2019. 09. 17.
Debrecen
Mechwart András Ifjúsági Találkozó

Budapesti Műszaki és Gazdaságtudományi Egyetem

A villamosenergia-rendszer kiberfizikai biztonsága

Molnár Martin

konzulens: Dr. Vokony István

Agenda

Rendszerirányítás	**Hálózat**	**EMS/SCADA**
Smart Grid	**Struktúrák**	**SCADA integráció**
Kiberbiztonság	**Veszélyek és kockázatok**	**Támadások és védelmi módok**

Korszerű villamosenergia-rendszerek

Hálózati rendszerirányítás, EMS/SCADA rendszerek, Smart Grid koncepció

Hálózati rendszerirányítás

Definíció: az átviteli hálózati rendszerirányító (Transmission System Operator – TSO) a szabályozási zóna irányítását végzi, hatásköre az elosztóhálózat fölé terjed ki, mely elsősorban a nagyfeszültségű átviteli hálózatot, az erőműveket és NaF/NaF alállomásokat foglal magába.

Feladatok:

- hurkolt NaF átviteli hálózat üzemeltetése
- átviteli hálózatba termelő erőművek irányítása
- Kapcsolattartás az elosztói engedélyesekkel (DSO)
- **számítógépes támogatás**

EMS/SCADA rendszerek

A számítógépes támogatás legfőbb oka, hogy hatalmas mennyiségű offline és online **adatot** kell kezelni: információgyűjtés, elemzés, számítások és tárolás.

SCADA (Supervisory Control and Data Acquisiton):

- **online**, **real-time** elosztott irányítórendszer
- főbb feladatai a névből is adódó szabályozás és adatgyűjtés

EMS (Energy Management System):

- alkalmazott adatkezelések és számítások, ezek alapján energiaelosztás
- nincsen egységesített struktúra

A Smart Grid koncepció

A **decentralizált** ,,okos" hálózatban jelentős mértékben jelenik meg **elosztott termelés** és a **kommunikációs** infrastruktúra. A SG lényegében **real-time** monitoring és **kétirányú** digitális kommunikáció által megvalósított **dinamikus** microgrid-menedzsment különböző technológiák alkalmazása mellett.

Az irányítási egységek kapcsolatban állnak egymással, és több villamos szolgáltatás is **együttműködik**. Az optimális működést robosztus **információs** irányítórendszer biztosítja. Legfőbb előnyei **lehetnek**:

- *megbízható, rugalmas és biztonságos energiaelosztás*
- *optimalizált hálózati forgalom, DSM*
- *csökkentett veszteségek, rövidebb hibaidők, hatékonyabb működés*

Modern hálózati infrastruktúra

A Smart Grid definíciója és modelljei, SCADA és SG struktúra

A Smart Grid definíciója

Nincsen! ☺ Néhányan azért próbálkoztak, például:

- *„Továbbfejlesztett villamos hálózat mely kétirányú digitális kommunikációval és intelligens mérő-monitorozó rendszerrel került kibővítésre.”* – Európai Bizottság
- *„Olyan villamos hálózat, amely hatékonyan építi be saját működésébe a hozzá csatlakozó felhasználók és komponensek viselkedését és tevékenységét …”* – The European Smart Grid Task Force

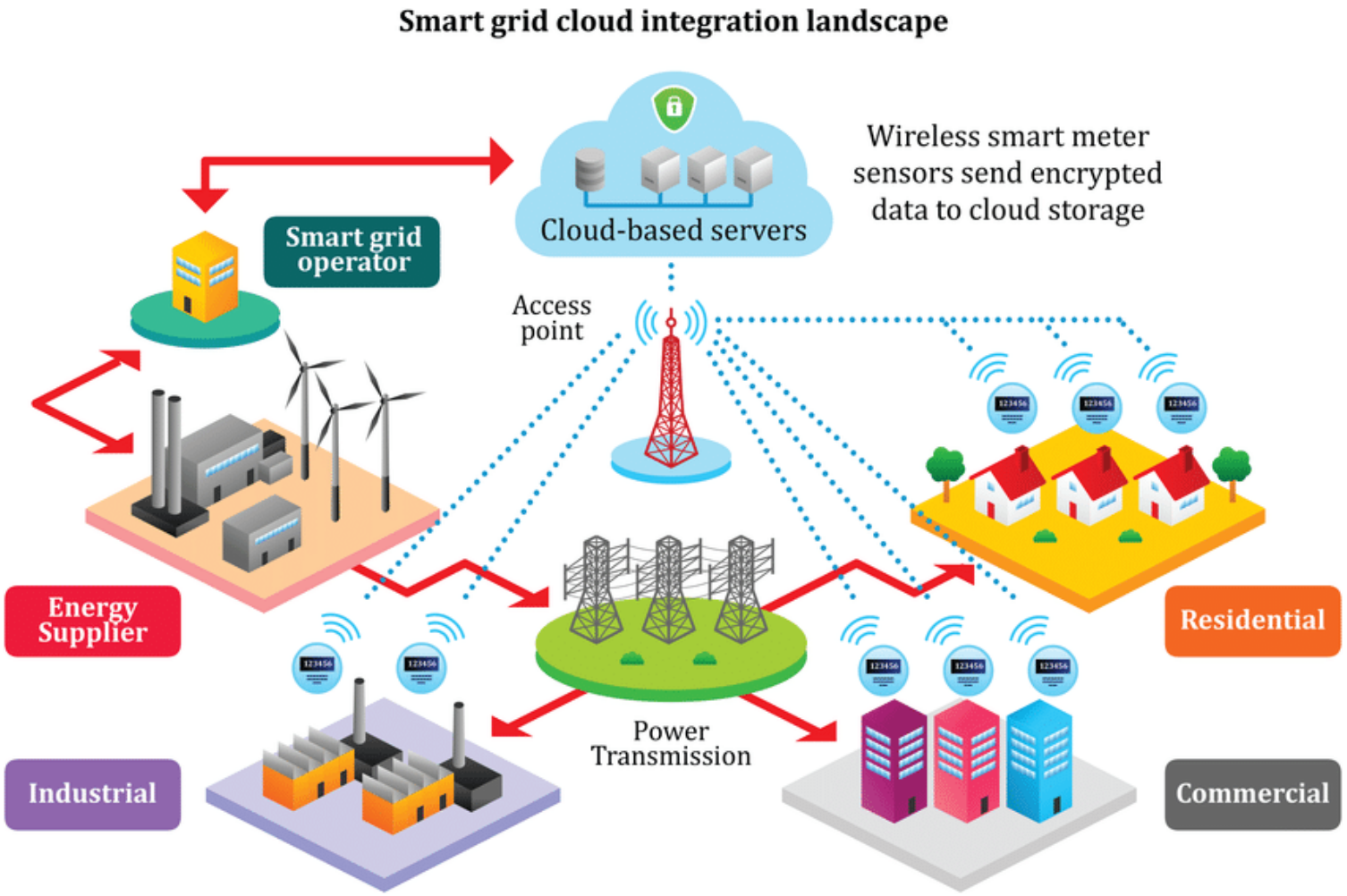
Leggyakrabban centralizált hálózathoz hasonló felépítéssel lehet találkozni, viszont egyre népszerűbb a rétegzett struktúra.

Centralizált Smart Grid struktúra

Közös kapcsolódási pont a felhő-alapú szerverekhez.

Külön egységként jelennek meg: energiatermelés, -szállítás, -elosztás és különböző felhasználások.

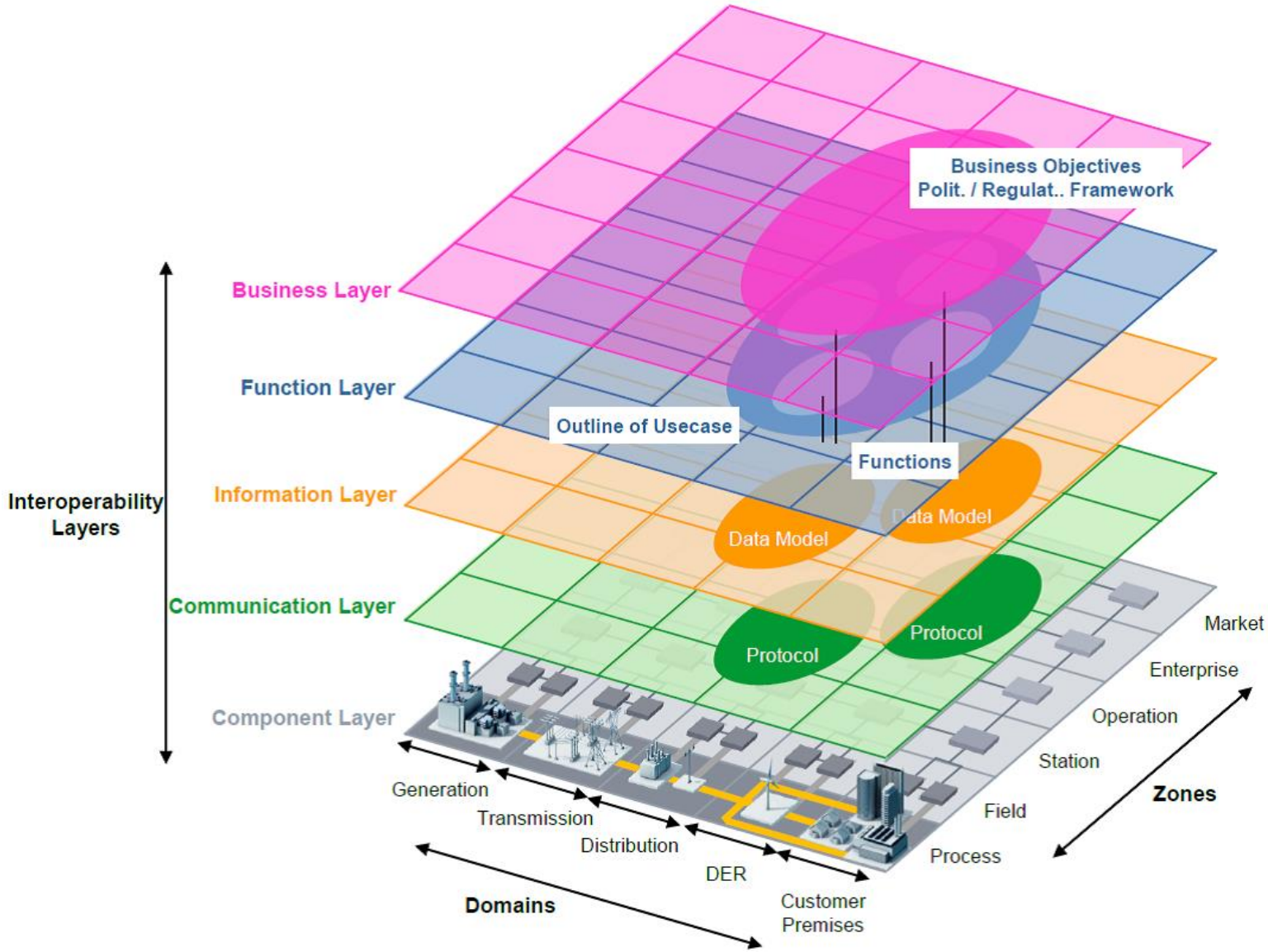
Komplexitás?



Rétegzett SG felépítés

Moduláris megközelítés szerint jól elkülöníthető az 5 szint a hálózatban betöltött szerepek alapján.

Ezek jól beleillenek a SCADA rendszerek rétegjeibe: fizikai, kommunikációs, adat és szoftverréteg. Utóbbit a funkcionális és üzleti/felhasználói szint közösen alkotja az elosztott alkalmazások révén.



SCADA rendszerek felépítése

Nincsen standard, de általánosságban 5 részre bonthatók.

Fizikai alrendszer: folyamatok, berendezések, szenzorikák, automatikák, különböző mechanizmusokat működtető eszközök.

Kiberfizikai kapcsolat: fizikai réteg adatait adott szállítási platformon el kell juttatni az irányítórendszerhez, hogy az felhasználhassa őket.

Elosztott irányító-alrendszer: kétirányú kommunikációra képes, összeköti a rendszerirányítást a fizikai szinttel jelfeldolgozás és válasz valamilyen logika szerint (PLC, MTU, RTU, IED).

Hálózati infrastruktúra: felső szintű irányítást köti össze az alrendszerekkel, protokoll alapú kommunikációt és hálózati forgalomirányítást biztosít.

(Al- és) Végrendszerek: lehetőség biztosítása a folyamatos monitorozásra és távvezérlésre ,,historian” rendszerek által HMI-ken keresztül.

Kapcsolat a SCADA és SG felépítések között

Komponens szint: fizikai alrendszerek és az összes hálózati működést biztosító berendezés.

Kommunikációs réteg: hálózati kapcsolatok kiépítési és működtetésére használt szabványok és protokollok.

Információs/adatréteg: hatalmas mennyiségű adat, általában felhő-alapú adatbázis struktúrában tárolva.

Funkcionális szint: irányíthatóságot megvalósító számítások, műveletek, logikák és vezérlések.

Felhasználói szint: távvezérlést és távműködtetést megvalósító HMI-k és grafikus felületek, melyeken keresztül az egész rendszer elérhető.

Kiberbiztonsági alapok

Kritikus infrastruktúrák veszélyei, Támadási modellek és típusok, Védelmi mechanizmusok

Veszélyek a kritikus infrastruktúrákban

Hárompillérű alapvető elvárások: **megbízhatóság**, **hitelesség** és **információ-biztonság**.

A hagyományoktól eltérő módon **csökken a szegmentáltság**, hiszen nagy az ellátás korlátlanságára irányuló törekvés. Emiatt minimalizálódnak vagy esetenként akár el is tűnnek a fizikai határok.

Az **Internet of Things** trendje jól megfigyelhető a kritikus infrastruktúráknál, így a villamosenergia-rendszernél is.

A vizsgálódás szempontjából kiemelt fontossággal bírnak a **fizikai**, **információ-biztonsági** és **pénzügyi** következményekkel járó veszélyek.

Támadási modellek

A kritikus infrastruktúrák **komplexitásából** fakadóan számos típusú támadás létezik, melyek **strukturális** ismerete elengedhetetlen a megfelelő védelmi mechanizmus kialakításához.

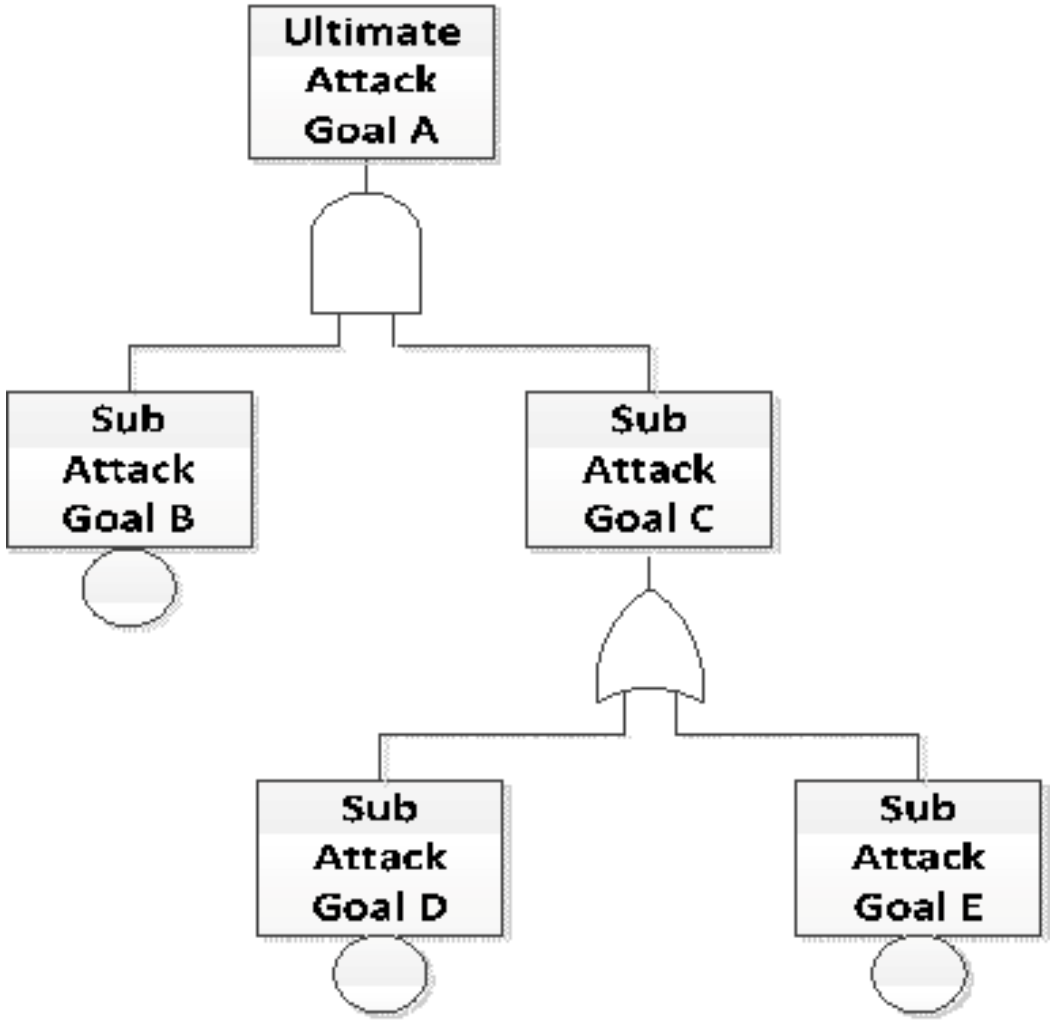
Sokszínűségük miatt kihívást jelentő feladat általános modellezésük és vizsgálatuk, azonban a **támadási fa** jó megközelítést ad. Ez lehetőséget biztosít a **támadások** és **résztámadások megismeréséhez** és **logikai megértéséhez**, a mély működési mechanizmusokról nem szolgáltat információt.

Támadási fa

Segítségével jól megfigyelhető a támadások elérésének módja.

Elemezhető, hogy milyen résztámadások által juthatunk el a végső célig, illetve vizsgálható a köztük lévő logikai kapcsolat is (AND, OR, NOR, NAND, XOR).

Forrás: https://www.semanticscholar.org/paper/Security-Analysis-on-Cyber-physical-System-Using-Xie-Lu/7ce025a4a59e3cd348135262c9ff97f2914a2678/figure/0



Támadási típusok és csoportok

Több csoportba sorolhatók aszerint, hogy a kritikus rendszer sebezhetőségét milyen irányból használják ki. Számos megközelítés létezik erre, a valósághoz legközelebb azonban talán az alábbi áll:

- **hardver** irányú
- **szoftver** irányú
- **kommunikáció** irányú

A kategorizálások azonban nem diszjunktak, így az előbbit például tökéletesen kiegészíti a következő csoportbontás: hagyományos **IT** alapú, **protokoll**-specifikus, **konfiguráció** alapú és **irányítófolyamatok** elleni támadások.

Védekezési módszerek és lehetőségek

A Smart Grid és SCADA rendszerek ellen számos különböző támadás követhető el, melyeket ráadásul folyamatosan továbbfejlesztenek és kombinálják egymással.

Az adott támadások megismerése elengedhetetlen, azonban általános védekezi stratégia ezen az útvonalon nem alakítható ki.

Egy újabb megközelítés szerinte nem a támadások elhárítására, hanem azok megelőzésére kell törekedni, vagy esetleg a behatolások károkozás előtti felismerésére, azonosítására.

Cél: IDS (Intrusion Detection System) és ADS (Anomaly Detection System), azaz behatolás- és anomáliafelismerő-rendszerek fejlesztése.

Aktuális kihívások és jövőbeli tervek

Jelenleg megoldandó feladatok a témában:

- gyakorlatban is alkalmazható ADS-IDS rendszerek fejlesztése
- testbed kialakítása

Terveim a kutatásban:

- támadások megismerése, modellezése, hatásuk vizsgálata
- létező ADS-IDS fejlesztések tanulmányozása
- új **IDS platform** és hozzá tartozó **mini testbed** fejlesztése

Köszönöm szépen a figyelmet!

Várom az esetleges kérdéseket!