Ellátásbiztonság – felelősség – cselekvőképesség

2021. április 29.

Dr. Grabner Péter
energetikai szakértő

Átalakuló működés – változó gazdasági feltételrendszer (1)

- Az elmúlt évtized biztonság- és energiapolitikai fejleményei egyértelműen azt jelzik, hogy újra kell értékelni a vezetékes energiaellátó rendszerek üzemeltetésének biztonsági feltételrendszerét.
- A villamos energetikában a hagyományos megközelítés alapján az ellátás biztonságának két kulcseleme volt:
  - a fizikai infrastruktúra (hálózati elemek) megfelelő állapota és rendelkezésre állása, valamint
  - a megfelelő mértékű erőművi tartalékok megléte.
- A szokásos hálózattervezési módszertanok alapján az úgynevezett (n-1) elv alkalmazásával a nagyfeszültségű hálózatok működése megfelelően biztosítottnak tűnt azzal, hogy az egyes főberendezések, illetve távvezetékek kiesése ellenére, az ellátás alternatív útvonalon megszervezhetővé vált.
- A fő szabály mellett azonban már eddig is voltak olyan kritikus hálózati csomópontok, ahol a tervezés szigorított kritériumok mellett történt (tipikusan ilyen lehet jelentősebb erőművek környezete).

Átalakuló működés – változó gazdasági feltételrendszer (2)

- A közép- és kisfeszültségű hálózatokon normál üzemi körülmények között olyan hálózati alakzatok kialakítására törekedtek a hálózatüzemeltetők, hogy üzemzavar esetén az ellátás folyamatossága távműködtetett átkapcsolásokkal, véges idő alatt biztosítható legyen
- Az erőművi tartalékok tekintetében az elmúlt évtized radikális átalakulást eredményezett.
  - Gazdasági és környezetvédelmi okok miatt számos korábban fontos hazai erőmű működése (pl. Tisza, Vértes) ellehetetlenült, majd
  - ennek következtében megnövekedett az import villamos energia részaránya, illetve
  - egyre nagyobb ütemben kezdett terjedni az elosztott villamosenergia-termelés, amelynek kontrollja, illetve a rendszerszabályozásba történő bevonása egyre összetettebb infokommunikációs eszközök alkalmazását igényli.

Az ellátásbiztonság összetevői (jellemzői)

Elkind alapján az energiaellátás (minden energiaforrás esetén értelmezhető) biztonságának négy összetevője van („*Energy Security: Call for a Broader Agenda*” In Carlos Pascual and Jonathan Elkind (Eds.) *Energy Security: Economics, Politics, Strategies, and Implications* (Washington, DC: Brookings Institution Press), pp. 119-148. 2010):

1. **Rendelkezésre állás (availability):** a felhasználók (fogyasztók) számára rendelkezésre áll a szükségletüknek megfelelő kapacitás és megfelelő mennyiségű energia. Ennek feltétele a megfelelő szabályozási környezet, a kiszolgálást lehetővé tevő technológiai rendszerek és az azok megújításához szükséges befektetések léte.
2. **Megbízhatóság (reliability):** az energetikai technológiai rendszerek megfelelő védelemmel rendelkeznek az ellátási zavarok kivédésére (pl. az diverzifikált energiaforrások, technológiák és szállítási útvonalak; tájékoztatás a működéssel összefüggésben; energiaforrás és technológiai tartalékok)
3. **Megfizethetőség (affordability):** a lehető legalacsonyabb, a jövedelmekhez képest méltányos és stabil árak
4. **Fenntarthatóság (sustainability):** a társadalmi, környezeti és gazdasági károk olyan minimalizálása, amely hosszú távon fenntartható energetikai rendszerek eredményez.

Vannak ettől részben eltérő felosztási módok is, de a fenti bontás általánosan használt (idézett) megközelítést tartalmaz (pl. WEF felosztás).

Kockázatok és fenyegetések a villamosenergia-rendszerben

- A piaci működés zavarai
  - *Pl. A likviditás hiánya, versenykorlátozó magatartás, árszabályozási korlátok, nem megfelelő hatósági kontroll, a támogatási rendszerek problémái*
- A fizikai infrastruktúra biztonságos működése és ellenállóképessége
  - *Pl. Az infrastruktúra tervezésének, létesítésének és üzemeltetésének nem megfelelő megvalósítása, külső (emberi) hatások miatt bekövetkező sérülések*
- Klimatikus és geotechnikai hatások miatti zavarok
  - *Pl. Szélsőséges időjárási hatások fokozott megjelenése, földrengés, árvíz*
- Elöregedő infrastruktúra (erőművek, hálózatok)
  - *Pl. A beruházásokat elnehezítő szabályozási környezet, különadók, kiszámíthatatlan piacszabályozás, az innováció hiánya, a piaci működés által elnehezített banki finanszírozás*
- Az új technológiák illesztése a meglévő rendszerekhez
  - Pl. Időjárásfüggő termelőkapacitások, P2X, tárolás
- A szakképzett munkaerő hiánya
  - *Pl. Nem megfelelő szakképzés, nem megfelelő bérezési rendszer, pandémia,*
- Kiberbiztonsági fenyegetések
- Együttes kiberbiztonsági és fizikai fenyegetés, illetve bármely egyéb kockázatok kombinációja

Elrettentő műveletek lehetőségei a kibertérben

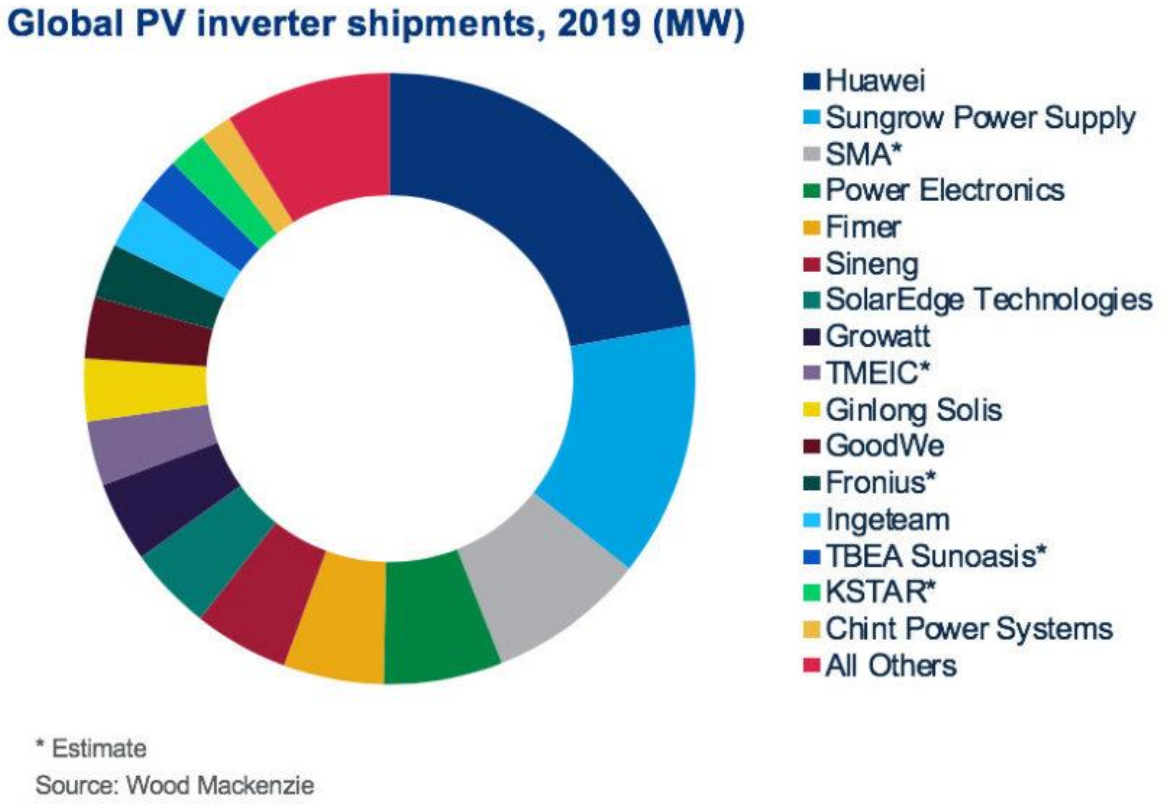
Szereplő	Súlyosság (szándékolt vagy tényleges)		
	Az erő alkalmazását megelőző állapot	Erő alkalmazása	Katonai támadás
Állami szereplő	Nem kényszerítő jellegű ellenintézkedések (beleértve a kibertámadásokat is)	Nem kényszerítő jellegű ellenintézkedések vagy korlátozott megtorlások (beleértve a kibertámadásokat is)	Erő alkalmazása az önvédelem érdekében egy idegen állam ellen
Nem állami szereplő közvetlen, vagy közvetett állami irányítás alatt	Nem kényszerítő jellegű ellenintézkedések (beleértve a kibertámadásokat is állami és nem állami célpontok ellen)	Nem kényszerítő jellegű ellenintézkedések vagy korlátozott megtorlások (beleértve a kibertámadásokat is állami és nem állami célpontok ellen)	Erő alkalmazása az önvédelem érdekében egy idegen államhoz köthető szereplő ellen
Nem állami szereplő csekély mértékű állami befolyással	Nem kényszerítő jellegű ellenintézkedések, de csak akkor, ha a befogadó állam nem hajlandó fellépni a támadók ellen		Erő alkalmazása az önvédelem érdekében az idegen állam területén lévő nem állami szereplő ellen, de csak akkor, ha a támadót befogadó állam nem akar, vagy nem képes fellépni.

Forrás: ANU NARAYANAN, JONATHAN WILLIAM WELBURN, BENJAMIN M. MILLER, SHENG TAO LI, AARON CLARK-GINSBERG: Deterring Attacks Against the Power Grid, **RAND Corporation**, 2020. és saját szerkesztés

Milyen inverter szállítóktól függ az ellátásbiztonság?

Ezek az eszközök nem csak a villamosenergia-rendszerhez jelentenek csatlakozási pontot, hanem az informatikai rendszerekhez is!

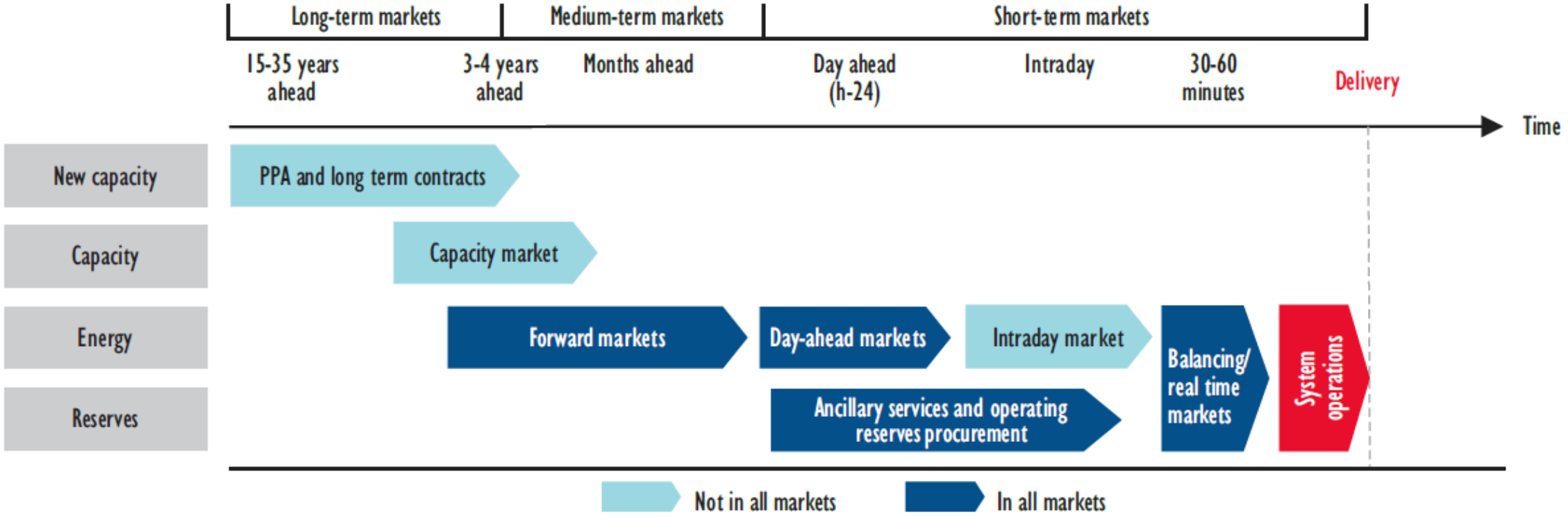
IoT?



Hogyan lehet úgy biztonsági szabályozást kialakítani, hogy a működtetéssel kapcsolatos feltételek sem egyértelműek?
Lehet-e műszaki-biztonsági szabályozást alkotni politikai keretben?

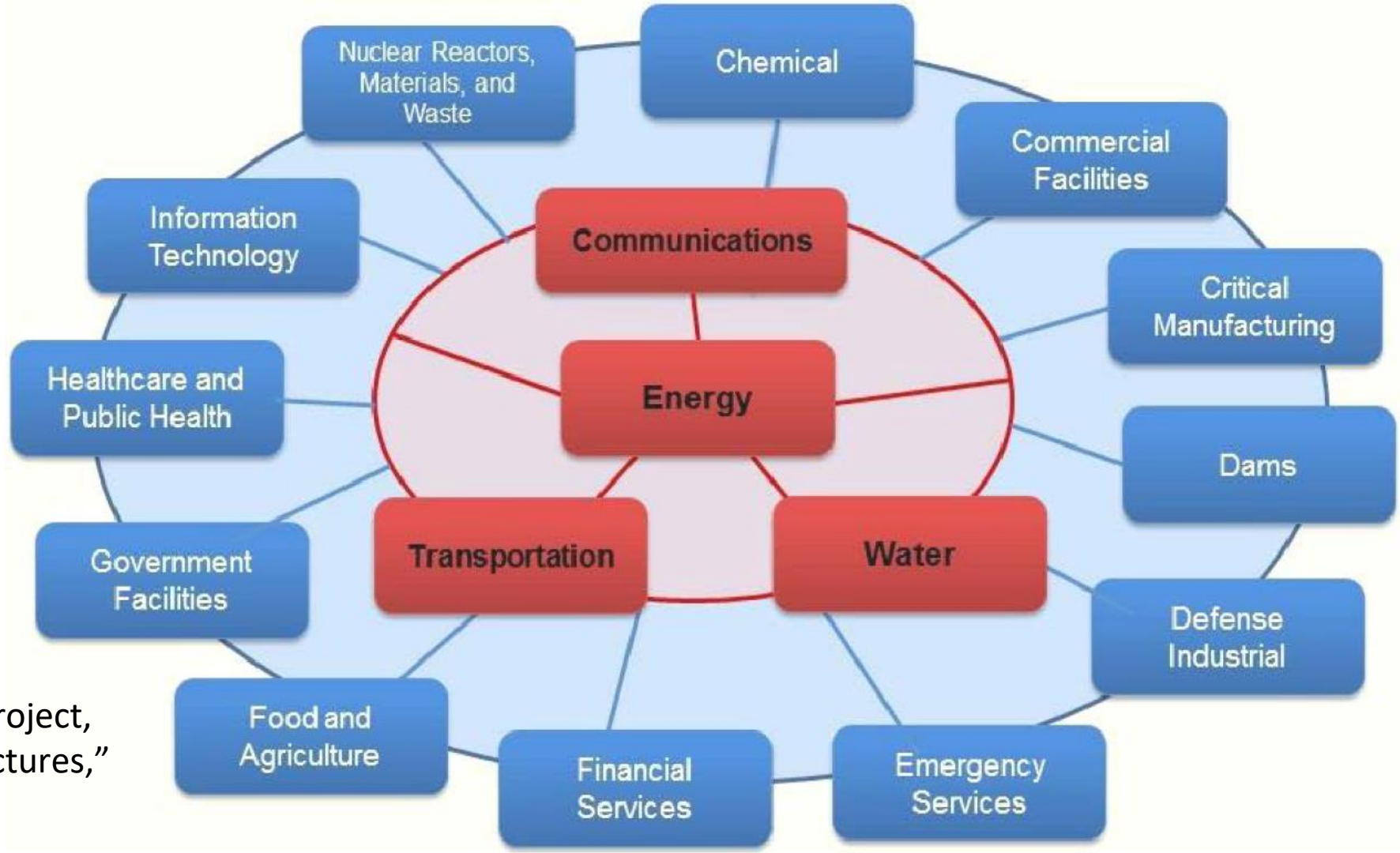
A villamosenergia-termelők működésével kapcsolatos jellemző időtávok

A kockázatok időtávjainak szemléltetése



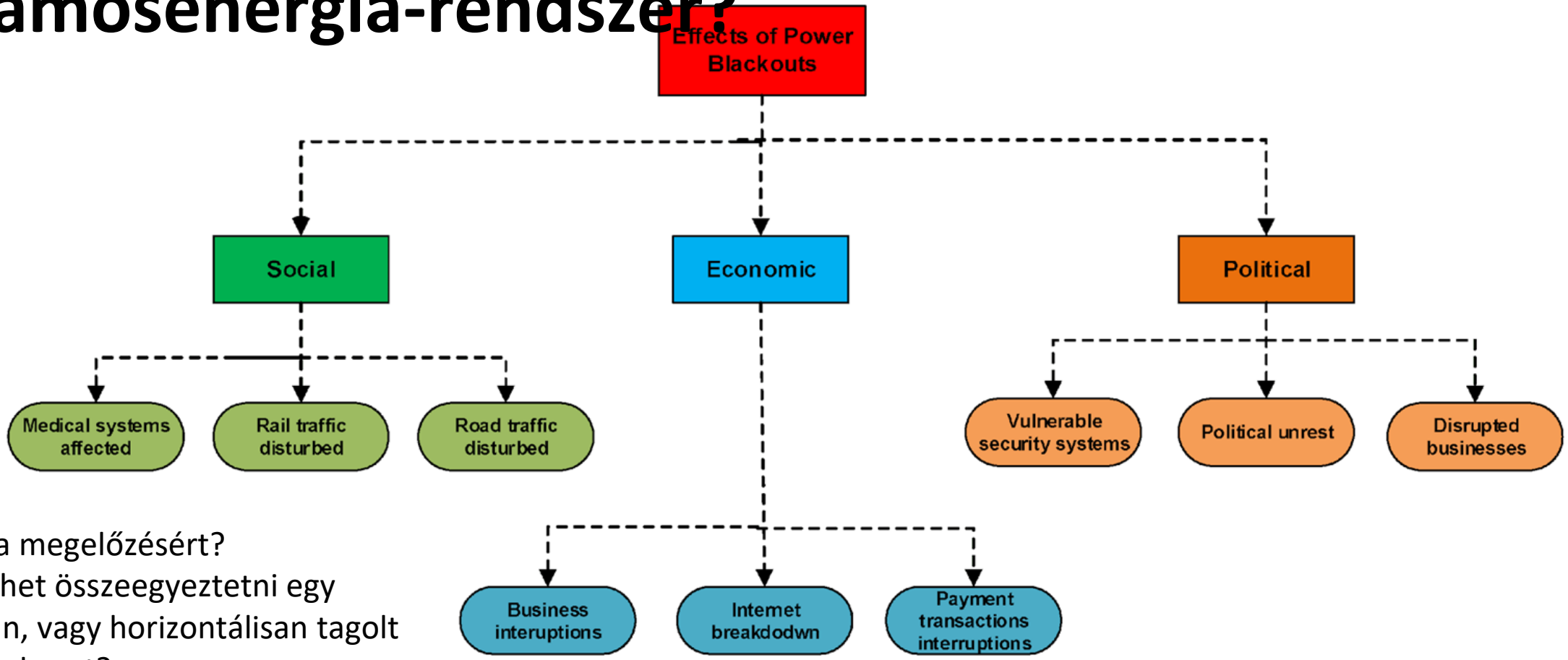
Forrás: IEA Re-powering Markets: Market design and regulation during the transition to low-carbon power systems, 2016

A kritikus infrastruktúra rendszerek kölcsönös függőségei



Forrás: H2020 700416, SUCCESS project, "Securing Critical Energy Infrastructures,"

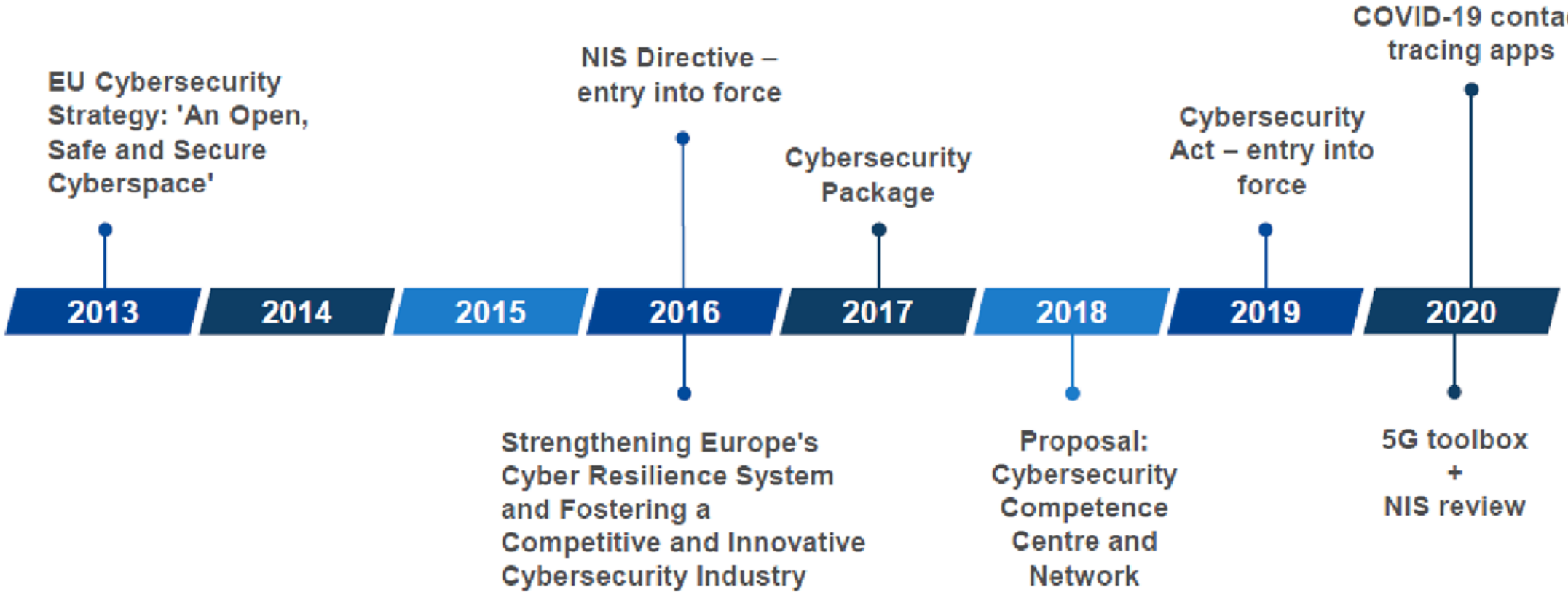
Mi történhet, ha összeomlik egy villamosenergia-rendszer?



- Ki felelős a megelőzésért?
- Hogyan lehet összeegyeztetni egy vertikálisan, vagy horizontálisan tagolt szabályrendszert?

Az összetett kihívásokra nincsenek egyszerű válaszok. Csak a szisztematikus felkészülés segíthet.

Az EU kiberbiztonsági szabályozásának főbb történései



3rd Energy Package → Clean Energy Package → Green Deal

Néhány a villamosenergia-rendszer működési biztonsága szempontjából releváns EU szabályozás

- A Európai Parlament és a Tanács 2019. június 5-i (EU) **2019/941** rendelete a villamosenergia-ágazati kockázatokra való felkészülésről és a 2005/89/EK irányelv hatályon kívül helyezéséről
  - A preambulum bemutatja a **horizontális jogszabályi kapcsolódások**at is!
  - a villamosenergia-ipari vállalkozások és a fogyasztók a villamosenergiaellátási válságok leküzdése során a lehető leghosszabb ideig az (EU) 2019/943 rendeletben és az (EU) 2019/944 irányelvben meghatározott piaci mechanizmusokra támaszkodjanak

- Az Európai Parlament és a Tanács 2019. június 5-i (EU) **2019/943** rendelete a villamos energia belső piacáról
  - *„59. cikk (2) bekezdésében a Bizottság felhatalmazást kap arra, hogy … jogi aktusokat fogadjon el e rendelet kiegészítésére a következő területekre kiterjedő üzemi és kereskedelmi szabályzatok kidolgozása céljából:*

    *e) ágazatspecifikus szabályok a határkeresztező villamosenergia-áramlások **kiberbiztonsági szempontjaira**, ideértve a közös minimumkövetelményekre, a tervezésre, a nyomon követésre, a jelentéstételre és a válságkezelésre vonatkozó szabályokat.*”

Új Network Code készítése (NC CS)

- Az ACER-t a keretjellegű iránymutatást készít elő a kibervédelem tárgykörben a 2019/943 rendelet alapján.
- Az iránymutatást a 2021. májusban induló nyilvános konzultációt követően terjesztik a BoR (Board of Regulators) elé szavazásra, a Bizottság felé júliusban kell megküldeni. ACER várakozásai szerint az NC CS elfogadására 2022 elején kerülhet sor, átültetése 2022. Q2-től indulhat.
- Az NC CS-ben a szabványok (és azok frissítései) kiemelt szerepet kapnak majd. Nincs egyetlen általános szabvány, csak szabványok „készletek”. A jelenlegi tervek szerint:
  - határkeresztező-kockázatelemzést kell végezni,
  - minimum kiberbiztonsági szabványokat és funkcionális követelményeket kell meghatározni a teljes villamos energia értékláncra,
  - Információgyűjtési követelményeket kell meghatározni,
    - Ez különösen kritikus, hiszen itt kellene elrendezni, hogy milyen információkat és hogyan kellene megosztani!
  - meg kell védeni az EU-s kritikus információkat.
- Egyelőre fontos alapelvnek tűnik, hogy a megalkotásra kerülő közös szabályok esetében az ACER-nek lesz jóváhagyási jogköre (vélhetően az egyéb ügyekben szokásos eljárások szerinti logikával), akinek ki kell kérni az ENISA (European Union Agency for Cybersecurity) véleményét.

Néhány változás a hazai szabályozásban

- Módosításra került:
  - 2012. évi CLXVI. törvény (Lrtv.)
  - 65/2013. (III. 8.) Korm. rendelet (Lrtv. Vhr.)
  - A villamosenergia-rendszer jelentős zavara és a villamosenergia-ellátási válsághelyzet esetén szükséges intézkedésekről szóló 280/2016. (IX. 21.) Korm. rendelet
- Hatályon kívül helyezve:
  - 360/2013. (X. 11.) Korm. rendelet (Energetikai ágazati kormányrendelet)
- Új jogszabály:
  - 374/2020. (VII. 30.) Korm. rendelet (új Energetikai ágazati kormányrendelet)

További módosítások is szükségesek lesznek

EU 2019/941 és NC CS

VET / Vhr módosítás

280/2016 (IX. 21.) rendelet módosítás

Üzemi Szabályzat / Krízisterv