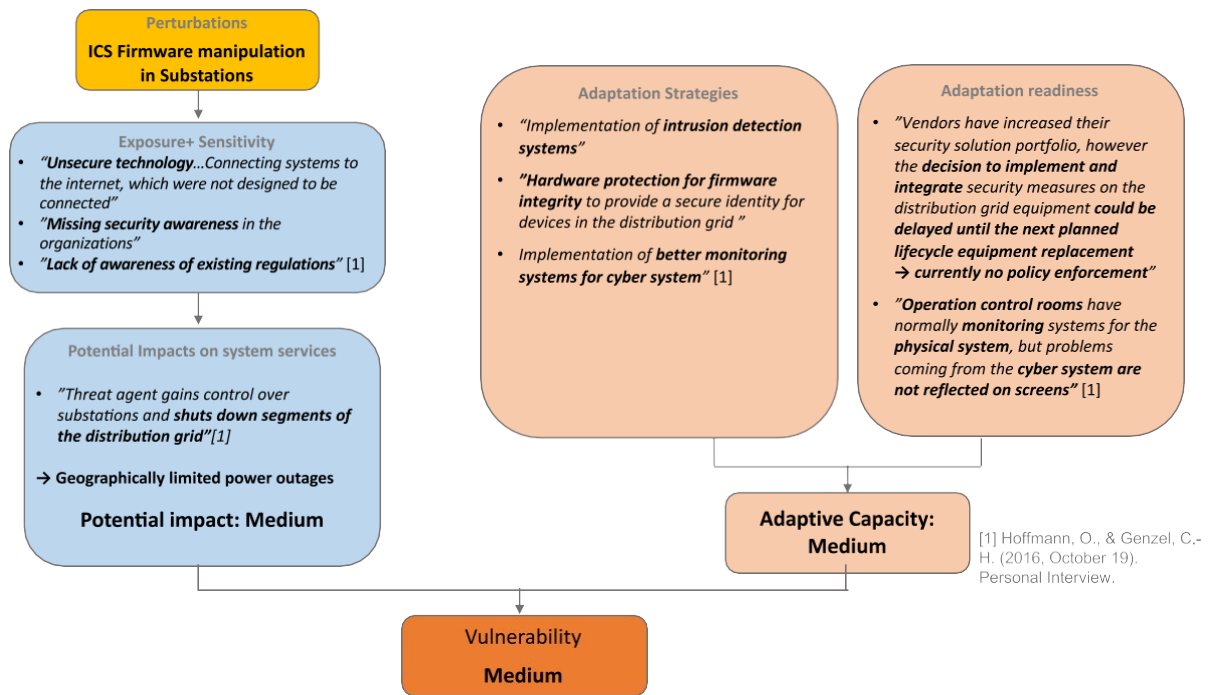
Az EVA módszertant (lásd az 1. ábrát) alkalmazták az egyes stresszorok okozta sebezhetőség értékelésére, és az eredményeket a 22., 23., 24. és 25. ábra mutatja.



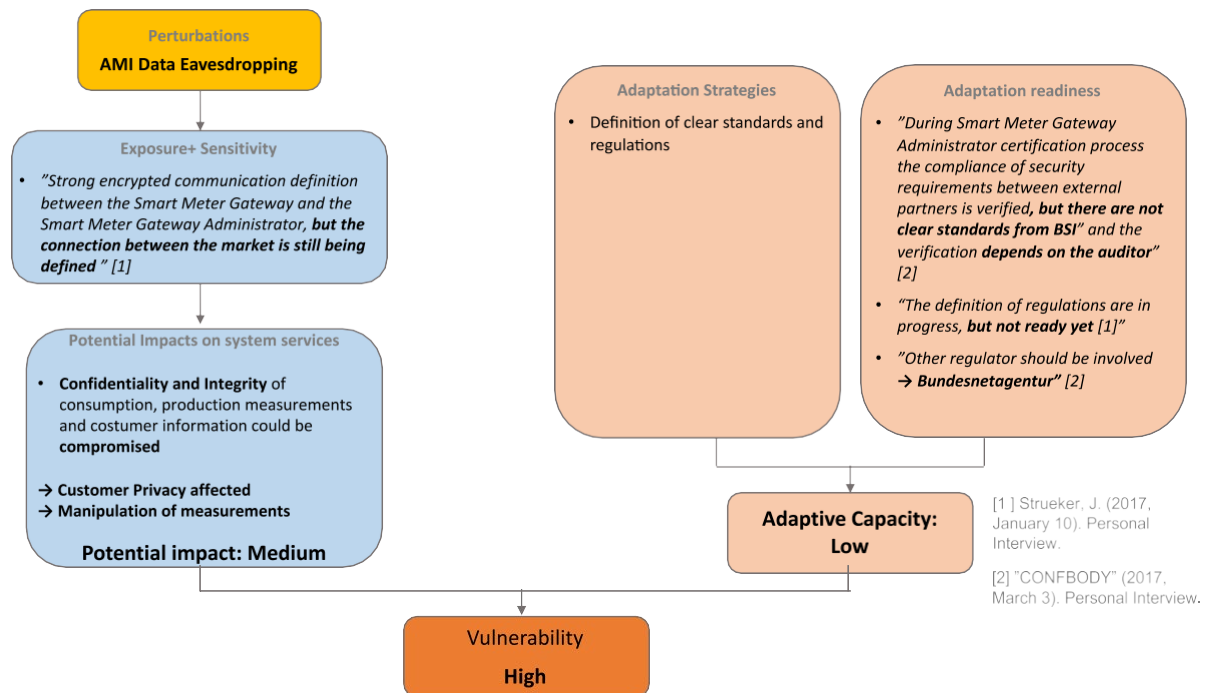
22. ábra A CPPS sebezhetőségének értékelése a stresszor (1) GPS-jel hamisítás miatt. Forrás: Saját ábrázolás.



23. ábra A CPPS sebezhetőségének értékelése a (2) stresszor (SCADA-rendszereken belüli belső fenyegetés) miatt. Forrás: Saját ábrázolás.



24. ábra A CPPS sebezhetőségének értékelése a stresszor (3) ICS firmware manipulálása miatt az állapotásokon. Forrás: Saját ábrázolás



ábra A CPPS sebezhetőségének értékelése a (4) stresszor (Advance Metering Infrastructure data eavesdropping) miatt. Forrás: Saját ábrázolás

## 4.6 Sebezhetőségi értékelés Összefoglaló

A 3. táblázat összefoglalja a sebezhetőségi értékelés eredményeit a fent részletesen ismertetett egyes kategóriák és alkategóriák tekintetében. Amint az értékelés alapján látható, a különböző kategóriákban azonosított összes körülmény sebezhetőbbé teszi a kiberfizikai villamosenergia-rendszert. Az adatbiztonsági követelmények sérülnek, ha a fenyegető tényezők kihasználják az azonosított kritikus pontok közül egyet vagy többet. A támadási mechanizmustól függően ez nemcsak a hálózat instabilitásához vagy áramkimaradásokhoz vezet, hanem a fogyasztók magánéletét is érintheti. Áramkimaradás esetén annak mértéke és időtartama a rendszer felépítésétől függ. Egyrészt a központosított műveletek mindig vonzóbbak a támadók számára, mivel egyetlen hibapontot jelentenek, és egy sikeres támadás széles körű áramkimaradást eredményezhet. Másrészt a cellaszerkezetű, kisebb egységekből álló, elosztottabb architektúra csökkentheti a támadás hatását, mivel ezek képesek önállóan működni és elszigetelni magukat a hálózat meghibásodása esetén.

Annak ellenére, hogy léteznek olyan alkalmazkodási mechanizmusok, amelyek minimalizálhatják a hatásokat, kiderült, hogy ezek végrehajtását akadályozhatja a szakpolitikák végrehajtásának hiánya vagy az érintett szereplők hajlandóságának hiánya ezen intézkedések végrehajtására. Ezért a kihívást a megfelelő szabályozási környezet meghatározása jelenti anélkül, hogy bonyolult eljárásokkal egészítenénk ki, és figyelemmel kell kísérni a hatékony végrehajtást.

*táblázat A kiber-fizikai hatalom kritikus tulajdonságait, struktúráit és elemeit tükröző kategóriák és alkategóriák, valamint a potenciális hatások, az alkalmazkodóképesség és a sebezhetőség megfelelő minősítései az L: alacsony, M: közepes, H: magas skálán.*

Kategória	Alkategória	Potenciális hatások	Alkalmazkodóképesség	Sebezhetőség
Technológia	Bizonytalan végpontok	M-H	M	H
	Bizonytalan kommunikáció	M-H	M	H
Szervezeti biztonsági politikák és eljárások	Helytelen javításkezelés	M-H	M	H
	Az interdiszciplináris IT-OT ismeretek hiánya	M-H	M	H
Az emberi tényező	A biztonságtudatosság hiánya a szervezetekben	M-H	M	H
	A fogyasztók biztonságtudatosságának hiánya	M-H	L	H
Szabályzat	A szabványok és rendeletek hatékony végrehajtásának hiánya	M-H	M	H

	A biztonság javítására irányuló összehangolt erőfeszítések hiánya	M-H	M	H
--	---	-----	---	---

## 5 Rugalmassági menedzsment stratégia

A VA feltárta a kiberfizikai energiarendszerek kritikus sebezhető pontjait. A biztonsági intézkedések alkalmazása esetén nagy lehetőség van egyes sebezhetőségek csökkentésére. Vannak azonban további kihívások. Először is, a biztonsági intézkedések elsősorban arra összpontosítanak, hogy a rosszindulatú támadókat a rendszeren kívül tartsák, és kevésbé összpontosítanak a sikeres támadás utáni helyreállítási mechanizmusra. Másodsorban, az IKT-rendszerek dinamikus jellemzői, valamint a villamosenergia-rendszerekkel való összetett összeköttetések és kölcsönös függőségek miatt nem lehetséges a kibertérből származó, a villamosenergia-rendszert fenyegető összes lehetséges stresszor elemzése. Az ismeretlen természetű, általában "fekete hattyúként" emlegetett további stresszorok, mint például a nem várt informatikai rendszerhibák (pl. hibák, "nulladik napi kihasználások") vagy az innovatívabb és kifinomultabb támadási mechanizmusok (pl. fejlett tartós fenyegetések), valamint ezek ismeretlen gyakorisága (előfordulási valószínűsége) jelentős kihívást jelentenek a megelőző biztonsági módszerek kidolgozásában.

Ilyen bizonytalan, alacsony valószínűségű, de pusztító tendenciájú eseményekre példa a 2017-ben bekövetkezett "WannaCry" zsarolóprogram és a "NotPetya" kibertámadás. Az ukrán energetikai infrastruktúra ellen 2016-ban a "Crashoverride / Industroyer" nevű, nagymértékben tesztelt rosszindulatú szoftver által okozott kibertámadás (a "Crashoverride" rosszindulatú szoftverről bővebben lásd a 4.1.1. Bizonytalan kommunikáció című szakasz 1. keretes írásában) egy másik példa a kiber-fizikai rendszerek elleni "fekete hattyú" esetére.

Ezért a villamosenergia-rendszer biztonságának egyik legnagyobb kihívása, hogy megtaláljuk a módját annak, hogy a sikeres támadások utáni helyreállítási, alkalmazkodási és tanulási mechanizmusok bevonásával kiszélesítsük az ismert és ismeretlen stresszorok kezelésének horizontját, ahelyett, hogy csak a megelőzésre és a felderítésre összpontosítanánk. Ez volt a tanulmány második részének célja. Fő szempontunk az volt, hogy megvizsgáljuk, hogyan növelhető a CPPS rugalmassága. Ebből a célból a 3.2. szakaszban bemutatott rugalmassági menedzsment megközelítés alkalmazásával egy rugalmassági stratégiát dolgoztunk ki, hogy meghatározzuk, hogyan lehet a CPPS-t jobban felkészíteni bármilyen stresszorra.

A következő szakaszokban az egyes szakaszokra vonatkozóan ismertetjük a rugalmassági stratégia eredményeit és a kapcsolódó intézkedéseket.

### 5.1 Felkészülés és Megelőzés

A felkészülési és megelőzési szakasz első lépéseként azonosítani kell a rendszer gyenge

*vizsgálati eredményei*

---

pontjait, és az eredményekből hatékony megelőző intézkedéseket és iránymutatásokat kell levezetni (Acatech et al., 2017). Ha a sebezhetőségek, a támadásvektorok és a rendszerre gyakorolt hatások ismertek, a hagyományos kockázatértékelési és -kezelési eljárások alapján ellenintézkedéseket kell kidolgozni. Ezekhez a feladatokhoz az informatika és az IT közötti közös erőfeszítésre és együttműködésre van szükség.

üzemeltetési technológiára (OT) van szükség. Az informatikai kiberbiztonság jellemzően a kibereszközök titkosságának, integritásának és rendelkezésre állásának biztosításán alapul, míg az energiarendszer biztonsága a műszaki tervezésen és az üzemeltetési stratégiákon alapul. Ezért az informatikai és az energiarendszer-biztonságot kombinálni kell a kiber-fizikai energiarendszer ellenálló képességének biztosítása érdekében (IEC, 2016).

A biztonsági elemzés, a fenyegetések modellezése és az általános rendszertervezés javítása segíteni fogja az ellenálló rendszer kiépítésének célját (13. interjúalany, személyes közlés, 2017). A modelleken és szimulációkon alapuló kockázatkezelés és kockázatértékelés segíteni fog a szükséges biztonsági intézkedések kitalálásában (18. interjúalany, személyes kommunikáció, 2017; 19. interjúalany, személyes kommunikáció, 2017). A holisztikus és átfogó kockázatértékelés, amely magában foglalja a politikák és eljárások felülvizsgálatát, valamint az eszközök és rendszerek, a kommunikációs útvonalak és támadási vektorok, a gyenge pontok és a fenyegetésforrások azonosítását, segít meghatározni az eszközök és rendszerek kockázati szintjét. A támadási forgatókönyvek és támadási fák értékelése sokkal pontosabb elszámolást biztosít azok előfordulási valószínűségéről, ami egy jobban priorizált, célzottabb és költséghatékonyabb kockázatcsökkentési stratégiát eredményez (Bodungen et al., 2017).

A kockázatértékelés és -kezelés kereteinek kifejezetten a kiber-fizikai rendszerekre kell összpontosítaniuk, és figyelembe kell venniük a két infrastruktúra közötti összetett összekapcsolódást, figyelembe véve a két infrastruktúra közötti lehetséges kaszkádatásokat. Néhány példa az ICS vagy a közműhálózatokra tervezett kockázatkezelési eszközökre található (Bodungen et al., 2017; Schauer et al., 2017). A támadások megértése elengedhetetlen a védekezés tervezéséhez és értékeléséhez. A példatámadásokon alapuló megközelítés alkalmazása segíthet abban, hogy a kockázatokról hatékonyan lehessen kommunikálni az üzleti döntéshozók felé. Lásd például a(Ginter, 2017) által kidolgozott, az ICS-t ért 20 legfontosabb kibertámadást felhasználó megközelítést.

Az ICS-ek ellenálló képességének további növelése érdekében az üzleti informatikai biztonság néhány szabványa és általános intézkedése is alkalmazható, mint például a robusztus programozás és a biztonsági szabványok alkalmazása. A CPPS esetében azonban specifikusabb biztonsági szabványokra lenne szükség, amelyek megkönnyítik az ilyen típusú hálózatok kialakítását (15. interjúalany, személyes közlés, 2017). Ehhez az informatikai és fizikai rendszerüzemeltetők közös erőfeszítésére és együttműködésére van szükség, hogy felügyeljék a lehetőségeket és az adott rendszerhez szükséges szabványokat, mivel a számítógépes rendszerhálózatokra vonatkozó egyes biztonsági szabványok nem alkalmasak az ICS-re. Például a nem támogatott protokollokkal kapcsolatos kérdéseket ebben a fázisban kell kezelni a további kapcsolódó problémák

vizsgálat eredményei

---

elkerülése érdekében (1. interjúalany, személyes közlés, 2016).

Amint azt a VA szakaszban említettük, az ICS-re már léteznek biztonsági szabványok és előírások. Ezek hatékony végrehajtása azonban még mindig hiányzik (1. interjúalany, személyesen

közlemény, 2016). Ahogy az ICS informatikai szakértői említették: "Úgy véljük, hogy (az ipari vezérlőrendszerekre vonatkozó *jelenlegi biztonsági szabványok*) nem gyengék, de valószínűleg a vállalatokon belüli tényleges végrehajtásuknak lehetnek gyengeségei." (15. interjúalany, személyes kommunikáció, 2017). A meglévő biztonsági szabványok és előírások hatékony végrehajtása tehát fontos kérdés ebben a fázisban.

Ezen túlmenően a tárgyak internete eszközök folyamatos telepítése az energiaágazatban több iránymutatás, referencia és nyílt forráskódú szoftver kidolgozását teszi szükségessé a megfelelő biztonsági követelmények megvalósításának támogatására (5. interjúalany, személyes közlés, 2016). A meglévő iránymutatások és bevált gyakorlatok egységesítése, valamint értékelése segíteni fogja a közműszolgáltatókat vagy a hálózatüzemeltetőket abban, hogy megtalálják az adott rendszerüknek megfelelő biztonsági méréseket. Például a BDEW (Bundesverband der Energie- und Wasserwirtschaft e.V.) által kidolgozott fehér könyv (BDEW, 2015) ajánlásokat fogalmaz meg minden újonnan beszerzett irányítási és távközlési rendszerre vonatkozóan az energiaipari szervezetek számára. A SPARKS (Smart Grid Protection Against Cyber Attacks) kutatási projekt keretében kidolgozott jelentés (lásd (SPARKS Consortium, 2016) szintén ajánlásokat fogalmaz meg az intelligens hálózatok biztonsága szempontjából releváns meglévő és új szabványokkal kapcsolatban, és meghatározza a meglévő és a fejlesztés alatt álló szabványok kritikus hiányosságait.

Más szempontból a vállalati alkalmazottak és az IT/OT személyzet számára szervezett hatékonyabb és vonzóbb biztonsági képzési és tudatosságnövelő programok kiemelkedő fontosságúak. A személyzet jobb tudatossága és elkötelezettsége hozzájárul az olyan támadási mechanizmusok kezeléséhez, mint a social engineering.

Technológiai szempontból hasznos az adattárolásra vonatkozó további intézkedések végrehajtása és a fel nem használt erőforrások - a működési lazaság - megőrzése a meglepetések jobb kezelése érdekében (Fischer és Lehnhoff, 2019).

### 5.1.1 Informatikai megelőzés Mechanizmus

Vannak olyan speciális informatikai megelőzési mechanizmusok, amelyek hozzájárulnak a CPPS előkészítéséhez és megelőzéséhez. Például a biztonságvezérelt tervezésnek ("security by design") kellene a szabványnak lennie ahelyett, hogy a biztonsági funkciókat csak frissítések és javítások révén adnánk hozzá (13. interjúalany, személyes közlés, 2017). Ezenkívül több biztonsági szintet kellene alkalmazni, és a biztonsági mechanizmusokat egymásra kellene építeni a rendszer általános biztonságának megőrzése érdekében. Először is, az adatok és a kommunikációs csatornák kriptográfiai módszereinek alkalmazása szükséges az adatok integritásának biztosítása és a tranzit során az információk nem szándékos felfedésének megakadályozása érdekében. Ezen túlmenően a támadók

tevékenységének hatékony átláthatósága érdekében behatolásérzékelő rendszerek (IDS) bevezetésére van szükség. (Interjúalany 1, személyes kommunikáció, 2016; Interjúalany 13, személyes kommunikáció, 2017).

Azonban még ha a kommunikációs csatorna biztonságos is, a végpontok akkor is veszélybe kerülhetnek. Ezért a végpontok közötti biztonság kihívásainak kezelése érdekében, ahogyan azt egy IT-biztonsági szakértő is kijelentette, biztosítani kell, hogy a biztonsági résekről gyorsan tudomást lehessen szerezni (5. interjúalany, személyes közlés, 2016). Nagyon fontos követelmény a biztonság javítása érdekében a biztonsági képességek hatékony implementálása a végpontokba a hitelesítés, valamint a használat és az ellenőrzés engedélyezése tekintetében (Interviewee 5, személyes kommunikáció, 2016). A biztonságtechnika szempontjából az egyik különleges követelmény a végpontok felügyeletének, karbantartásának és frissítésének skálázhatósága, mivel egyre több a csatlakoztatott eszköz, amelyeket felügyelni, frissíteni és karbantartani kell (Interviewee 5, személyes kommunikáció, 2016).

A megbízható számítástechnikai funkciók megvalósítása a szoftverek/firmware-ek integritása szempontjából is fontos. Ahogy az egyik interjúalany említette, nincs biztonságos szoftver, és a biztonságnak hardveralapúnak kell lennie. Megbízható platformot kell használni, amely egy olyan hardvereszköz, amely a rendszerekbe integrálva van, és amelyet nem lehet eltávolítani a rendszer tönkretétele nélkül, így biztosítva az integritást (Interjúalany 1, személyes közlés, 2016).

Ezenkívül az eszközök ellenállóvá tételét is végre kell hajtani, amely a rendszerelemek támadási felületének csökkentésére szolgáló különböző technikákra utal. Elsősorban a rendelkezésre álló szolgáltatások és funkciók szigorúan szükségesekre való csökkentése. A nem kívánt szolgáltatási portok lezárása és a nem szükséges könyvtárak eltávolítása segít csökkenteni annak valószínűségét, hogy az eszköz sebezhető legyen a biztonsági kihatásokkal szemben (Fischer és Lehnhoff, 2019). A keményítés második része a szoftver és a firmware naprakészen tartása, valamint olyan javításkezelési folyamatok létrehozása, amelyek a szoftver és a hardver hibáinak kezelésére irányuló tesztelést is magukban foglalják. Az eszközkeményítés növeli a rendszer képességét a folyamatos kibertámadások elnyelésére azáltal, hogy növeli a rendszer eszközein belüli sebezhetőségek megtalálásának és kihasználásának összetettségét (Fischer és Lehnhoff, 2019).

A szoftverekhez vagy berendezésekhez való hozzáférés-szabályozás tekintetében a komplexitás csökkentésének egyik gyakori módja a szerepalapú hozzáférés-szabályozás (RBAC), ahol az alanyok nem egyéni személyeket, hanem funkcionális szerepeket képviselnek. Egy személy ekkor meghatározott szerepkörökben tevékenykedhet, és minden szerepkörhöz alanyként jogok kapcsolódnak a hozzáférés-szabályozási mátrixban (Fischer és Lehnhoff, 2019). Az IEC 62351-8 szabvány iránymutatást ad az RBAC architektúrájához és megvalósításához az energiarendszerekben. Az eszközök időbeli és számítási korlátai

lehetetlenné teszik a teljes körű hozzáférés-szabályozási mechanizmusok alkalmazását egészen a mező rétegig. Olyan kölcsönös bizalmi területeket kell meghatározni, ahol nem valósul meg hitelesítés vagy hozzáférési korlátozás. Mindazonáltal a rendszertervezésnek kifejezetten meg kell határoznia a hozzáférés-szabályozási döntések kontextusát és indoklását, különösen azt, hogy milyen körülmények között nem szabad egy adott hozzáférés-szabályozási mechanizmust megvalósítani egy eszközön (Fischer és Lehnhoff, 2019).

A csoportok közötti adatáramlás jobb ellenőrzése és az egész hálózatra kiterjedő támadások megelőzése érdekében elengedhetetlen a különböző funkcionális csoportokra történő szegmentálás. Az ICS-ben a legalapvetőbb elválasztások az ICS, a SCADA és az üzleti hálózat között vannak, mivel mindegyiknek más-más biztonsági követelményei vannak (Fischer és Lehnhoff, 2019).

## 5.2 Robusztus és elővigyázatos tervezés megvalósítása

Amint fentebb említettük, a kiberfizikai rendszerekre ható potenciális jövőbeli stresszorok ismeretlen jellege megnehezíti a megelőzési vagy felkészülési intézkedések meghatározását. Ezért az ellenálló képesség kiépítésének második szakaszának a robusztus és elővigyázatos rendszertervezés megvalósítására kell összpontosítania. Ez képessé teszi a rendszert arra, hogy stressz vagy zavarok esetén is fenntartsa szolgáltatásait.

A 3.2. szakaszban röviden bemutattuk a rugalmassági tervezési elveket. Ebben a szakaszban a tervezési elvek a CPPS esetében kerülnek operacionalizálásra.

- A sokféleség pozitívan járul hozzá ahhoz, hogy egy rendszer hogyan tud reagálni a stresszorokra. Technológiai szinten a rendszer struktúráiban és funkcióiban növelni kell az informatikai komponensek gyártóinak, az operációs rendszereknek vagy a kommunikációs protokolloknak a **sokféleségét**.
- A redundancia a rendszer elemeinek többszörös rendelkezésre állását írja le, akár számban, akár funkcionális egyenértékűségben. A CPPS-ben biztosítani kell a kommunikációs csatornák és eszközök **redundanciáját**.
- A kiber-fizikai rendszerekben kedvezőek a **földrajzilag elosztott**, esetleg virtualizációval kibővített (Mangharam és Pajic, 2013), vagy a többágenses vezérlésen alapuló (Lehnhoff és Krause, 2013) vezérlési architektúrák.
- A pufferek és tárolók tekintetében a szakértők a CPPS-ben több szinten javasolták a **biztonsági mentések használatát**. Az energiaellátás (UPS) triviális esetén kívül a digitális rendszerek, valamint az adatok és a hardverek biztonsági másolatai vagy pontos másolatai is szükségesek. Mindkettőt offline, biztonságos módon kell tárolni (Interjúalany 2, személyes kommunikáció, 2016; Interjúalany 13, személyes kommunikáció, 2017). A rendszerekről a kritikus szoftverfrissítések előtt készült pillanatfelvételeknek rendelkezésre kell állniuk, hogy enyhítsék a manipulált javítások hatását, és lehetővé tegyék a gyors helyreállítást.
- A **szubszidiaritás** elvének alkalmazása csökkenti a munkaterhelést és az adatáramlást a hierarchikusan magasabb struktúrákban. Ez hozzájárulhat a nagyobb hatékonysághoz és a struktúrát érő támadások esetén a megfelelőbb reagáláshoz.
- A kiber-fizikai rendszerek esetében a **modularitás az** interfészek szigorú

szabványosításával és nyílt protokollok használatával érhető el. Egy példa a szabványosítási megközelítésekre

Az energiahálózati elosztásirányítási rendszerek (DMS) az OpenKONZEUENZE<sup>9</sup> (oK) nevű konzorcium által kifejlesztett munka, amely a német és holland elosztórendszer-üzemeltetőket (DSO-k), szoftvergyártókat, szolgáltatókat és kutatókat tömöríti. Az oK a DMS-funkcionalitások modularizálását ösztönzi, referenciaarchitektúrát és minőségi szabványokat hoz létre a jelenlegi szállítói kötöttségek és a rendszer összetettségének leküzdése érdekében. A cél az interoperabilitás biztosítása, valamint a szoftverfejlesztő szállítók függetlenné és gyorsabbá tétele, a szoftverminőség magas szinten tartása mellett (Goering et al., 2016).

- Az elemzett interjúk alapján az erősen centralizált, nagy erőművekkel, központi vezérlőegységekkel és központi adatfeldolgozással rendelkező struktúrákat kevésbé ellenállónak tekintik, mivel ezek egyetlen hibapontot jelentenek, és vonzóbbak a támadók számára. Ugyanakkor az erősen decentralizált struktúrát sem tekintik ellenállónak, mivel magasabb szintű koordinációt és szinkronizálást igényel annak érdekében, hogy ne veszélyeztesse a hálózat teljesítményét és megbízhatóságát. Ráadásul, ha a koordináció egy decentralizált rendszerben erősen automatizált, az a komplexitás egy újabb rétegét adja hozzá, és még tovább növeli a támadási felületet. A nagyobb ellenálló képesség elérésének jobb módja lenne egy **cellás struktúra, pl. a** (VDE, 2015) által javasolt cellás megközelítés, ahol a termelés és a fogyasztás kiegyensúlyozott a megfelelően méretű cellákon belül. Németországban az SWW Wunsiedel GmbH közműszolgáltató vállalat ezen a koncepción alapuló megoldást dolgozott ki, amely az integrált mikroerőművekből, intelligens fogyasztókból és energiatároló kapacitásokból álló kisebb egységekre történő szegmentálást alkalmazza a megújuló energia volatilitásának kezelése és a kiberbiztonság növelése érdekében (lásd (Kleineidam, Jung, et al., 2016; Kleineidam, Krasser, et al., 2016).
- A szakértőkkel folytatott megbeszélések szerint **decentralizált fizikai tartalékrendszerekre** van szükség, amelyek képesek a decentralizált struktúrákban stabil áramellátást fenntartani, még akkor is, ha a központi informatikai és kommunikációs rendszerekben áramszünet van. Képesnek kell lenniük arra, hogy a fizikai hálózati paraméterek alapján kiigazításokat hajtsanak végre a rendszer terhelése, frekvenciái és a reaktív teljesítmény kompenzációja tekintetében, amennyiben a digitális kommunikáció meghibásodik.

Általánosságban elmondható, hogy a rugalmassági tervezési intézkedések technikai (azaz hatékonysági) vagy gazdasági konfliktusokat okozhatnak. Ezért a tervezési intézkedéseket szisztematikus költség-haszon elemzéssel kell értékelni, amely magában foglalja a hosszú távú hatásokat és a ritka, de lehetséges, rendkívül káros eseményekből eredő kárköltések értékelését (Gößling-Reisemann, 2016).

---

<sup>9</sup> <https://www.openkonsequenz.de>

### 5.2.1 Érzékelés Mechanizmus

A kiberbiztonság arra összpontosít, hogy a rosszindulatú támadókat a rendszeren kívül tartsa. A kibertér-ellenálló képesség magában foglalja a rendszert fenyegető ágens által veszélyeztetett rendszer észlelésére és helyreállítására irányuló intézkedéseket. Különböző algoritmusokat (pl. többek között gépi tanulási, statisztikai vagy Bayes-hálózati módszereket) kell alkalmazni a manipulált adatok azonosítására és megbízhatatlannak való megjelölésére, hogy azokat gyanúsnak tekintsék vagy figyelmen kívül hagyják (14. interjúalany, személyes közlés, 2017).

A fizikai rendszerek esetében az energiagazdálkodási rendszerekben (EMS) meglévő biztonsági algoritmusok, mint például az energiarendszer állapotának becslése vagy a rossz adatok észlelése, felhasználhatók arra, hogy váratlan viselkedés esetén riasztást indítsanak (Friedberg et al., 2015). Az állapotbecslés működések megzavarására irányuló szándékos támadások észleléséhez (lásd például a hamis adatinjekciós támadásokat (Liu et al., 2011)) további intézkedéseket kell figyelembe venni a rosszindulatú adatok észlelésére. A szakirodalomban található néhány észlelési megoldást. Például a (Kosut et al., 2010) című tanulmányban a szerzők a villamosenergia-rendszer állapotbecslésében a hamis adatok ellenséges injektálásának problémáját vizsgálták, és újszerű megfogalmazást mutattak be a rossz adatok felismerésének problémájára. Bevezettek egy heurisztikus módszert egy adott támadás ellenfél általi észlelhetőségére, amely lehetővé teszi, hogy a különösen rossz támadások könnyen kiszámíthatók legyenek bármilyen kompromittált mérés-készletre. A (Gaber et al., 2015) egy stratégiát tárgyalnak a rossz adatok jelenlétének detektálására és egyidejű becslésére, hogy képesek legyenek elkülöníteni a rossz adatokat az energiarendszer megfigyeléseitől.

Az IKT-rendszerek esetében a meglévő biztonsági megoldásokat, például a behatolásjelző rendszert (IDS) kell használni. Az IDS által használt konkrét észlelési eszközök lehetnek például a tűzfalak által használt szabályokhoz hasonló szabályok, amelyek lehetővé teszik a biztonsági irányelveket sértő hálózati forgalom észlelését. Az IDS-t úgy is be lehet konfigurálni, hogy felderítő tevékenységeket, például állomás- és portvizsgálatokat észleljen, amelyek jelezhetik, hogy támadás közeleg (McLaughlin et al., 2015) Ha a rendszereket vagy komponenseket nem lehet frissíteni vagy foltozni, az IDS megvalósítása ezért fontos, hogy észlelje, ha és amikor a rendszereket veszélyeztetik (18. interjúalany, személyes közlés, 2017). A Snort<sup>10</sup> nevű nyílt forráskódú, hálózat alapú behatolásérzékelő rendszer (NIDS) az egyik legismertebb és legelterjedtebb IDS a kutatóközösségben. A hálózati forgalomban valós időben képes protokollelemzést, tartalomkeresést és tartalomillesztést végezni (McLaughlin et al., 2015).

A kommunikációs csatornákon keresztüli anomália-alapú észlelő rendszerek lehetővé teszik

---

a folyamatok zavarainak észlelését és megkülönböztetését a kapcsolódó kibertámadásoktól.

Összehasonlítják a következők meghatározását

---

<sup>10</sup> <https://www.snort.org/>

a tevékenységre vonatkozó normálisnak tekintett értékeket a megfigyelt eseményekkel összevetve a jelentős eltérések azonosítása érdekében. A normális meghatározás lehet: (a) küszöbérték-alapú vagy b) profil-alapú.

(a) Egy küszöbérték-alapú folyamat képes bizonyos események előfordulási gyakoriságának megfigyelésére, és riasztást adhat, ha a küszöbértéket megsértik. A kommunikációban például a másodpercenkénti csomagok száma, bizonyos csomagok vagy áramlások mérete stb. lehet. (b) A profil alapú anomália-érzékelés a múltbeli viselkedés jellemzésére és az esetleges változások észlelésére összpontosít. Ehhez általában képzési időszakra és a megfigyelendő értelmes jellemzők gondos kiválasztására van szükség (McLaughlin et al., 2015). A szakirodalomban található egy tanulmány a többváltozós statisztikai folyamatszabályozáson (MSPC) alapuló anomália-felismerő és diagnosztikai rendszerek megoldásairól, amelyek célja a támadások és a zavarok megkülönböztetése (lásd (Iturbe et al., 2016)).

Egy másik módszer a rendszer átvételére törekvő támadók felderítésére az üzemeltetők használati szokásainak és a kapcsolódó adattörténetnek a vizsgálatára támaszkodhat, ahogy azt egy szakértő javasolta. E használati minták elemzése megmutathatná, hogy az egyes üzemeltetők hogyan használják a rendszert. Ha valaki egy másik felhasználótól jogtalanul megszerzett bejelentkezési adatokat használ, és a jogos üzemeltetőtől eltérő módon működteti a rendszert, ezeket az eltéréseket fel lehetne fedezni. Ezzel kapcsolatban a megfelelő jelszókezelés kulcsfontosságú a bejelentkezési hitelesítő adatok jogosulatlan használatának elkerülése érdekében (4. interjúalany, személyes közlés, 2016).

### 5.3 Aválságok kezelése és a válságokból való kilábalás

Sikeres támadás esetén a lehető legkisebb területre vagy alrendszerre való korlátozással kell kezelni a válságot, és a lehető leggyorsabban helyre kell állítani a rendszer szolgáltatásait. A legkritikusabb következmények a hosszú távú áramkimaradások, amelyek mértékének csökkentése érdekében regionális vagy helyi szinten üzletmenet-folytonossági tervezést, vészhelyzeti tervezést és megfelelő intézkedéseket kell végrehajtani (Acatech et al., 2017; Gößling-Reisemann, 2016).

Ezenkívül a rendszerre való reagáláshoz és helyreállításához gyorsan azonosítani kell a hiba helyét. Az informatikai rendszerrészek meghibásodásának észleléséhez az OT felügyeleti rendszerekkel integrált vagy összekapcsolt IKT felügyeleti rendszerekre van szükség. A hálózati irányítóközpontokban mind az informatikai, mind az OT-szakértőkre szükség van, akiknek képesnek kell lenniük a különböző informatikai és fizikai infrastruktúrák együttes kezelésére. Az esetleges meghibásodásokra való reagálást előre meg kell tervezni és ki kell képezni, illetve meg kell valósítani, nem pedig csak a támadásokra és meghibásodásokra adott reakcióként (1. interjúalany, személyes közlés,

2016; 4. interjúalany, személyes közlés, 2016). Ehhez aktív vészhelyzeti tervezésre és valóság-hű kibertámadásokkal kapcsolatos gyakorlatokra van szükség. Emellett a megfigyelés és a dinamikus szegmentálás lehetővé teszi a veszélyeztetett végpont azonosítását és elkülönítését (Interviewe 5, személyes kommunikáció, 2016). A szegmentálási képességek a moduláris tervezési elvhez és a laza (vagy opcionális) csatolási paradigmához kapcsolódnak.

Ezenkívül előnyös a rendszer azon képességének javítása, hogy minimális IKT-vel vagy anélkül is működtethető legyen, így lehetővé válhatna a rendszer kézi vezérlése, vagy legalább a rendszer puha leszállása az IKT-infrastruktúrát ért támadás esetén.

A szükséges helyreállítási mechanizmusok a támadástól és az abból eredő hatástól is függenek. A szoftverrendszer elleni támadás esetén a programlogika újratelepítése szükséges. Ezért a vezérlési logika kompromisszummentes biztonsági másolatára van szükség. Továbbá a programlogika frissítése szükséges a hibák kijavítása/javítása érdekében (15. interjúalany, személyes közlés, 2017). A számítógépek és terminálok támadás utáni helyreállításához bármilyen szoftverszintű biztonsági mentésre szükség van. Az offline biztonsági mentések itt is nagyobb biztonságot nyújtanak, mivel a támadók nem tudják kompromittálni őket (13. interjúalany, személyes közlés, 2017), bár e biztonsági mentések telepítése munkaigényes.

A központosított rendszerben bekövetkező meghibásodások esetén azonosítani kell a meghibásodott részeket, és hasznos lehet a rendszer elosztottabb módon történő újrakonfigurálása. A több ágensre épülő decentralizált vezérlési konszenzus koncepciója javíthatja a stabilitást és a biztonságot meghibásodások esetén (lásd (Lehnhoff és Krause, 2013)). A helyreállítási mechanizmus végrehajtása és a veszélyeztetett komponensek biztonsági mentésekből történő beállítása után a korábbi központosított konfiguráció visszaállítható. A rendszer így képes lenne arra, hogy meghibásodások esetén fokozatosan a centralizáltból decentralizálttá váljon, majd ismét visszaálljon. Ezzel a megközelítéssel kapcsolatban egy szakértő megemlítette, hogy "a kisebb cellákban való munka kevésbé lehet hatékony, mivel minden cellának tartalék- és kiegészítő szolgáltatásokat kell nyújtania, de ez megvalósítható és működőképes, amíg ez nem válik általános esetté". Amint lehetséges, a rendszernek vissza kell térnie egy központibb konfigurációhoz, amely hatékonyabb tartalékolást és kiegészítő szolgáltatások nyújtását biztosítja (14. interjúalany, személyes közlés, 2017).

#### 5.4 Tanuljon a jövőre nézve

A múltbeli katasztrófákat és az elkerült katasztrófákat fel kell használni a **jövőre vonatkozó tanulságok levonására**, és ezáltal a rendszer alkalmazkodóképességének javítására. Ezt úgy lehet elérni, hogy dokumentáljuk és elemezzük ezeket a válságokat és eseményeket, hogy azonosítsuk azokat a gyengeségeket, amelyek bekövetkezésükhöz vezettek (sebezhetőségi tároló). Ebben az értelemben a digitális törvényszéki vizsgálat lehetővé tenné az incidensek és a majdnem incidensek alapos kivizsgálását és a tanulságok levonását. Ezzel szemben a megelőzéshez vagy helyreállításhoz hozzájáruló erősségek azonosítása (megoldásraktár) alapul szolgálhat a stratégiák és vészhelyzeti forgatókönyvek tervezéséhez (Acatech et al., 2017; Gößling-Reisemann, 2016).

*vizsgálati eredményei*

A korábbi támadásokból való tanulás feltárhatja a támadási felületet, amelyet a fenyegető ügynökök használtak, a támadás mechanizmusait, és segít megtanulni, hogyan lehet ezeket a felületeket biztosítani vagy a hibákat kezelni. A Stuxnethez hasonló támadások tanulsága például az, hogy a vállalatoknak jobban fel kell készülniük a social engineering támadásokra. Ez magában foglalja az alkalmazottak jobb biztonsági képzését

valamint az üzleti és irányítástechnikai hálózatok megfelelő elkülönítése (1. interjúalany, személyes közlés, 2016; 13. interjúalany, személyes közlés, 2017).

Ha a rendszerben hibát fedeznek fel és jelentenek be, az nemcsak a potenciális támadókat figyelmezteti, hanem a forgalmazókat is, akik ezután ellenintézkedéseket tehetnek. Ha a hibákat nem jelentik be, az eladók nem tudnak róluk, és nem tudnak ellenintézkedéseket tenni (15. interjúalany, személyes kommunikáció, 2017). Emellett a sikeres vagy sikertelen támadásokkal kapcsolatos információkat meg lehetne osztani a vállalatok között, hogy tanuljanak az incidensekből, hasonlóan a CERT- Bund (Computer Emergency Response Team for federal agencies) által végzett munkához (Interviewe 19, személyes kommunikáció, 2017). Különösen az elhárított támadások jelenthetnének nagyon jó tanulási forrást. A jelenlegi "ne mondd el" gyakorlatot egy olyan átláthatósági szabállyal kellene felváltani, amely lehetővé teszi a múltbeli hibákból és sikertörténetekből való tanulást, ugyanakkor fenntartja az energiarendszer-üzemeltetők jogát a kritikus üzleti adataik védelmére.

## 5.5 A rugalmassági menedzsment összefoglalása Stratégia

Az előző szakaszokban az ellenálló képességet fokozó intézkedéseket a rugalmassági menedzsment megközelítés négy szakaszának megfelelően tárgyaltuk. Most ezeket foglaljuk össze a különböző intézkedéseknek a VA-ban használt kategóriák szerinti rendezésével. Ez lehetővé teszi, hogy jobban áttekinthessük az ellenálló képességet fokozó intézkedéseket, és összekapcsoljuk őket a VA-ban azonosított kritikus pontokkal.

A 4. táblázat a technológia kategóriára javasolt intézkedéseket foglalja össze, az 5. táblázat a szervezeti biztonsági politikák és eljárások kategóriára javasolt intézkedéseket foglalja össze, a 6. táblázat az emberi tényező kategóriára javasolt intézkedéseket foglalja össze, a 7. táblázat pedig a szabályozások kategóriára javasolt intézkedéseket foglalja össze.

4. táblázat: Az ellenálló képességet fokozó intézkedések és elemek a technológia kategóriában a következő fázisok szerint: (1) Felkészülés és megelőzés, (2) Robusztus és elővigyázatos tervezés végrehajtása, (3) Kezelés és helyreállítás, valamint (4) Tanulás a jövőre nézve. Forrás: Saját ábrázolás.

Technology			
Prepare and prevent	Implement robust and precautionary design	Manage and recover from crises	Learn for the future
Implement <b>security measures at endpoints</b> e.g. encryption, authentication and authorization (Interviewee 5, 2016)	Increase the <b>diversity</b> of IT components (at least in respect to manufacturing, operating systems and communication protocols)	<b>Multi-agent based control</b> with decentralized consensus findings could enhance stability and security during crises (Lehnhoff & Krause, 2013)	Make use of <b>digital forensics</b> , to draw conclusions from 'near failures' and learn from them (Gößling-Reisemann, 2016; Acatech et al., 2017)
Implement <b>test routines for patch management</b> in order to counteract compromised hardware and software with manipulated updates (Fischer and Lehnhoff, 2018).	Ensure <b>redundancy</b> in communication channels and devices.	Improve the ability to <b>operate the system without ICT</b> , i.e. manually, or to at least secure a <i>soft landing</i>	Implement additional measures for data storage (Interviewee 9, 2017; Interviewee 15, 2017)
Use a holistic security approach between IT and OT, considering complex interconnections and interactions (International Electrotechnical Commission (IEC), 2016)	Maintain the ability to rely only on decentralized <b>physical parameters</b> for operation and hardware-based security, in order to secure a minimum and stable power supply, in case of a failing central ICT infrastructure ("discussed by the interviewed experts")		
Organize the system in a way that security breaches and gaps can be found out quickly (Interviewee 5, 2016)	<b>Cellular structure</b> can improve resilience (Verband der Elektrotechnik Elektronik Informationstechnik), 2015		
Use of a trusted platform, in form of a hardware device integrated with the system that cannot be removed without destroying the system (Interviewee 1, 2016)	Implement intrusion and anomaly <b>detection systems</b> (McLaughlin et al., 2015; Interviewee 18, 2017)		
Keep uncompromised backup of the control logic and updating of the program logic (Interviewee 15, 2017)			
Use of role-based access control (RBAC) in order to make access control more manageable (Fischer & Lehnhoff, 2018)			

5. táblázat: Ellenálló képességet növelő intézkedések és elemek a Szervezeti biztonsági politikák és eljárások kategóriában a következő fázisok szerint: (1) Felkészülés és megelőzés, (2) Robusztus és elővigyázatos tervezés végrehajtása, (3) Kezeljük és helyreállítjuk, és (4) Tanuljunk a jövőre nézve. Forrás: B: Saját ábrázolás.

Organizational Security Policies and Procedures			
Prepare and prevent	Implement robust and precautionary design	Manage and recover from crises	Learn for the future
Use <b>security by design</b> taking into account new threats and vulnerabilities, e.g. bug bounty programs (Interviewee 13, 2017)	Implement <b>adaptive mechanisms allowing for real-time monitoring</b> , intrusion and anomaly detection in communication channels (Interviewee 14, 2017)	Provide <b>business continuity and emergency plans</b> on a regional and local level, e.g. 'supply islands' at least in and around public properties/ buildings (Acatech et al., 2017a; Gößling-Reisemann, 2016)	Identify strengths in avoided failures that in the past or enhanced recovery as the basis for planning strategies and emergency measures ( <b>Solution Store</b> ) (Gößling-Reisemann, 2016)
Apply <b>energy-focused risk assessments and management approaches</b> (Interviewee 18, 2017; Interviewee 19, 2017)	Perform periodic <b>backups of the complete systems</b> (control logic and updating of the program logic) for quick recovery. (Offline backups prevent manipulation) (Interviewee 13, 2017 ; Interviewee 15, 2017)	Restrict crises to the smallest possible area or sub-system and overcome them as quickly as possible (Goessling-Reisemann and Thier, 2019)	Learn from mastered crisis by documentation and analysis, i.e. learn from previous attacks, e.g. Ukraine, Wannacry or Stuxnet. (Interviewee 1, 2016; Interviewee 13, 2017)
<b>Less is more:</b> reduce services and functionalities in terms of data, ports, libraries, group permissions, (Fischer and Lehnhoff, 2018)	<b>Proper password management</b> is key to avoid unauthorized usage of login credentials (Interviewee 4, 2016)	<b>Monitoring and dynamic segmentation</b> enables the identification and isolation of a compromised endpoint (Interviewee 5, 2016).	Identify weaknesses and document them in a way that the information is accessible to everyone ( <b>Vulnerability Store</b> ) (Gößling-Reisemann, 2016)
Develop more and <b>better guidelines and references</b> to support the implementation of adequate security requirements (Interviewee 5, 2016)	<b>Security by obscurity:</b> intentionally implement a system in a way that is not consistent with conventions and standards in order to confuse attackers and force them to invest more time in system reconnaissance (Fischer & Lehnhoff, 2019)	Identify failing parts and reconfigure the system in a more distributed fashion during a crisis. (Interviewee 14, 2017)	Make use of digital forensics, to draw conclusions from 'near failures' and learn from them (Gößling-Reisemann, 2016; Acatech et al., 2017)
Obtain evidence of trustworthiness from manufacturers and suppliers, ensure product integrity, <b>avoid monocultures</b> (BSI, 15.10.2019)	Use existing security algorithms in the energy management systems (EMS), such as power system state estimation or bad data detection, to trigger <b>alerts in the case of unexpected behavior</b> (Friedberg et al., 2015)		
<b>Examine usage patterns</b> of operators and the connected data history (Interviewee 4, 2016 )			
<b>Evaluation of attack scenarios and attack trees</b> will produce a risk mitigation strategy that is better prioritized, more targeted, and cost-effective (Bodungen et al.,2017).			
Reaction on possible failures should be planned and <b>trained or implemented in advance</b> , not just as a reaction to attacks and failures (Interviewee 1, 2016; Interviewee 4, 2016)			

6. táblázat: Az emberi tényező kategóriára vonatkozó ellenálló képességet fokozó intézkedések és elemek a következő fázisok szerint: (1) Felkészülés és megelőzés, (2) Robusztus és elővigyázatos tervezés megvalósítása, (3) Kezelés és helyreállítás, és (4) Tanuljon a jövőre nézve. Forrás: B: Saját képvisolet.

The Human Factor			
Prepare and prevent	Implement robust and precautionary design	Manage and recover from crises	Learn for the future
Implement more effective and engaging security training and awareness programs for IT and OT personnel	Enable a tight cooperation between IT and OT for operating and monitoring cyber-physical systems (Interviewee 1, 2016; Interviewee 4, 2016)	Prepare for active emergency planning and exercises based on realistic cyber-attacks	Preserve unused resources - operational slack – will improve the learning.
Preserve unused resources - operational slack - to better deal with surprises (Fischer and Lehnhoff 2018)			Provision of security training for employees, and proper isolation of business and control system networks (Interviewee 1, 2016; Interviewee 13, 2017)

7. táblázat: Az ellenálló képességet fokozó intézkedések és elemek a Rendeletek kategóriában, majd az (1) Felkészülés és megelőzés, (2) Robusztus és elővigyázatos tervezés végrehajtása, (3) Kezelés és helyreállítás, valamint (4) Tanulás a jövőre nézve. Source: Saját ábrázolás.

Regulations			
Prepare and prevent	Implement robust and precautionary design	Manage and recover from crises	Learn for the future
Implement effective guidelines and best practices e.g BDEW (Bundesverband der Energie- und Wasserwirtschaft e.V., 2015)	Make it mandatory to implement resilience principles: Diversity and Redundancy in structures and function, Buffer and Storages. Decentralize management with subsidiarity principle, Modular components, flexible Couplings. (Acatech et al., 2017), (Gößling-Reisemann and Thier, 2019)		Use the understanding of attacks to plan and evaluate defenses and share this information (Solution store)
Ensuring effective implementation of existing Intrusion detection systems(IDS) (Interviewee 1, 2016) (Interviewee 15, 2017)			Make documentation regarding failures, attack mechanisms and implement countermeasures publicly available between companies mandatory. (Interviewee 19, personal communication, 2017)
Make the monitoring and the effective implementation of a minimum security requirement mandatory.	Strengthen resource efficiency and flexibility, increase participation and burden sharing (Acatech et al., 2017)		

## 6 Következtetések és Kilátások

Széles körben elfogadott tény, hogy az energiarendszer gyorsan egy nagy és összetett kiber-fizikai energiarendszerré fejlődik, amely sebezhető a kiber-fizikai támadásokkal szemben. Ezzel egyidejűleg a támadási változatok is egyre összetettebbé válnak, ami szükségessé teszi a meglévő védelmi mechanizmusok megváltoztatását, amelyek általában a múltbeli események tanulságain alapulnak, és nem hatékonyak a rendszer ismeretlen fenyegetésekkel szembeni védelmében. Ezért olyan megközelítésre van szükség, amely túlmutat a múltbeli események és támadási mechanizmusok ismeretén, hogy segítse az energiarendszer védelmét az ismert és ismeretlen fenyegetésekkel szemben. E tanulmánynak ez volt a középpontjában. Felmértük a villamosenergia- és kiberinfrastruktúra meglévő és ismert sebezhetőségeit, és kidolgoztunk egy ellenálló képesség-kezelési stratégiát a kiber-fizikai villamosenergia-rendszerek váratlan fenyegetésekre való felkészítésére.

A tanulmány első részében a kiberfizikai energiarendszerek sebezhetőségét növelő kritikus tulajdonságokat, struktúrákat és elemeket azonosították a sebezhetőségi értékelésen alapuló megközelítéssel (Gößling-Reisemann et al., 2013; von Gleich et al., 2010). Két értékelési módszert alkalmaztak, egy eseményalapú sebezhetőségi értékelést (EVA) és egy strukturális alapú sebezhetőségi értékelést (SVA). Az értékeléshez szükséges inputot az energetikai és az informatikai ágazat szakértőitől kaptuk félig strukturált interjúk és két szakértői műhelybeszélgetés során. A szakértői nyilatkozatokat átfogó kvalitatív tartalomelemzési módszerrel értékelték. Az értékeléshez a témával kapcsolatos releváns szakirodalom áttekintését is bevonták. Az eredményeket a következő kategóriákba sorolták:

(1) Technológia,

(2) Szervezeti biztonsági politikák és eljárások, (3) Az emberi tényező és (4) Szabályozások.

Minden egyes kategória esetében további alkategóriákat határoztak meg, amelyek megfeleltek az értékelésnek az IKT-infrastruktúrából származó stresszorokra való összpontosításának. A magas sebezhetőségi besoroláshoz hozzájáruló néhány azonosított körülmény: a nem biztonságos kommunikáció vagy a végpontok gyenge biztonsági jellemzői, különösen az ügyfél telephelyén, amelyek veszélyeztethetik az adatok sértetlenségét, rendelkezésre állását és bizalmas jellegét. A social engineeringet kritikus támadási mechanizmusként azonosították, amely egy gyorsan növekvő biztonsági probléma, amely lehetővé teszi a fenyegető tényezők számára, hogy kihasználják a minden szervezetben jelen lévő egyik gyenge pontot: az emberi tényezőt. Annak ellenére, hogy léteznek olyan adaptációs mechanizmusok, amelyek javíthatják a biztonsági szintet és minimalizálhatják e fenyegetések hatását, kiderült, hogy ezek végrehajtását akadályozhatja a politika érvényesítésének hiánya vagy az érintett szereplők felkészületlensége ezen

*vizsgálat eredményei*

---

intézkedések végrehajtására. A VA eredményeiből arra a következtetésre jutottak, hogy e kiberbiztonsági kihívások kezelése érdekében a fizikai, kiber- és társadalmi szempontokból álló integrált értékelést kell alkalmazni.

A tanulmány második részében egy rugalmassági menedzsment megközelítést dolgoztunk ki, amely arra a kérdésre próbál választ adni, hogyan lehet felkészíteni a kiber-fizikai energiarendszereket az ismeretlen ismeretlenekre. A rugalmassági menedzsment megközelítés négy fázisból áll: (1) Felkészülés és megelőzés, (2) Robusztus és elővigyázatos tervezés megvalósítása, (3) Válságok kezelése és helyreállítása, valamint (4) Tanulás a jövőre nézve. Ezeket a fázisokat iteratív módon kell lefuttatni.

A javasolt stratégiában az ellenálló képességet fokozó intézkedéseket a VA esetében használt kategóriák szerint sorolták be, és az egyes fázisokhoz rendelték. Az intézkedések a VA eredményeire épültek, és a szakértői interjúk, a szakirodalomkutatás és a saját megítélés alapján születtek. Az ellenálló képesség-kezelési stratégia az ellenálló képességet fokozó intézkedések strukturálására összpontosít, amelyek magukban foglalják a váratlan eseményekre való felkészülés mechanizmusát, az elővigyázatos tervezés végrehajtását, az alkalmazkodási mechanizmusokat és a rendszer tanulási képességét a jövőre nézve.

Az első fázisban - Felkészülés és megelőzés - azonosítani kell az ismert sebezhetőségeket és gyenge pontokat, és hatékony megelőző intézkedéseket kell végrehajtani. Ilyen például a hitelesítés és titkosítás bevezetése a végpontokon, biztonsági mentések készítése a vezérlő- és programlogikáról, a szolgáltatások csökkentése csak a szükségesekre és jobb irányelvek kidolgozása. Emellett megfelelő kiberbiztonsági szabályozási kereteket kell létrehozni, és a végrehajtást hatékonyan nyomon kell követni. A második fázisban a hangsúly a robusztus és elővigyázatos tervezés megvalósítására helyeződik át. Itt a fő hangsúly az ellenálló tervezési elvek használatán és alkalmazásán van, mint például az összetevők és protokollok diverzifikálása, redundáns és moduláris struktúrák és kommunikáció létrehozása, valamint többek között anomália-felismerő rendszerek bevezetése. Ha a fenti intézkedések kudarcot vallanak, és a rendszer stressznek van kitéve, például egy sikeres támadás következtében, akkor a lehető legkisebb területre vagy alrendszerre való visszaszorítással kell kezelni a válságot, és a lehető leggyorsabban helyre kell állítani a rendszer szolgáltatásait. Ez elvezet az ellenálló képesség-kezelési stratégia harmadik szakaszához, amely az alkalmazkodási mechanizmusok biztosítása. A válságok kezelése és a válságokból való felépülés érdekében a rendszer architektúrájának rugalmasnak kell lennie, például egy cellás struktúra révén, több ágensre épülő, decentralizált konszenzuson alapuló vezérléssel. Ezenkívül offline fizikai biztonsági mentéseket kell létrehozni, hogy a sikeres támadások esetén jobb biztonságot és IKT-független helyreállítást lehessen biztosítani. Az utolsó fázisban - Tanulni a jövőre - a megfelelő intézkedések közé tartozik egy sebezhetőségi tár létrehozása, amelyben az azonosított gyengeségeket dokumentálják, valamint egy megoldási tár, amelyben a múltban elkerült hibák erősségeit rögzítik. Ezeket az információkat a szervezeteknek meg kell osztaniuk egymással, hogy tanulhassanak az incidensekből vagy a majdnem bekövetkezett

hibákból.

Az ellenálló képességet fokozó intézkedéseket az 5.5. szakasz 4., 5., 6. és 7. táblázata foglalja össze. A javasolt intézkedések nem kívánnak átfogóak lenni, és látható, hogy egyes fázisok vagy kategóriák esetében nem sok intézkedést vezettek le. Például a következő esetekben

az "irányítás és helyreállítás" és a "jövőre való tanulás" fázisok, valamint az "emberi tényező" és a "szabályozás" kategóriák esetében csak kevés intézkedést javasoltak, noha ezek a fázisok rendkívül fontosak a rendszer rugalmas viselkedése szempontjából. Ezért arra a következtetésre jutottunk, hogy több erőfeszítést kell tenni arra, hogy megfelelő intézkedéseket találjunk ezekre a fázisokra és kategóriákra, figyelembe véve a nem technológiai és szervezeti szempontokat.

Az alkalmazott módszertanokat illetően úgy véljük, hogy a sebezhetőségi vizsgálat megközelítése egyszerű, könnyen alkalmazható és eredményes, ugyanakkor időigényes lehet. Míg az ellenálló képesség kezelési stratégia levezetése nagyobb kihívást jelentő folyamat volt. A VA és a rugalmassági tervezési elv-elmélet eredményei támogatták az első és a második fázis intézkedéseinek meghatározását. A másik két fázis esetében azonban, amelyek erősen kapcsolódnak az ellenálló képesség kiépítéséhez, és nem szerepelnek a hagyományos kockázatkezelési megközelítésekben, kihívást jelentett olyan általánosított tanácsokat adni, amelyek segítenek bármilyen stressz enyhítésében. Ez tükröződik az e fázisok esetében felsorolt korlátozott intézkedésekben.

Úgy véljük, hogy a rugalmassági elvek és elemek alkalmazása, valamint a rugalmassági menedzsment megközelítés kialakítása támogathatja az érdekelt feleket és a felhasználókat abban, hogy a fejlődő energiarendszereket felkészítsék a váratlan eseményekre. További munkára van azonban szükség e feltételezés bizonyításához és az e területre vonatkozó ismeretek bővítéséhez. Ezért azt javasoljuk, hogy a következő lépések a kéziratban leírt javasolt intézkedések végrehajtása, a rendszerek stresszhelyzetben való viselkedésének nyomon követése és a különböző fázisokra vonatkozó további intézkedések iteratív hozzáadása legyen a következő lépés. Az eljárásokat és az eredményeket dokumentálni kell, és nyíltan hozzáférhetővé kell tenni, lehetővé téve ezzel a közös hozzájárulást és a korábbi tapasztalatokból való tanulást. Ez lehetővé teszi az ellenálló képesség kezelésének stratégiájának, valamint magának az ellenálló képességgel kapcsolatos ismereteknek a folyamatos fejlesztését.

## 7 Hivatkozások

- Acatech, Leopoldina és Akademienunion. (2017). *Das Energiesystem resilient gestalten: Maßnahmen für eine gesicherte Versorgung*. Acatech, Leopoldina, Akademienunion.
- Arghandeh, R., von Meier, A., Mehrmanesh, L., and Mili, L. (2016). A kiber-fizikai ellenálló képesség meghatározásáról az energiarendszerekben. *Renewable and Sustainable Energy Reviews*, 58, 1060-1069.  
<https://doi.org/10.1016/j.rser.2015.12.193>.  
<https://doi.org/10.1016/j.rser.2015.12.193>
- Baig, Z. A. és Amoudi, A. R. (2013). Az intelligens hálózatok támadásainak és ellenintézkedéseinek elemzése. *Journal of Communications*, 8(8), 473-479. <https://doi.org/10.12720/jcm.8.8.473-479>.  
<https://doi.org/10.12720/jcm.8.8.473-479>.
- Basagiannis, S., Chabukswar, R., Yang, Y., McLaughlin, K., and Boubekour, M. (2015). 10. fejezet - Az intelligens hálózatbiztonsági alkalmazások megvalósítási tapasztalatai és a jövőbeli kutatás kilátásai. In F. Skopik and P. Smith (Eds.), *Smart Grid Security* (pp. 283-306). Syngress. <https://doi.org/10.1016/B978-0-12-802122-4.00010-9>
- BDEW. (2015). *Whitepaper Anforderungen an sichere Steuerungs- und Telekommunikationssysteme White Paper Requirements for Secure Control and Telecommunication Systems*.  
[https://www.bdew.de/internet.nsf/id/232E01B4E0C52139C1257A5D00429968/\\$file/OE-BDEW-Whitepaper\\_Secure\\_Systems V1.1 2015.pdf](https://www.bdew.de/internet.nsf/id/232E01B4E0C52139C1257A5D00429968/$file/OE-BDEW-Whitepaper_Secure_Systems V1.1 2015.pdf)
- Becker, C. (2013). *Bedrohungsanalyse für Smart Grids und Anpassung des Sicherheitskonzeptes*. Hochschule Bremen.
- BNetzA. (2019). *Bundesnetzagentur-Sicherheitsanforderungen*.  
[https://www.bundesnetzagentur.de/DE/Sachgebiete/Telekommunikation/Unternehmen\\_Institutionen/Anbieterpflichten/OeffentlicheSicherheit/KatalogSicherheitsanforderungen/aktualisierung\\_sicherheitsanforderungen/aktualisierung\\_sicherheitsanforderungen-node.html](https://www.bundesnetzagentur.de/DE/Sachgebiete/Telekommunikation/Unternehmen_Institutionen/Anbieterpflichten/OeffentlicheSicherheit/KatalogSicherheitsanforderungen/aktualisierung_sicherheitsanforderungen/aktualisierung_sicherheitsanforderungen-node.html)
- Bodungen, C., Singer, B., Hilt, S., Shbeeb, A., and Wilhoit, K. (2017). *Hacking Exposed Industrial Control Systems (Feltárt ipari vezérlőrendszerek feltörése): ICS and SCADA Security Secrets & Solutions* (1. kiadás). McGraw-Hill Education.
- Brand, U., Giese, B., von Gleich, A., Heinbach, K., Petschow, U., Schnülle, C., Stührmann, S., Stührmann, T., Thier, P., Wachsmuth, J., and Wigger, H. (2017). *Resiliente Gestaltung des Energiesystems am Beispiel der Transformationsoptionen "EE-Methan-System" und "Regionale Selbstversorgung": Schlussbericht des vom BMBF geförderten Projektes RESYSTRA (FKZ: 01UN1219A-B)*. Universität Bremen. <https://doi.org/10.2314/KXP:1667649884>.
- BSI. (2013). *TR-03109 Anforderungen an die Interoperabilität der Kommunikationseinheit eines intelligenten Messsystems für Stoff- und Energiemengen*.  
<https://www.bsi.bund.de/SharedDocs/Downloads/DE/BSI/Publikationen/TechnischeRichtlinien/TR03109/TR03109-1.pdf?blob=publicationFile&v=1>
- BSI. (2014). *Védelmi profil az intelligens mérőkapuk biztonsági moduljához ( Security Module PP )*.  
[https://www.bsi.bund.de/SharedDocs/Downloads/DE/BSI/Zertifizierung/Reporte/ReportePP/pp0077V2b\\_pdf.pdf?blob=publicationFile&v=1](https://www.bsi.bund.de/SharedDocs/Downloads/DE/BSI/Zertifizierung/Reporte/ReportePP/pp0077V2b_pdf.pdf?blob=publicationFile&v=1)
- BSI. (2015a). *Das Smart-Meter-Gateway*.  
<https://www.bsi.bund.de/SharedDocs/Downloads/DE/BSI/Publikationen/Broschueren/>



- BSI. (2015b). *KRITIS-Sektorstudie Energie*.  
[https://www.dqs.de/fileadmin/files/de2013/Files/Standards/Informationsmanagement/IT-Netzbetreiber/KRITIS-Sektorstudie\\_Energie.pdf](https://www.dqs.de/fileadmin/files/de2013/Files/Standards/Informationsmanagement/IT-Netzbetreiber/KRITIS-Sektorstudie_Energie.pdf)
- Cellan-Jones, R. (2018, július 24.). *Orosz hackerek hatoltak be az erőművekbe*. BBC News. <https://www.bbc.com/news/technology-44937787>.
- CEN-CENELEC-ETSI intelligens hálózat koordinációs csoport. (2012). *Smart Grid referenciarchitektúra*.  
[https://ec.europa.eu/energy/sites/ener/files/documents/xpert\\_group1\\_reference\\_architecture.pdf](https://ec.europa.eu/energy/sites/ener/files/documents/xpert_group1_reference_architecture.pdf)
- Cherdantseva, Y., Burnap, P., Blyth, A., Eden, P., Jones, K., Soulsby, H., and Stoddart, K. (2015). A SCADA-rendszerek kiberbiztonsági kockázatértékelési módszereinek áttekintése. *Computers & Security*, 56, 1-27.  
<https://doi.org/10.1016/j.cose.2015.09.009>  
<https://doi.org/10.1016/j.cose.2015.09.009>
- Cherepanov, A. (2017). *WIN32/INDUSTROYER Egy új fenyegetés az ipari vezérlőrendszerekre*. ESET. [https://www.welivesecurity.com/wp-content/uploads/2017/06/Win32\\_Industroyer.pdf](https://www.welivesecurity.com/wp-content/uploads/2017/06/Win32_Industroyer.pdf)
- Cherepanov, A. és Lipovsky, R. (2017, június 12.). *Industroyer: A Stuxnet óta a legnagyobb fenyegetés az ipari vezérlőrendszerekre*. WeLiveSecurity. <https://www.welivesecurity.com/2017/06/12/industroyer-biggest-threat-industrial-control-systems-since-stuxnet/óta>.
- Cleveland, F. (2016). *IEC 62351 Security Standards for the Power System Information Infrastructure*.  
<http://iectc57.ucaiug.org/wg15public/Public%20Documents/White%20Paper%20on%20Security%20Standards%20in%20IEC%20TC57.pdf>
- Belbiztonsági Minisztérium. (2018. március 15.). *Russian Government Cyber Activity Targeting Energy and Other Critical Infrastructure Sectors | CISA*. <https://www.us-cert.gov/ncas/alerts/TA18-074A>.
- Detken, K.-O., Genzel, C.-H., Hoffmann, O., and Sethmann, R. (2014). Biztonsági koncepció az átjárók integritásának védelmére a német intelligens hálózatokon belül. *3rd ASE International Conference on Cyber Security, ASE (Academy of Science and Engineering)*. [https://www.spider-smartmetergateway.de/cms/upload/pdf/ECSaR2014\\_Stanford.pdf](https://www.spider-smartmetergateway.de/cms/upload/pdf/ECSaR2014_Stanford.pdf).
- Detken, K.-O., Genzel, C.-H., Rudolph, C., and Jahnke, M. (2014). Integritásvédelem intelligens hálózati környezetben az intelligens fogyasztásmérők vezeték nélküli eléréséhez. *2014 2nd IEEE International Symposium on Wireless Systems within the Conferences on Intelligent Data Acquisition and Advanced Computing Systems*, 79-86. [https://www.spider-smartmetergateway.de/cms/upload/pdf/IDAACS-Wireless2014\\_SMGS-Integrity\\_final.pdf](https://www.spider-smartmetergateway.de/cms/upload/pdf/IDAACS-Wireless2014_SMGS-Integrity_final.pdf).
- Dondossola, G., Garrone, F., Szanto, J. és Gennaro, F. (2008). Laboratóriumi tesztkörnyezet az energiahálózat-üzemeltetők interaktív IKT-infrastrukturái elleni kibertámadások értékelésére. *CIPRED szeminárium 2008: SmartGrids for Distribution*, 54-54. <https://doi.org/10.1049/ic:20080459>  
<https://doi.org/10.1049/ic:20080459>.
- Dondossola, G., Garrone, G., Szanto, J., Deconinck, G., Loix, T. és Beitollahi, H. (2009). A teljesítményszabályozó rendszerek IKT-rezilienciája: A CRUTIAL tesztkörnyezetek kísérleti eredményei. *2009 IEEE/IFIP International Conference on Dependable Systems & Networks*, 554-559.  
<https://doi.org/10.1109/DSN.2009.5270292>  
<https://doi.org/10.1109/DSN.2009.5270292>

---

Dragos Inc. (2017). *CRASHOVERRIDE Az elektromos hálózat működését fenyegető veszély elemzése*. <https://dragos.com/blog/crashoverride/CrashOverride-01.pdf>.

ENISA. (2012). *Intelligens hálózat biztonsága: Security Related Standards Guidelines and Regulatory Documents*. <https://www.enisa.europa.eu/topics/critical-information-infrastructures->.

and-services/smart-grids/smart-grids-and-smart-metering/smart-grid-security-related-standards-guidelines-and-regulatory-documents/view

- ENISA. (2016). Az ICS / SCADA rendszerek kommunikációs hálózati függőségei. <https://www.enisa.europa.eu/news/enisa-news/attacks-on-ics-scada-how-to-protect-critical-infrastructures>.
- Experten-Workshop 1. (2016). *Strom-Resilienz Experten-Workshop 1 Protokoll*.
- Experten-Workshop 2. (2017). *Strom-Resilienz Experten-Workshop 2 Protokoll*.
- Fischer, L. és Lehnhoff, S. (2019). IT-biztonság a funkcionális rugalmasságért az energiaiparban. Rendszerek. In M. Ruth and S. Goessling-Reisemann (Eds.), *Handbook on Resilience (Kézikönyv a rugalmasságról) of Socio-technical Systems* (pp. 316-340). Edward Elgar Publishing Limited.
- Fischer, L., Uslar, M., Morrill, D., Döring, M., and Haesen, E. (2018, October 30). *Tanulmány a kiber-incidensek kockázatainak értékeléséről és a kiber-incidensek megelőzésének költségeiről az energiaágazatban. Final Report*. [https://ec.europa.eu/energy/sites/ener/files/evaluation\\_of\\_risks\\_of\\_cyber-incidents\\_and\\_on\\_costs\\_of\\_preventing\\_cyber-incidents\\_in\\_the\\_energy\\_sector.pdf](https://ec.europa.eu/energy/sites/ener/files/evaluation_of_risks_of_cyber-incidents_and_on_costs_of_preventing_cyber-incidents_in_the_energy_sector.pdf)
- Friedberg, I., McLaughlin, K., and Smith, P. (2015). Az intelligens hálózatok kiber-fizikai ellenálló képességének kerete felé. In S. Latré, M. Charalambides, J. François, C. Schmitt, and B. Stiller (Eds.), *9th IFIP WG 6.6 International Conference on Autonomous Infrastructure, Management, and Security, AIMS 2015, Ghent, Belgium, June 22-25, 2015. Proceedings* (Vol. 9122, pp. 140-144). Springer, Cham. [https://doi.org/10.1007/978-3-319-20034-7\\_15](https://doi.org/10.1007/978-3-319-20034-7_15).
- Gaber, A., Seddik, K. G., and Elezabi, A. Y. (2015). Kibertámadások közös becslésfelderítése intelligens hálózatokban: Bayesi és nem-bayesi megfogalmazások. *2015 IEEE Wireless Communications and Networking Conference (WCNC): -Track 4 - Services, Applications, and Business Joint*, 2245-2250. <https://doi.org/10.1109/WCNC.2015.7127816>. <https://doi.org/10.1109/WCNC.2015.7127816>
- Ginter, A. (2017). *The Top 20 Cyberattacks on Industrial Control Systems*. <https://static.waterfall-security.com/Top-20-ICS-Attacks.pdf?submissionGuid=181753232c-9229-4b7f-987e-5288b36b017d>
- Goering, A., Meister, J., Lehnhoff, S., Jung, M., Rohr, M., and Herdt, P. (2016). Architektúra és minőségi szabványok a moduláris nyílt forráskódú szoftverek közös fejlesztéséhez a villamosenergia-hálózati elosztásirányítási rendszerekhez. *D-ACH+ Energy Informatics 2016*, 36-39. [http://www.energieinformatik2016.org/wp-content/uploads/2016/09/Proceedings\\_DACH-Energy-Informatics\\_ComForEn-2016-Web.pdf](http://www.energieinformatik2016.org/wp-content/uploads/2016/09/Proceedings_DACH-Energy-Informatics_ComForEn-2016-Web.pdf)
- Goessling-Reisemann, S. és Thier, P. (2019). A kritikus infrastruktúrák kockázatkezelése és ellenálló képességének kezelése közötti különbségről. In M. Ruth és S. Goessling-Reisemann (szerk.), *Handbook on Resilience of Socio-technical Systems (A társadalmi-technikai rendszerek rugalmasságának kézikönyve)*. (117-135. o.). Edward Elgar Publishing Limited.
- Gößling-Reisemann, S. (2016). Rugalmasság - Az energiarendszerek felkészítése a váratlan helyzetekre. In I. Link és V. Florin (szerk.), *IRGC Resource Guide on Resilience*. EPFL Nemzetközi Kockázatkezelési Központ (IRGC).
- Gößling-Reisemann, S., Wachsmuth, J., Stührmann, S., and von Gleich, A. (2013). Éghajlatváltozás és egy nagyvárosi energiarendszer strukturális sebezhetősége: Az

északnyugat-németországi Brema-Oldenburg esete. *Journal of Industrial Ecology*,  
17(6), 846- 858. <https://doi.org/10.1111/jiec.12061>. <https://doi.org/10.1111/jiec.12061>

Greveler, U. (2016). Die Smart-Metering-Debatte 2010-2016 und ihre Ergebnisse zum  
Schutz der Privatsphäre. *Datenbank-Spektrum*, 16(2), 137-145.  
<https://doi.org/10.1007/s13222-016-0219-4>. <https://doi.org/10.1007/s13222-016-0219-4>

- Hirschl, B., Aretz, A., Bost, M., Tapia, M., and Gößling-Reisemann, S. (2018). *Vulnerabilität und Resilienz des digital Stromsystems. Endbericht des Projekts "Strom-Resilienz"* (111. o.). Institut für ökologische Wirtschaftsforschung (IÖW) und Universität Bremen, Fachgebiet Resiliente Energiesysteme. [https://www.strom-resilienz.de/data/stromresilienz/user\\_upload/Dateien/Schlussbericht\\_Strom-Resilienz.pdf](https://www.strom-resilienz.de/data/stromresilienz/user_upload/Dateien/Schlussbericht_Strom-Resilienz.pdf)
- Huang, C.-C. és Kusiak, A. (1998). Moduláris felépítés a termékek és rendszerek tervezésében. *IEEE Transactions on Systems, Man, and Cybernetics - Part A: Systems and Humans*, 1, 66-77.
- IEC. (2016). *Villamosenergia-rendszerek irányítása és a kapcsolódó információcsere - Adat- és kommunikációs biztonság - 12. rész: Ellenálló képességre és biztonságra vonatkozó ajánlások elosztott energiaforrásokkal (DER) rendelkező kiberfizikai rendszerekkel rendelkező villamosenergia-rendszerek számára* (1.0). IEC. [https://webstore.iec.ch/preview/info\\_iec62351-12%7Bed1.0%7Den.pdf](https://webstore.iec.ch/preview/info_iec62351-12%7Bed1.0%7Den.pdf).
- IEC. (2020). *Intelligens hálózat szabványterkép. Architecture View.* <http://smartgridstandardsmap.com>.
- Nemzetközi Elektrotechnikai Bizottság (IEC). (2007). *IEC műszaki előírás TS 62351-1. Villamosenergia-rendszerek irányítása és a kapcsolódó információcsere - Adat- és kommunikációs biztonság. 1. rész: Kommunikációs hálózat- és rendszerbiztonság - Bevezetés a biztonsági kérdésekbe.*
- Interjúalany 1. (2016). [Személyes közlés].
- Interjúalany 2. (2016). [Személyes közlés].
- Interjúalany 4. (2016). [Személyes közlés].
- Interjúalany 5. (2016). [Személyes közlés].
- Interjúalany 6. (2016). [Személyes közlés].
- Interjúalany 8. (2017). [Személyes közlés].
- Interjúalany 9. (2017). [Személyes közlés].
- Interjúalany 12. (2017). [Személyes közlés].
- Interjúalany 13. (2017). [Személyes közlés].
- Interjúalany 14. (2017). [Személyes közlés].
- Interjúalany 15. (2017). [Személyes közlés].
- Interjúalany 17. (2017). [Személyes közlés].
- Interjúalany 18. (2017). [Személyes közlés].
- Interjúalany 19. (2017). [Személyes közlés].
- Iturbe, M., Camacho, J., Garitano, I., Zurutuza, U., and Uribeetxeberria, R. (2016). A folyamatzavarok és a behatolások megkülönböztetésének megvalósíthatóságáról a folyamatirányítási rendszerekben többváltozós statisztikai folyamatirányítással. *Proceedings of the 46th Annual IEEE/IFIP International Conference on Dependable Systems and Networks Workshop (DSN-W 2016)*, 2016, 155-160. <https://doi.org/10.1109/DSN-W.2016.32>.
- Jesse, B.-J., Heinrichs, H. U., and Kuckshinrichs, W. (2019). Az ellenálló képesség elméletének adaptálása az energiarendszerekre: Egy áttekintés és kilátások. *Energy, Sustainability and Society*, 9(1), 27. <https://doi.org/10.1186/s13705-019-0210-7>. <https://doi.org/10.1186/s13705-019-0210-7>.
- Kleineidam, G., Jung, G., Krasser, M., and Koch, B. (2016). A cellás megközelítés- A

mikro intelligens hálózatok biztonsága. *SPARKS Workshop Nov 2016.*

[https://www.researchgate.net/publication/301231063\\_The\\_Cellular\\_Approach\\_-\\_Security\\_of\\_Micro\\_Smart\\_Grids\\_biztonsága](https://www.researchgate.net/publication/301231063_The_Cellular_Approach_-_Security_of_Micro_Smart_Grids_biztonsága)

- Kleineidam, G., Krasser, M., and Reischböck, M. (2016). A celluláris megközelítés: Wunsiedel intelligens energiaregiója. Az intelligens hálózat, az intelligens mérés és az intelligens otthoni megoldások tesztkörnyezete. *Electrical Engineering*, 98(4), 335-340. <https://doi.org/10.1007/s00202-016-0417-y>.
- Knapp, E. (2011). 3. fejezet - Bevezetés az ipari hálózatok biztonságába. In *Industrial Network Security* (pp. 31-54). <https://doi.org/10.1016/B978-1-59749-645-2.00003-3>. <https://doi.org/10.1016/B978-1-59749-645-2.00003-3>.
- Knapp, E. és Samani, R. (2013). 3. fejezet - Az intelligens hálózat feltörése. In *Applied Cyber Security and the Smart Grid* (Syngress, pp. 57-86). <https://doi.org/10.1016/B978-1-59749-998-9.00003-7>.
- Kosut, O., Jia, L., Thomas, R. J., and Tong, L. (2010). A hamis adatokkal kapcsolatos támadások korlátozása az energiarendszer állapotbecslésében. *44th Annual Conference on Information Sciences and Systems, CISS 2010*, 1-6. <https://doi.org/10.1109/CISS.2010.5464816>. <https://doi.org/10.1109/CISS.2010.5464816>.
- Kush, N., Ahmed, E., Branagan, M., and Foo, E. (2014). Poisoned GOOSE: A GOOSE protokoll kihasználása. *AISC '14 Proceedings of the Twelfth Australasian Information Security Conference*, 149, 17-22.
- Kushner, D. (2013, február 26.). *A Stuxnet valódi története*. IEEE Spectrum: Technology, Engineering, and Science News. <https://spectrum.ieee.org/telecom/security/the-real-story-of-stuxnet>
- Langner, R. (2013). *To Kill a Centrifuge-A Technical Analysis of What Stuxnet's Creators Tried to Achieve to Achieve* (november; pp. 1-36). The Langner Group. <https://www.langner.com/wp-content/uploads/2017/03/to-kill-a-centrifuge.pdf>
- Lee, C., Zappaterra, L., Kwanghee Choi és Hyeong-Ah Choi. (2014). Az intelligens otthon biztonsága: Technológiák, biztonsági kihívások és biztonsági követelmények. *2014 IEEE Conference on Communications and Network Security*, 67-72. <https://doi.org/10.1109/CNS.2014.6997467>. <https://doi.org/10.1109/CNS.2014.6997467>.
- Lehnhoff, S. és Krause, O. (2013). Agentenbasierte Verteilnetzautomatisierung. In P. Göhner (Ed.), *Agentensysteme in der Automatisierungstechnik* (pp. 207-223). Xpert.press Springer-Verlag. [https://doi.org/10.1007/978-3-642-31768-2\\_12](https://doi.org/10.1007/978-3-642-31768-2_12)
- Liu, Y., Ning, P. és Reiter, M. K. (2011). Hamis adatinjekciós támadások az elektromos hálózatok állapotbecslése ellen. *ACM Transactions on Information and System Security*, 14(1), 1-33. <https://doi.org/10.1145/1952982.1952995>. <https://doi.org/10.1145/1952982.1952995>.
- Lopez, C., Sargolzaei, A., Santana, H., and Huerta, C. (2015). Smart Grid Cyber Security: An Overview of Threats and Countermeasures. *Journal of Energy and Power Engineering*, 9(7), 632-647. <https://doi.org/10.17265/1934-8975/2015.07.005>. <https://doi.org/10.17265/1934-8975/2015.07.005>.
- Lovins, A. B. és Lovins, L. H. (2001). *Törékeny hatalom - Energiastratégia a nemzetbiztonságért*. Brick House Pub. Co.
- Luijff, E. (2016). Fenygetések az ipari vezérlőrendszerekben. In E. J. M. Colbert és A. Kott (Eds.), *Cyber-security of SCADA and Other Industrial Control Systems* (pp. 69-93). Springer International Publishing. [https://doi.org/10.1007/978-3-319-32125-7\\_5](https://doi.org/10.1007/978-3-319-32125-7_5).
- Mangharam, R. és Pajic, M. (2013). Elosztott vezérlés kiberfizikai rendszerekhez. *Journal of the Indian Institute of Science*, 93(3), 353-388.

Marin Fernandes, P. (2012). 11. fejezet: Bevezetés az intelligens hálózatok kiberbiztonságába. In L. Berger and K. Iniewski (Eds.), *Smart Grid Applications, Communications, and Security* (pp. 229-320). John Wiley & Sons.

- Maynard, P., Mclaughlin, K., and Haberler, B. (2014). Towards Understanding Man-In-The-Middle Attacks on IEC 60870-5-104 SCADA Networks. *2nd International Symposium on ICS & SCADA Cyber Security Research 2014 (ICS-CSR 2014)*, Pages 30-42. <https://doi.org/10.14236/ewic/ics-csr2014.5>. <https://doi.org/10.14236/ewic/ics-csr2014.5>
- Mayring, P. (2014). *Minőségi tartalomelemzés: Elméleti alapok, alapvető eljárások és szoftveres megoldás*. <https://nbn-resolving.org/urn:nbn:de:0168-ssoar-395173>.
- McCarthy, J., Powell, M., Stouffer, K., Tang, C., Zimmerman, T., Barker, W., Ogunyale, T., Wynne, D., and Wiltberger, J. (2018). *Gyártó ipari vezérlőrendszerek biztosítása: Behavioral Anomaly Detection. NISTIR 8219*. <https://www.nccoe.nist.gov/sites/default/files/library/mf-ics-nistir-8219.pdf>
- McLaughlin, K., Friedberg, I., Kang, B., Maynard, P., Sezer, S., and McWilliams, G. (2015). 5. fejezet - Biztonságos kommunikáció az intelligens hálózatban: Hálózatok és protokollok. In F. Skopik and P. Smith (Eds.), *Smart Grid Security* (pp. 113-148). Syngress. <https://doi.org/10.1016/B978-0-12-802122-4.00005-5>
- Mo, Y., Kim, T. H.-J., Brancik, K., Dickinson, D., Perrig, A. és Sinopoli, B. (2012). Az intelligens hálózati infrastruktúra kiber-fizikai biztonsága. *Proceedings of the IEEE, 100(1)*, 195-209. <https://doi.org/10.1109/JPROC.2011.2161428>. <https://doi.org/10.1109/JPROC.2011.2161428>.
- Morgner, P., Mattejat, S., Benenson, Z., Müller, C., and Armknecht, F. (2017). Bizonytalan a tapintásig: A ZigBee 3.0 támadása a Touchlink üzembe helyezésén keresztül. *Proceedings of the 10th ACM Conference on Security and Privacy in Wireless and Mobile Networks - WiSec '17*, 230-240. <https://doi.org/10.1145/3098243.3098254>. <https://doi.org/10.1145/3098243.3098254>.
- NESCOR. (2015). *Villamosenergia-ágazat meghibásodási forgatókönyvei és hatáselemzései - 3.0. verzió*. <http://smartgrid.epri.com/doc/NESCOR Failure Scenarios v3 12-11-15.pdf>
- New Jersey Cybersecurity & Communications Integration Cell. (2017). *Stuxnet*. NJCCIC. <https://www.cyber.nj.gov/threat-profiles/ics-malware-variants/stuxnet>.
- Nissim, N., Yahalom, R., and Elovici, Y. (2017). USB-alapú támadások. *Computers and Security, 70*, 675-688. <https://doi.org/10.1016/j.cose.2017.08.002>. <https://doi.org/10.1016/j.cose.2017.08.002>
- NIST. (2014). *National Institute of Standards and Technology Interagency Report 7628 Rev. 1*. <https://doi.org/10.6028/NIST.IR.7628r1>
- Qi, J., Hahn, A., Lu, X., Wang, J., és Liu, C.-C. (2016). Az elosztott energiaforrások és az intelligens inverterek kiberbiztonsága. *IET Kiber-fizikai rendszerek: Theory & Applications, 1(1)*, 28-39. <https://doi.org/10.1049/iet-cps.2016.0018>. <https://doi.org/10.1049/iet-cps.2016.0018>
- Rossebo, J. E. Y., Wolthuis, R., Fransen, F., Bjorkman, G., and Medeiros, N. (2017). Továbbfejlesztett kockázatértékelési módszertan az intelligens hálózatokhoz. *Computer, 50(4)*, 62-71. <https://doi.org/10.1109/MC.2017.106>. <https://doi.org/10.1109/MC.2017.106>.
- Rubin, H. és Rubin, I. (2005). *Minőségi interjúkészítés (2. kiadás): Az adatok meghallgatásának művészete*. SAGE Publications, Inc. <https://doi.org/10.4135/9781452226651>
- Schauer, S., König, S., Latzenhofer, M., and Rass, S. (2017). A kockázatok azonosítása és kezelése az összekapcsolt közműhálózatokban. 79-86. [http://www.thinkmind.org/index.php?view=article&articleid=securware\\_2017\\_5\\_20\\_3\\_0042](http://www.thinkmind.org/index.php?view=article&articleid=securware_2017_5_20_3_0042)

---

Sobczak, B. (2019, május 6.). **Szakértők értékelik a károkat az amerikai hálózatot ért első kibertámadás után.**

Biztonság. <https://www.eenews.net/stories/1060281821>

SPARKS konzorcium. (2016). *Deliverable D3.3 Smart Grid Security Standards Recommendations*. [https://project-sparks.eu/wp-content/uploads/2014/04/D-3-3\\_SmartGridSecurityRecommendations.pdf](https://project-sparks.eu/wp-content/uploads/2014/04/D-3-3_SmartGridSecurityRecommendations.pdf)

- Stirling, A. (2007). Általános keret a tudomány, a technológia és a társadalom sokszínűségének elemzéséhez. *Journal of the Royal Society Interface*, 4(15), 707-719. <https://doi.org/10.1098/rsif.2007.0213>.  
<https://doi.org/10.1098/rsif.2007.0213>
- Strauss, A. L. és Corbin, J. M. (2010). *Megalapozott elmélet: Grundlagen qualitativer Sozialforschung* (Unveränd. Nachdr. der letzten Aufl). Beltz.
- Styczynski, J. és Beach-Westmoreland, N. (2017). *Amikor kialudtak a fények. Az ukrán kritikus infrastruktúrát ért 2015-ös támadások átfogó áttekintése*. <https://www.boozallen.com/content/dam/boozallen/documents/2016/09/ukraine-report-when-the-lights-went-out.pdf>
- Tapia, M., Thier, P. és Gößling-Reisemann, S. (2020). Ellenálló kiber-fizikai energiarendszerek kiépítése. *TATuP - Zeitschrift Für Technikfolgenabschätzung in Theorie Und Praxis*, 29(1). <https://doi.org/10.14512/tatup.29.1.23>.
- Tazi, K. és Abdi, F. (2015). Az intelligens hálózat kiber-fizikai biztonságának áttekintése: Attacks and Defense Mechanisms (Támadások és védelmi mechanizmusok). 3. *Nemzetközi Megújuló és Fenntartható Energia Konferencia (IRSEC)*, 1-6. <https://doi.org/10.1109/IRSEC.2015.7455127>.  
<https://doi.org/10.1109/IRSEC.2015.7455127>.
- Teixeira, A., Kupzog, F., Sandberg, H., and Johansson, K. H. (2015). 6. fejezet - Kiberbiztonsági és ellenálló architektúrák ipari vezérlőrendszerekhez. In F. Skopik és P. Smith (szerk.), *Smart Grid Security: Innovative Solutions for a Modernized Grid* (149-183. o.). <https://doi.org/10.1016/B978-0-12-802122-4.00006-7>.  
<https://doi.org/10.1016/B978-0-12-802122-4.00006-7>
- VDE. (2015). *Der Zellulare Ansatz: Grundlage einer erfolgreichen, regionenübergreifenden Energiewende*. VDE ETG (Energietechnische Gesellschaft im VDE). <http://www.vde.com/de/fg/ETG/Arbeitsgebiete/V2/Aktuelles/Oeffenlich/Seiten/VDEETG-StudieDerZellulareAnsatz.aspx>
- Virsec. (2017. május 7.). Virsec Hack elemzés: Deep Dive into Industroyer (aka Crash Override). *Virsec Systems*. <https://virsec.com/virsec-hack-analysis-deep-dive-into-industroyer-aka-crash-override/>
- von Gleich, A., Gößling-Reisemann, S., Stührmann, S., Woizeschke, P. és Lutz-Kunisch, B. (2010). Resilienz als Leitkonzept - Vulnerabilität als analytische Kategorie. In K. Fichter, A. von Gleich, R. Pfriem, and B. Siebenhüner (Eds.), *Theoretische Grundlagen für erfolgreiche Klimaanpassungsstrategien. Nordwest2050 Berichte Heft 1* (pp. 13-49). Projektkonzorcium "nordwest2050".
- von Oheimb, D. (2012). Az intelligens mérés és az intelligens hálózat informatikai biztonsági architektúrájának megközelítései. *Smart Grid Security*, 1-25. [https://doi.org/10.1007/978-3-642-38030-3\\_1](https://doi.org/10.1007/978-3-642-38030-3_1). [https://doi.org/10.1007/978-3-642-38030-3\\_1](https://doi.org/10.1007/978-3-642-38030-3_1).
- von Oheimb, D. (2013). Az intelligens mérés és az intelligens hálózat informatikai biztonsági architektúrájának megközelítései. In J. Cuellar (Ed.), *Smart Grid Security* (pp. 1-25). Springer Berlin Heidelberg. [https://link.springer.com/chapter/10.1007/978-3-642-38030-3\\_1](https://link.springer.com/chapter/10.1007/978-3-642-38030-3_1).

## A. függelék: Interjúelemzés Módszertan

### Szakértői interjúk

Ahhoz, hogy megfelelő adatokat nyerjünk a releváns helyszíni forrásokból, a szakértői interjúkat választottuk az adatok előállításának optimális módszerének (Rubin és Rubin, 2005). A cél az volt, hogy olyan interjúpartnereket találjunk, akiknek az informatikai vagy az energiaágazatban szerzett hosszú távú szakértelme megalapozott áttekintést nyújthat a terület releváns témáiról. Végül 19 interjút készítettünk az informatikai, energetikai és automatizálási területek szakértőivel, valamint állami szervekkel. Az interjúk mindegyikét angol nyelven készítettük, átirtuk, majd tovább elemeztük (Mayring, 2014) alapján.

### Kérdőív

A félig strukturált interjúkhoz használt kérdések az alábbiakban szerepelnek:

#### **Szakmai információk**

1. Mi az Ön iskolai és szakmai háttere?
2. Jelenleg milyen munkakörben dolgozik? Mióta?
3. Le tudná írni jelenlegi munkakörét?
  - 3.1. Hogyan kapcsolódik az intelligens hálózatokhoz?
  - 3.2. Hogyan kapcsolódik ez az intelligens hálózatok kiberbiztonságához?
4. Részt vesz-e szervezetén belül az intelligens hálózatok kiberbiztonságával kapcsolatos K+F projektben?
  - 4.1. Ha igen, leírná röviden?

#### **Az intelligens hálózatok kiberbiztonságával és a kockázatértékeléssel kapcsolatos tanulmányok ismerete**

5. Számos szabvány, iránymutatás és ajánlás foglalkozik az intelligens hálózatok kiberbiztonságával és különösen a kockázatértékeléssel. Ilyen például az Egyesült Államok Nemzeti Szabványügyi és Technológiai Intézete (NIST) által kidolgozott jelentés: "Guidelines for Smart Grid Cyber Security (NIST-IR 7628)".
  - 5.1. Ismeri e kezdeményezések némelyikét?
  - 5.2. Tud más tanulmányról, amely az intelligens hálózatok kiberbiztonsági kérdéseivel foglalkozik Németországban, Európában és/vagy világszerte?
    - 5.2.1. Ha igen, meg tudná nevezni és röviden leírni őket?

#### **Kiberbiztonsági sebezhetőségek az intelligens hálózatokban**

Az alábbi intelligens hálózati referenciaarchitektúra-modellt \*(lásd (IEC, 2020)) figyelembe véve és az intelligens hálózati funkciók teljes körű megvalósítását feltételezve:

6. Véleménye szerint melyek az intelligens hálózat fő kiberbiztonsági kihívásai, amelyekkel foglalkozni kell? Miért?
7. A referenciaarchitektúra-modellben meg tudná határozni, hogy mely komponensek (áramellátó berendezések vagy információs eszközök) a potenciálisan legsebezhetőbbek?
  - 7.1. Melyek képviselnek különleges érdeklődést az Ön szakterületén?
  - 7.2. Milyen okokból?
8. Melyek azok a zavarok/események, amelyek hatással lehetnek a rendszer szolgáltatásaira?

9. Milyen lehetséges hatása lehetnek ezeknek a zavaroknak/eseményeknek?
10. Melyek a releváns stresszorok/agresszorok e zavarok/események bekövetkezése szempontjából?
  - a) emberek

- b) szervezetek
  - c) veszélyek
  - d) egyéb: kérjük, nevezze meg
11. Az alábbi területeken milyen feltételek segítik elő e zavarok/események bekövetkezését?
- a) technológia
  - b) szervezet/struktúra
  - c) gazdaság/szabályozás
  - d) kultúra/társadalom
12. Szándékos zavarok esetén, milyen lehetőség van arra, hogy ezeket a zavarokat/eseményeket a gyakorlatban is megvalósítsák, akár a jelenlegi, akár a jövőbeli energiarendszerekben?
- 12.1. Mik lennének a támadási mechanizmusok?
13. Mi szükséges, vagy mit kell módosítani annak érdekében, hogy megelőzzük az ilyen szándékos vagy nem szándékos zavarok/események előfordulását?
14. Milyen meglévő (vagy jövőbeli) alkalmazkodási lehetőségek vannak a rendszer szolgáltatásainak helyreállítására?
- 14.1. Mit lehetne tenni technikai és szervezeti szinten egy ilyen helyreállítás érdekében?
15. Hogyan tanulhatunk a múltbéli eseményekből és az úgynevezett "majdnem balesetekből"?
16. Mikor és milyen mértékben lehet végrehajtani a meghatározott alkalmazkodási intézkedéseket?
17. Kik azok a szereplők és intézmények, akik részt vesznek ezen alkalmazkodási lehetőségek kidolgozásában és végrehajtásának szabályozásában? A következőktől:
- energiaágazat
  - IT-szektor
  - szabályozó hatóságok
  - a piac

### **Rendszer szemcsézettsége**

Figyelembe véve a villamosenergia-rendszerek fejlődését a termelés, a fogyasztás és az irányítás szempontjából, amely a teljesen centralizált rendszertől egy granulárisabb vagy decentralizált rendszer felé halad:

18. Hogyan befolyásolná a rendszer szemcsézettsége az előzőekben azonosított perturbációkkal szembeni kitettséget és érzékenységet?
19. Hogyan befolyásolná a rendszer szemcsézettsége az ezek kezelésére azonosított intézkedéseket?

## **A tartalomelemzés áttekintése módszertan**

A kvalitatív tartalomelemzés módszertanának középpontjában az interjúadatokból szisztematikusan levezetett kódrendszer felépítése áll, miközben egy sor módszertani szabály mentén dolgozik (Mayring, 2014). A kvalitatív tartalomelemzés a hangsúlyt a kódok megkonstruálására és megalapozására helyezte a korábban lefolytatott szakértői interjúk adatai alapján (Mayring, 2014). A kódrendszerek az első elemzési lépések kiindulópontja és eredménye is egyben, miközben hozzájárulnak e módszertani megközelítés megbízhatóságához. Mivel ez a módszertan is erősen elméletvezérelt, ezek a kódok elméleti kategóriákként szolgálnak, amelyek az adatok tematikus szempontjaihoz, az

előzetes ismeretekhez és a korábbi tanulmányokhoz igazodnak. Ezeket a kódokat olyan szövegrészekkel töltöttük fel az anyagból, amelyek releváns tartalmat tartalmaznak, és megfelelnek a tematikus irányultságnak vagy a kategorikus kód témájának. További információ a kódolásról

folyamatot, amely a nyílt kódolással mint elemzési eszközzel foglalkozik (Mayring, 2014), a következő szakaszban ismertetjük.

Fontos továbbá, hogy az aktuális kutatási és elméleti szempontokat a tartalomelemzés minden lépésébe bevonjuk (Mayring, 2014). Ebben a projektben mind a szakirodalmi áttekintés, mind a sérülékenységvizsgálat módszertanának eredményei, beleértve a módszer mögött álló elképzeléseket is, jelentős szerepet kaptak a tartalomelemzés elvégzésében. A tartalomelemzés másik kritériuma az objektivitás. Ezt a kódolók közötti megbízhatósággal lehet elérni, amely egy olyan kutatási eszköz, amelynek célja a különböző kutatók kódjainak összehasonlítása és a tartalom kódolásának módja közötti különbségek keresése. Ez az eszköz több kutatót biztosít, és foglalkozik a helyhatár problémáival és a szöveges anyag túlságosan eltérő értelmezésével (Mayring, 2014). Továbbá a használt alapadatanyag pontos meghatározását, valamint annak eredetét kell figyelembe venni. Az elemzendő alapanyag minden nyelvi adatból, képből, sőt videóból is állhat. A leggyakoribb adatforrás az átírt interjúk formájában kerül bemutatásra (Mayring, 2014). A pontos kutatási kérdés meghatározása után meg kell állapodni az elemzési folyamat további részében. Ennek során az elemzési lépések a kutatási témától és a tartalomelemzés választott speciális módszerétől függően változhatnak (Mayring, 2014). Ezek a speciális technikák a szöveges adatok feldolgozásának különböző formáira összpontosítanak: a strukturálásra, az explikálásra és az összegzésre.

Ehhez a projekthez az összegzés technikáját választottuk. A cél itt az volt, hogy a kiinduló anyagot csökkentsük, miközben a fő tartalom és a jelentés érintetlenül marad. A (Mayring, 2014) által javasolt standard összefoglalási eljárást, amelyet ebben a tanulmányban használtunk, röviden ismertetjük:

- A kezdeti kódolás után a kódolt szövegrészeket parafráztuk, hogy egységes nyelvi szintet érjünk el. Itt először a kiinduló szöveganyagot redukálták, mivel az elhangzásuk szerint átírt szövegrészeket nyelvtani rövidítésekkel alakították át. A fő tartalom és a szerkezet ezekben a parafrázisokban is megmaradt, míg a jelentést vagy releváns tartalmat nem tartalmazó, lényegtelen elemeket törölték (Mayring, 2014).
- A parafrázálás után az anyagot még egyszer összesűrítték. Ehhez a lépéshez az absztrakciós szintről állapodtak meg, hogy ezeket a parafrázisokat szerkesszék. Mindent, ami a kívánt szint alatt volt, megtartottak a további absztrakció és általánosítás céljából, mindent, ami e szint felett volt, úgy hagytak, ahogy volt. Az azonos tartalmú parafrázisokat integrálták, a releváns jelentést nem tartalmazókat pedig kihagyták (Mayring, 2014).
- Az összegzés második fordulójában a parafrázisokat egymásba integrálták. Ily

módon a kívánt absztrakciós szintű kategóriák jöttek létre. Ezzel együtt egy előzetes kategóriarendszer, amely összefoglalókat tartalmazott minden egyes releváns

téma az anyagból származott. Ezt követően az eredeti kódrendszer, a kategóriák és a parafrázisok felülvizsgálatával ellenőrizték, hogy az alpanyagot továbbra is megfelelően reprezentálják-e. Ha a kiinduló adatok reprezentációja kielégítő volt, az összefoglalókat tovább csökkentették és integrálták, amíg el nem érték a kívánt koncentrátsági szintet (Mayring, 2014).

Ami a kódrendszer felépítését illeti, a módszertan szerint ez többféleképpen történhet: induktív, deduktív vagy a kettő keverékeként. Az induktív felépítés azt jelenti, hogy a kódolási folyamat megállapításakor még nem lesz kódrendszer. Ehelyett a kódolási folyamat és az anyag egymás utáni összekapcsolása során az adatokból fog kialakulni. A kódok közvetlenül az anyagon keresztül jönnek létre, először a kívánt absztrakciós szintre vonatkozó szelektív kritériumok levezetésével, majd az érdeklődés tárgyát képező téma szempontjából releváns tartalmak kiválasztásával. Ebben a lépésben szem előtt kell tartani a kutatási kérdést. A kódolás során az anyagot teljes egészében átnézzük, és kódokat konstruálunk és kódolással töltjük ki. Az első kódolási kör után a kódok ellenőrzésének és felülvizsgálatának újabb fordulója szükséges, hogy az összes kódot a teljes anyaggal együtt kódoljuk (Mayring, 2014).

A kódok deduktív felépítése azt jelenti, hogy egy korábban generált kódrendszerből indulunk ki, amely figyelembe veszi az összes elméleti háttér, a szakirodalmi áttekintést és a kutatási témát. Ez az előzetes kódrendszer ezután a kódolás és az összegzés fent leírt folyamatainak megy keresztül (Mayring, 2014).

A kódok generálásának utolsó módja a deduktív-induktív. Egyesíti az elméleti háttér, a kutatási hipotézis és a korábbi ismeretek mentén felépített előzetes kódrendszer előnyeit azzal az előnnyel, hogy a kódrendszer a kódolási folyamat során újra átnézhető, felülvizsgálható és átdolgozható (Mayring, 2014). Ezt a módszert választottuk megfelelő kiindulópontnak ebben a tanulmányban, mivel a VA elemei kódokként használhatók az első kódrendszerhez. Ezután a szakértői interjúkból származó kijelentéseket e kódok szerint kategorizáltuk, majd ennek megfelelően felülvizsgáltuk.

Az interdiszciplináris és vegyes módszertani projekt követelményeinek való megfelelés érdekében a tartalomelemzés szokásos eljárását meg kellett változtatni. Ezért a parafrázis és a redukció folyamata lerövidült, mivel a szakértők nyilatkozatai nagyon specifikusak és tematikusan koncentráltak voltak. Ez nagyobb szövegszegmensek kódolásához vezetett. Ezeket a szegmenseket ezután parafrázták, a szállított jelentésre összpontosítva, hogy állandó artikulációs szintet érjenek el. Ahelyett azonban, hogy a közvetlen beszéd szegmenseit rövidítésekkel alakítottuk volna át, egész mondatokat építettünk fel, hogy az érvek szerkezetét megőrizzük, és előkészítsük őket a későbbi összegzésekhez. A parafrázisokat ezután minden egyes

kutató, annak érdekében, hogy megbizonyosodjon arról, hogy a tartalom és a jelentés helyesen lett-e kinyerve és sűrítve.

Ezekkel az átfogóbb parafrázisokkal elkészültek az első összefoglalók a VA-módszertanhoz. A teljes mondatokban megfogalmazott és átfogóbb parafrázisok kiválasztásának oka az volt, hogy könnyebb legyen különbséget tenni a különböző szakértőktől származó kijelentések között.

Később, amikor a reziliencia stratégia fázisai kidolgozásra kerültek és bekerültek a kódrendszerbe, az anyagot ismét ezekkel az új kategóriákkal kódolták és parafrázták. Ezeket a parafrázisokat is összefoglalták, hogy minden főbb kódból átfogó szöveget kapjanak. Ezek az összefoglalók különböző kijelentéseket tartalmaznak, amelyeket a fentiekben leírtak szerint szétbontottak és redukáltak.

A kódolási rendszerből származó parafrázált állításokat témájuk szerint rendeztük. Az azonos témára vonatkozó, de különböző interjúalanyoktól származó kijelentéseket egymásba integráltuk. Hangsúlyt fektettünk arra, hogy a kijelentések sajátos szerkezetét és jelentését megőrizzük, hogy meg lehessen különböztetni a különböző szakértők kijelentéseit.

## Kódolás tartalom

Ebben a szakaszban a nyílt kódolás folyamatát részletesebben ismertetjük, hogy bemutassuk, hogyan elemeztük kezdetben a dokumentumokat, és így készítettük elő őket a tartalomelemzési módszertanra.

A megalapozott elmélet módszertanán alapuló nyílt kódolás nagyon jól alkalmas az anyag megnyitására az elemzés korai szakaszában és az első kategóriák kialakítására. Ez az eredeti adatok osztályozásával, fogalomalkotásával és kategorizálásával történik (Strauss és Corbin, 2010). A folyamat során a folyamatos összehasonlítás révén az adatok konkrétságot és pontosságot kapnak, amely során az anyaghoz kérdéseket is felvetünk - mit közvetít, hogyan fejezi ki, miért éppen azt a szót választották, milyen kontextusban írják le a szövegrészt, milyen jelentést közvetít? (Strauss és Corbin, 2010). Így fokozatosan egyre több fogalmat határoznak meg az adatokból, amelyeket aztán csoportokká egyesítenek, amelyekből jelenségeket lehet levezetni (Strauss és Corbin, 2010). A fogalmakat tehát megfelelően el kell nevezni. Ez történhet saját magunk által, vagy közvetlenül a szövegrészletből levezetett és elfogadott in vivo kódok segítségével (Strauss és Corbin, 2010). A fogalmak és jelenségek levezetése után jönnek létre az első kategóriák, amelyek dimenzionalitásokat tartalmaznak, és tükrözik a bennük szereplő fogalmak tulajdonságait (Strauss és Corbin, 2010).

A nyílt kódolásnak különböző módszerei vannak. Így az anyagot soronként, vagy még

pontosabban, szóról szóra lehet megtekinteni. Ez a legrészletesebb és egyben leghatékonyabb megközelítés, mivel a lehető legtöbb kategóriát lehet kiszűrni a szövegből.

(Strauss és Corbin, 2010). Ez különösen fontos a korai elemzési fázisokban, hogy a további eljárás során ellenőrizhető és felülvizsgálható kategóriák sokaságát hozzuk létre.

A következő kódolási módszer a szövegrészletekre összpontosít mondatonként vagy bekezdésenként. Itt a szakaszok fő gondolatait szűrik ki és hasonlítják össze a többi fogalommal. Ez különösen akkor alkalmas, ha egyes kategóriák már léteznek, és azokat tematikus környezetükben kell kódolni (Strauss és Corbin, 2010).

A harmadik megközelítés a teljes dokumentumok megtekintése. A fő cél a más dokumentumoktól való eltérések azonosítása vagy a dokumentum általános kontextusának megkülönböztetése (Strauss és Corbin, 2010). Eszerint a nyílt kódolás sajátos módon vezet a forrásanyag kezeléséhez annak érdekében, hogy első elméleti építőelemeket lehessen levezetni tartalommal teli kategóriák formájában. Éppen ezért a módszer alkalmas az interjúadatok tartalmi elemzésére és kategorizálására oly módon, hogy további elemzési lépések következhetnek.

A dokumentumok kódolásának másik módja a tengelykódolás. A tartalomelemzés lehetővé teszi ezt a lépést a kódolás első körét követően, hogy az adatokat egy meglévő kódrendszerre összpontosítva ellenőrizze. De az is lehetséges, hogy csak axiális kódolást végezzenek, ha egy már meglévő kódrendszert kell validálni. Ez azért fontos, hogy a meglévő kódok megfelelő kategóriáknak bizonyuljanak, és elegendő jelentést tartalmazzanak. Az anyagot a kódrendszerek mellett tekintik át, és folyamatosan összevetik vele. A meglévő kódokra való szigorú összpontosítás a meglévő kódok javítása és kitöltése érdekében különösen akkor szükséges, ha egy már létező kódrendszert használnak. Ebben az esetben a kódolás első fordulója biztosítja, hogy a meglévő kódok elegendőek legyenek, ellenkező esetben újakat kell létrehozni. A kódolás második fordulója biztosítja, hogy az összes dokumentum bekerüljön az újabb kódok közé, és megerősíti, hogy a meglévő kódok még mindig a megfelelő kategóriákba tartoznak-e. A kódolás második fordulójának befejezése után a kódrendszer pontosabbá és strukturáltabbá válik. Ha nem így van, további kódolási és újrakódolási körökre kerülhet sor, amíg a strukturáltság és a telítettség kielégítő szintjét el nem érjük (Mayring, 2014).

Az alábbiakban ismertetjük a tanulmányban elvégzett kódolási folyamatot:

- Az interjúk átiratából származó szövegrészleteket olyan kategóriákkal kódoltuk, amelyek egy adott témát tartalmaztak. Ezek a témák lehetnek: általános információk a szakmai információkról, vagy olyan tartalmak, amelyek a VA kategóriái vagy a reziliencia stratégia szempontjából relevánsak voltak. A konkrét témát tartalmazó teljes szövegrészletet a megfelelő kategóriába soroltuk.
- A kódolás első fordulója a nyílt kódolás előnyeit ötvözte a tengelyes kódolás fókuszával.

- A nyílt kódoláshoz hasonlóan az anyagból új kódokat vezettek le, és az anyagot kezdetben kódolásra bontották. Axiális kódolás az előzetes kódrendszerrel (8. táblázat)

biztosította, hogy a kódokat ebben a kódrendszerben megfelelően töltötték ki, így nyerve megbízhatóságot és érvényességet.

- Az is fontos volt, hogy minden, a tartomelemzésért felelős kutató elvégezte a kódolás teljes körét, beleértve az összes dokumentumot. Ezt követően a kódrendszert minden kutató egy teljes átkódolási menetnek vetette alá. E lépés során minden egyes kódoláson belüli kódolást áttekintettek, a következő pontok ellenőrzésére összpontosítva:  
(a) a kódolás a megfelelő kódhoz tartozik-e, vagy további strukturálásra volt szükség, b) a kód továbbra is közvetíti-e az eredeti tematikus irányultságát, c) a kód elég tartalmat közvetített-e ahhoz, hogy továbbra is kategória maradjon, vagy d) a kódnak egy másik fő kód alkódjának kell-e lennie.
- A kutatócsoport közösen felülvizsgálta az így kapott kódrendszert, amely az elemzési lépés során jelentős változásokon ment keresztül, mivel úgy döntöttek, hogy megváltoztatják a struktúrát, és felveszik a reziliencia stratégia fázisait, valamint a VA elemekre vonatkozó részek némi strukturálását. Ezzel az új kódrendszerrel egy újabb kódolási és átkódolási kör következett.

Az így kialakított kódrendszer (9. táblázat) megbízhatónak bizonyult a megkérdezett szakértők által átadott tartalom megragadására.

táblázat A szakértői interjú és a műhelytalálkozók alapján kialakított kezdeti kódrendszer

A kódok listája
Kódrendszer
Munkaterület
Kihívások
Nyílt kategória
Szakmai és oktatási háttér
Jelenlegi munkakör
Kutatási projekt
Szabályzat
Érzékeny eszközök
Humán erőforrás
Adminisztratív személyzet
Elektromos operátorok
IT-üzemeltetők
Kiberinfrastruktúra-eszközök
Elektromos infrastruktúra eszközök
Perturbációk
Külső zavarás
Belső zavarás
Potenciális hatások

Kiberinfrastruktúra
Bizalmasság
Visszautasíthatatlanság
Elérhetőség
Integritás
Elektromos infrastruktúra
Áramkimaradások
Nagy áramkimaradás
Kisebb áramkimaradás
Minőségi kritériumok
Közvetett paraméterek
Nyilvános elfogadás
Gazdasági hatások
A műszaki paraméterekre gyakorolt hatások
Stresszorok
Egyéb
Veszélyek
Lebomlás
Emberi hibák
Szervezetek
Emberek
Külső stresszor (P)
Belső stresszor (P)
Feltételek
Egyéb
Társadalom
Szabályzat (feltételek)
Gazdaság
Szervezet
Technológia
Támadási mechanizmusok
Megvalósíthatóság
Motiváció
Szint
Erőfeszítés
Tudás
Alkalmazkodási stratégiák
Előkészítés
Kihívások (előkészítés)
Megelőzés
Kihívások (Prev)
Érzékelés
Kihívások (Det)
Válasz
Kihívások (Resp)

Helyreállítás
Kihívások (Rec)
Tanulás
Kihívások (Lear)
Alkalmazkodási stratégiák végrehajtása
Hajlandóság a végrehajtásra
Végrehajtási hajlandóság
Közreműködő színészek
Piac
Egyéb
Szabályozó hatóságok
IT-szektor
Energiaágazat
A rendszer szemcsézettsége
Alacsony granularitás
Nagyfokú granularitás

táblázat Végleges kódrendszer, amely a megkérdezett szakértők által átadott tartalmakat rögzíti, és amelyet a sebezhetőségek értékeléséhez és az ellenálló képességet fokozó intézkedések levezetéséhez használtak fel.

A kódok végleges listája
Kódrendszer
Új kategóriák
Bizonytalan kommunikáció
Expozíció és érzékenység
Támadási mechanizmus és zavarok
Potenciális hatások
Alkalmazkodási stratégiák, végrehajtás
Bizonytalan végpontok
Expozíció és érzékenység
Támadási mechanizmus és zavarok
Potenciális hatások
Alkalmazkodási stratégiák, végrehajtás
Bizonytalan interfész a különböző gyártók összetevői között
Expozíció és érzékenység
Támadási mechanizmus és zavarok
Alkalmazkodási stratégiák, végrehajtás
nem megfelelő változás- és konfigurációkezelés
A helytelen beállítások károsítják a rendszert vagy lehetővé teszik a hozzáférést
A szoftver és a firmware lehetővé teszi a jogosulatlan módosítást
Expozíció és érzékenység
Támadási mechanizmus és zavarok
Potenciális hatások
Alkalmazkodási stratégiák, végrehajtás
Webszolgáltatásokban futó rendszerek



Támadási mechanizmus és zavarok
Potenciális hatások
Alkalmazkodási stratégiák, végrehajtás
"Szakértő" üzemeltetők hiánya
Expozíció és érzékenység
Támadási mechanizmus és zavarok
Potenciális hatások
Alkalmazkodási stratégiák, végrehajtás
IT-OT szakértők hiánya a szervezetben
Expozíció és érzékenység
Támadási mechanizmus és zavarok
Potenciális hatások
Alkalmazkodási stratégiák, végrehajtás
Helytelen hálózati szegregáció
Expozíció és érzékenység
Támadási mechanizmus és zavarok
Potenciális hatások
Alkalmazkodási stratégiák, végrehajtás
Nem megfelelő biztonsági javítások kezelése
Expozíció és érzékenység
Támadási mechanizmus és zavarok
Potenciális hatások
Alkalmazkodási stratégiák, végrehajtás
A biztonsági előírások hatékony végrehajtásának hiánya
Expozíció és érzékenység
Potenciális hatások
Alkalmazkodási stratégiák, végrehajtás
A biztonságtudatosság hiánya a szervezetekben
Expozíció és érzékenység
Támadási mechanizmus és zavarok
Potenciális hatások
Alkalmazkodási stratégiák, végrehajtás
A fogyasztók biztonságtudatosságának hiánya
Expozíció és érzékenység
Támadási mechanizmus és zavarok
Potenciális hatások
Alkalmazkodási stratégiák, végrehajtás
Nincs gazdasági ösztönzés a beruházásra / összehangolt erőfeszítések hiánya
Expozíció és érzékenység
Támadási mechanizmus és zavarok
Potenciális hatások
Alkalmazkodási stratégiák, végrehajtás
Rendszerhibák
Expozíció és érzékenység
Potenciális hatások

Alkalmazkodási stratégiák, végrehajtás
Hibaforgatókönyvek
Rugalmassági stratégiák
Alkalmazkodási stratégiák végrehajtása
Hajlandóság a végrehajtásra
Végrehajtási hajlandóság
Az ellenálló képességgel kapcsolatos kihívások
Kihívások (előkészítés)
Kihívások (Prev)
Kihívások (Det)
Kihívások (Resp)
Kihívások (Rec)
Kihívások (Lear)
Alkalmazkodási stratégiák
Előkészítés és megelőzés
Előkészítés
Megelőzés
Megbízható és elővigyázatos tervezés végrehajtása
Érzékelés
Válságkezelés és válságból való kilábalás
Válasz
Helyreállítás
Tanuljon a jövőért
Tanulás
A rendszer szemcsézettsége
Meghibásodások és üzemzavarok
Támadások és hatások
Biztonsági megoldások és válaszmechanizmusok
Cellák és mikrorácsok
Központosított architektúrák
Decentralizált architektúrák
Általános kódok
Közreműködő színészek
Nyílt kategória
Kihívások
Szabályzat
Szakértői információk és kutatási projektek
Kutatási projekt
Szakmai és oktatási háttér
Munkaterület