Budapesti Műszaki és Gazdaságtudományi Egyetem
Villamosmérnöki és Informatikai Kar
Villamos Energetika Tanszék

Molnár Martin

Szimulációs keretrendszer tervezése villamosenergia-rendszer elleni kiberfizikai támadások vizsgálatához

Tudományos Diákköri Konferencia

KONZULENS

Dr. Vokony István

BUDAPEST, 2019

Összefoglaló

Ahogyan egyre több internethez csatlakozó eszközt használunk mindennapjaink során, úgy terjed egyre szélesebben ipari körökben is az *IoT*, azaz az *Internet of Things*. A kritikus infrastruktúrák sem kivételek ezen trend alól, ami viszont súlyos következményekkel jár; hatalmas kiber fenyegetettségnek téve ki ezáltal. Kutatásom során a mindennapi életben egyik legfontosabb szerepet betöltő ilyen infrastruktúrát, a *villamosenergia-rendszert* (*VER*) vizsgálom meg kiberbiztonsági szempontok szerint, és bemutatok egy újszerű, támadás-szimulációkra is alkalmazható keretrendszer kialakítást.

Korunk egyik legalapvetőbb szolgáltatása a villamosenergia-ellátás, mely számos rendelkezésre állási és minőségi követelményt támaszt, hiszen a háztartási fogyasztók és az ipar számára is szükséges a folyamatos áramellátás. Az elmúlt évek tapasztalata azt mutatja, hogy egyre több kockázatot jelentenek a villamosenergia-rendszerek internethez csatlakoztatott egységei. Ennek oka, hogy a hagyományos, fizikai védelmi funkciókat ellátó berendezések kommunikációja során a leggyakoribb csatorna az internet, amely veszélyeit jól ismerjük. A kibertámadások a VER-ben valós, fizikai károkat is okozhatnak, ezért a rendszer ilyen behatolások elleni védekezési képességét kiberfizikai biztonságnak nevezzük.

A modern villamosenergia-rendszer működését és hatékonyságát különböző informatikai megoldások segítik. Az elmúlt években igencsak divatos kifejezéssé vált a smart grid, azaz az ,,okos hálózat". Az okosítás jelen esetben hálózatautomatizálási megoldásokat és számítógépes támogatást jelent, melynek központját az *EMS*/*SCADA* (*Energy Management System*/*Supervisory Control and Data Acquisition*) rendszerek jelentik. Ezek olyan elosztott alkalmazások, melyek menedzselik a rendszert jellemző adatokat; feladatuk tehát elsősorban az adatgyűjtés, adattárolás és a különböző hálózatszámítások. Ebből következik, hogy ezen szoftverek szolgáltatják és kezelik az összes olyan információt, melyek alapján a rendszerirányítás történik. A korszerű, okosított hálózat jellemzésére számos modell készült, azonban az irodalomban a SCADA rendszerek integrálása nélkül kerülnek ezek vizsgálatra. Dolgozatomban bemutatom a két struktúra közötti kapcsolatot, és javaslatot teszek azok együttes modellezésére.

A megfelelő vizsgálódási környezet kiválasztása után ismertetem a kiberbiztonság alapjait, és összefoglalom a legfontosabb támadási lehetőségeket, illetve a jelenleg alkalmazott védekezési módszereket. A villamosenergia-rendszer komplexitása nem teszi lehetővé, hogy nyugodt körülmények között elemezhessük a különböző támadások hatásait és a védelmi mechanizmusok működését. Kutatásom célja, hogy moduláris megközelítéssel kísérletet tegyek egy szimulációkra és elemzésekre alkalmas keretrendszer tervezésére. A környezet lehetőséget fog biztosítani a tématerület legégetőbb kérdésének, az anomália- és behatolás-detektáló rendszerek működésének vizsgálatára.

Abstract

As internet-access devices are used in our everyday life more and more, the *IoT* – *Internet of Things* – spreads in almost every level of industry. The modern cyber-physical systems, like smart power grids, have to face several cyber-threats and issues. In this paper a short review is given about the grid control automation, network structure perspectives, cyber-attacks and defense mechanisms.

The literature approaches the smart grid mainly in two different ways. One of them considers the SG a centralized cloud-based structure, while the other one in a modular way. The last one seems to be the best and most realistic model as it makes possible to integrate grid control automation systems. The *EMS*/*SCADA* (*Energy Management System*/*Supervisory Control and Data Acquisition*) distributed architectures are likely to be examined from cybersecurity perspectives apart from the whole grid, which may lead to several problems and non-existent challenges. In this paper a complex view of these two integrated structures is demonstrated.

Due to various forms of cyber-attacks exist, a proper modeling method is necessary. Here comes the attacking-tree handy; it allows to structurally model the cyber-attacks, hence experts can get to know them deeply in modular way. Unfortunately studying all these attacking possibilities would require way too much resource and time, so an alternative defensive perspective has to be considered. A new trend getting widespread in the literature; the defence shall be based on prevention and not elimination. In this paper i propose a new perspective of the smart power grid's structure, and a modular system for modeling cyber attacks, anomaly- and intrusion detection.

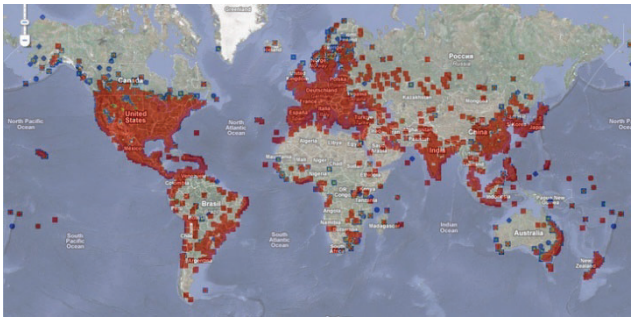
Tartalomjegyzék

Bevezető

Aktív villamosmérnöki tanulmányaim során nagyon közel került hozzám a rendszerszintű gondolkozásmód, a villamosenergetikával való megismerkedésem után pedig egyértelművé vált számomra, hogy a villamosenergia-rendszerrel szeretnék tudományos munkásságom alatt foglalkozni. A képzés informatikaibb jellegű tárgyai is nagy mértékben felkeltették az érdeklődésemet, igy némi internetes kutakodás, illetve látóképszélesítés után megtaláltam a két terület egyik legizgalmasabb egyvelegét, a kiberfizikai biztonságot.

Statisztikai adatok szerint jelenleg mintegy 7 billió internethez csatlakozó – IoT – eszköz van aktív használatban a világon, és ez a szám 2025-re az előrejelzések szerint körülbelül 21,5 billióra nőhet [1]. Ezen óriási mennyiségű berendezés jelentős része az ipari szegmensben kerül alkalmazásra, elősegítve ezzel a gyárak modernizálását és az ipar 4.0 kialakulását. A villamosenergia-rendszerek is egyre több IoT eszközt használnak világszerte, elmozdítva ezáltal a smart grid irányába a hálózatot. A kiberbiztonság jelentőségére legrémísztőbben a 2008-as *Conflicker* féreg hívta fel a figyelmet, amely képes volt fél év alatt a világ számítógép-hálózata nagy részének megfertőzésére. Ez a kártevő képes lett volna az internet ,,felét" megbénítani, azonban szerencsére semmilyen komoly célra nem használták fel, sőt, a Conflicker végül saját magát pusztította el [2]. A villamos hálózat ellen is követtek el hasonló támadásokat, melyek közül az első jelentős és jelzésértékű a 2010-es *Stuxnet* féreg volt, amely korszakalkotó módon egy nukleáris üzemanyagdúsító gyár irányítórendszerébe férkőzött be, és okozott ott maradandó károkat. A média általi legtöbb figyelmet azonban mégis a 2015-ös ukrán eset kapta, melynek során a *Black Energy 3* nevezetű kártevő bénította meg a hálózatot, több órás áramkimaradást okozva ezzel közel 225.000 fogyasztónak.

Kutatásom során a villamosenergia-rendszer moduláris megközelítése segítségével javaslatot teszek egy kiberbiztonsági vizsgálatokra alkalmas tesztelői keretrendszer tervezésére. Ehhez először az **1. fejezetben** részletesen bemutatom a villamos hálózat felépítését, majd a smart gridet veszem górcső alá a **2. fejezetben**. Ezt követően a **3. fejezetben** ismertetem a kutatás kiberbiztonsági alapjait, majd bemutatom a **4. fejezetben** a keretrendszer prototípusát. Dolgozatom végén röviden értékelem az eddigi eredményeket és tanulságokat, illetve összefoglalom a platform hordozta lehetőségeket.



1. ábra: A Conflicker világméretű fertőzése [2]

1 Korszerű villamosenergia-rendszerek

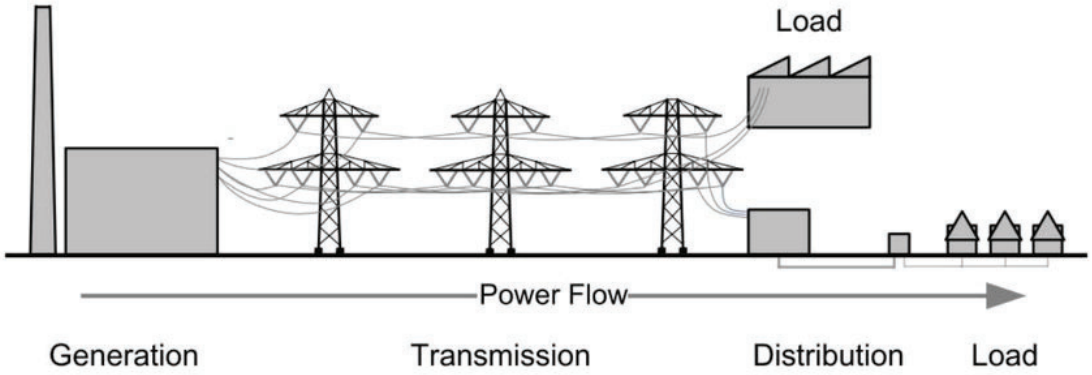
1.1 A villamosenergia-ellátás szerepe

Mindennapi életünk egyik legmeghatározóbb alapellátása a villamos energia, hiszen *„Ha áram van, minden van.”* – szól a híres mondás. Ez az egyszerű mondat azonban röviden és tömören foglalja össze mindazt, amit a villamosenergia-ellátás tekintetében feltétlenül szem előtt kell tartanunk: ezen szolgáltatás jelenléte az élet minden területén alapvető fontosságú. Különleges követelmény továbbá, hogy áramnak a nap 24 órájában folyamatosan rendelkezésre kell állnia, hiszen szinte minden infrastruktúra szerves részét képzik az elektromos, általában hálózatról működtetett eszközök és berendezések. Ezen kívül természetesen más fontos követelményeket is támasztunk a villamos energiával szemben, melyek közül számunkra kiemelt jelentőséggel bír a biztonság. Ennek tükrében elvárjuk, hogy az áram előállítása, szállítása és felhasználása is biztonságos körülmények között, biztonságosan módon történjen.

A villamosenergia-rendszer megbízhatóságát jól jellemző mérőszám a *SAIDI* (*System Average Interruption Duration Index*). Ez egy olyan indikátor, amely megmutatja éves tekintetben az egy fogyasztóra eső átlagos áramkimaradást. Az ellátás megszakadását számos tényező okozhatja, melyek közül statisztikai adatok szerint a természeti jelenségek a leggyakoribbak. Ezen felül a villamosenergia-rendszer műszaki meghibásodása is vezethet kimaradáshoz, de olykor szándékos ellátásmegszakítás is előfordulhat. A szolgáltatás megszakadásának következményei közül legnagyobb jelentőséggel a gazdasági kihatás bír, hiszen óriási fizikai károkat is okozhat egy-egy nagyobb kimaradás, melyeket bizony ki kell javítani. Szélsőséges esetekben akár olyan kritikus helyzet is előállhat, hogy a társadalmi jólét veszélyeztetése miatt politikai problémák is bekövetkezhetnek. Mint látható, a villamosenergia-ellátás folytonossága óriási jelentőséggel bír, pontosan ezért fokozott figyelmet igényel a szolgáltatás biztonsága. Az ismertetett következmények sajnos kecsegtető célpontként tüntetik fel a villamosenergia-rendszert, hiszen szándékos rosszakarással hatalmas károkat is lehet okozni, akár politikai, akár gazdasági célból.

1.2 Az erőműtől a fogyasztóig

A villamosenergia-rendszer hatalmas területeteken átívelő hálózat, melynek feladata, hogy a megtermelt villamos energiát eljuttassa a fogyasztókhoz. Szerkezetét tekintve három alapvető részre bontható a részegységek funkcionalitása alapján. A lentebbi ábrán jól elkülönítve látható a villamosenergia-rendszer három szegmense; a termelés, átvitel és elosztás, illetve fogyasztás.



2. ábra: A villamosenergia-rendszer szegmensei [3]

1.2.1 Villamosenergia-termelés

A villamos energia előállítása alapvetően a természeti erőforrásokból nyert mechanikai energia hasznosításával történik, melyből áramot termelhetünk. Annak függvényében, hogy az elektromos generátor milyen energiát alakít át, megkülönböztethetünk számos típusú termelőegységet. A villamosenergia-rendszer egyik fő szegmense tehát a termelés, amely történhet például hagyományos módon hőerőművekben, ahol valamilyen tüzelőanyag elégetése során nyert energiával fejlesztik a turbinát meghajtó gőzt – így működik például a széntüzelésű erőmű is. Napjainkban egyre elterjedtebbé válnak a nem fosszilis üzemanyaggal működő erőművek is, melyek közül az atomerőművek a legismertebbek. A klímaproblémákra és környezetszennyezésre igyekeznek megoldást nyújtani a nem elsődleges energiahordozókat hasznosító erőművek, mint például a naperőmű, szélerőmű, geotermikus erőmű vagy vízerőmű. A villamosenergia-termelésben bekövetkezett modernizáció hatására már nem centralizált termelés a jellemző, hanem a hálózat többi részén is egyre gyakrabban jelennek meg energiatermelő egységek, melyek lehetnek például háztartási méretű kiserőművek. Az megújuló (szekunder) energiaforrások villamosenergia-rendszerbe történő integrálása komplex kihívást okoz a kor szakembereinek, ugyanis a decentralizáltság és a kiegyensúlyozatlan viselkedés feszültségstabilitási problémákhoz vezethet a hálózaton, ami viszont rendszerszabályozási igényt vet fel. Ezt a problémát mélyítik még inkább el a hálózatra csatlakoztatott energiatároló egységek is, jellemzően az akkumulátorok.

1.2.2 Az átviteli- és elosztóhálózat

A megtermelt áramot valamilyen módon természetesen el is kell juttatni a felhasználás helyszínére. Ezt biztosítja a VER szállítási részegysége, mely magába foglalja mind a villamos energia átvitelét, mind az elosztását. E két folyamat lényegében nem tér el egymástól, azonban mégis több szempontból is fontos megkülönböztetni őket. Az átvitel a megtermelt villamos energia veszteségminimalizálás céljából nagyfeszültségű távvezetéken történő elszállítását jelenti azon csomópontokra, melyek a célfelhasználási terület meghatározott közelségében vannak. Ezen csomópontokon alállomásokon történik a nagyfeszültségű áram középfeszültségűvé való átalakítása transzformátorok segítségével. Az alállomásokról, mint

elosztóhálózati csomópontokról tovább kell szállítani a villamos energiát, azonban mivel a célpont itt már maga a fogyasztó, ezért ezt a folyamatot elosztásnak nevezzük átvitel helyett. Az alállomások jelentik az átviteli és elosztóhálózat közötti kapcsolatot, amely szükségessé teszi számos a teljes infrastruktúrához is csatlakozó telemechanikai és kommunikációs berendezés használatát. Ezen berendezések kiemelt szerepet játszanak a hálózati rendszerirányításban, melyről bővebben az *1.3. alfejezetben* lesz szó.

1.2.3 Fogyasztói típusok

Mindennapi életünkhöz legközelebb a fogyasztói szegmens áll, amely magába foglalja a megtermelt és célhelyre eljuttatott villamos energia minden típusú felhasználását. A háztartási fogyasztás a legáltalánosabb felhasználási cél, azonban mára ez a szerepkör is megváltozott. Egyre jellemzőbb, hogy a fogyasztók háztartási méretű kiserőművet telepítenek, melyek hálózati szempontból káros hatása a rendszerbe történő visszatáplálás. Fontos réteg ezen felül még az ipari és üzemi fogyasztók köre, melyek esetében fokozott jelentőséggel bír a villamosenergia-ellátás folytonossága és biztonsága. A felhasználási szegmens legnagyobb problémája, hogy a háztartási fogyasztók viselkedése változó, motiválásuk pedig a mai napig megoldandó probléma. Mivel ezen réteg energiafelvétele nem (vagy csak nagyon komplex módon) szabályozható, szintén feszültségstabilitási gondok keletkezhetnek a hálózaton. A jelenlegi trendek szerint okosmérők alkalmazásával igyekeznek kiküszöbölni ezt problémát, melyek hatékonysága és biztonsága igencsak megkérdőjelezhető.

1.3 Hálózati rendszerirányítás

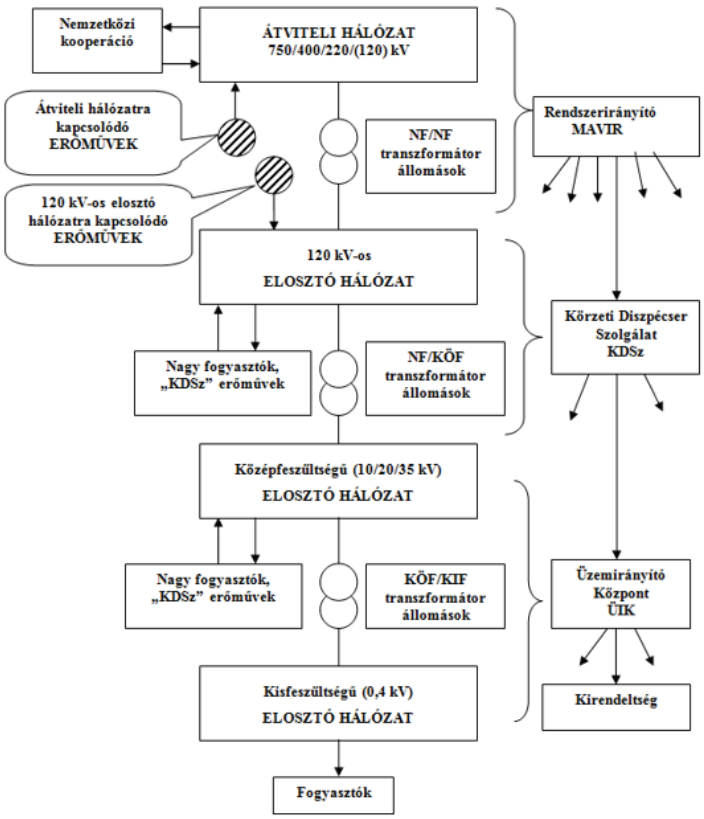
1.3.1 A rendszerirányítás fogalma

A villamosenergia-rendszer komplexitása megkövetel valamilyen felsőbbrendű beavatkozó szervet, amely a rendszer irányítását látja el. Az erre irányuló szükséglet az együttműködő rendszerek kialakulásával jelent meg, hiszen ezzel inhomogénné vált a hálózat. A rendszerirányítás alapfeladata, hogy biztosítsa a folyamatos és biztonságos villamosenergia-ellátást, a VER biztonságos és hatékony működését, mindezt átlátható formában, a jogi és műszaki előírások betartásával. *TSO*-n (*Transmission System Operator*) egy szabályozási zóna irányítását végző átviteli hálózati rendszerirányítót értünk, amely hazánkban a Magyar Villamosenergia-ipari Átviteli Rendszerirányító Zrt., azaz röviden a MAVIR. Ezzel közel analóg módon a középfeszültségű elosztóhálózati engedélyeseket *DSO*-nak (*Distribution System Operator*) nevezzük. A két szerv egymáshoz és hálózathoz való viszonya jól látható az alábbi blokk-diagramon. Míg a rendszerirányító a *NaF* (*nagyfeszültségű*) átviteli hálózat irányításáért felel, addig a DSO a *KöF* (*középfeszültségű*) elosztóhálózat üzemirányítását látja el. [4]

A rendszerirányító feladatai nagyon sokszínűek, melyek a teljesség igénye nélkül alább kerülnek bemutatásra. A TSO felelős a nagyfeszültségű hurkolt átviteli hálózat üzemeltetéséért; feladatai közé tartozik annak tervezése, fejlesztése, karbantartása, kapcsolási állapotainak meghatározása, *real-time* (*valós idejű*)

monitorozása és távvezérlése, a rendszer határértékeinek – pl. terhelődési és csomóponti feszültség-határértékek – betartásának ellenőrzése. A rendszerirányító feladata az átviteli hálózatba betápláló erőművek irányítása, amely magába foglalja a menetrend-átadást, üzemállapot követést, *AGC*-t (*Automatic Generation Control*), illetve a tartalékok lekötését és igénybevételét. Folyamatosan kapcsolatot kell tartania a környező szabályozási zónák TSO-ival leginkább a határkeresztező vezetékek üzemállapotának real-time mérése, adatcsere, segítségnyújtás és -igénybevétel, illetve a nemzetközi szervezetekben való képviselet biztosítása miatt. Kapcsolatot tart a rendszerirányító továbbá az elosztói engedélyesekkel is, amelyre tervezett és terven kívüli kapcsolások jóváhagyása, elosztóhálózati monitorozás, DSO-i hatáskörbe tartozó erőművek termelési menetrendjének fogadása, fogyasztói korlátozási tervek és egyéb adatok kezelése miatt van szükség. Feladatai közé tartozik még a villamosenergia-piac működtetése, az olyan rendszerszintű szolgáltatások biztosítása, mint például a szabályozási és üzemzavari tartalékok beszerzése, illetve a határkeresztező teljesítményáramlások kiegyenlítése is. Természetesen az operatív üzemirányítás szintén a TSO feladata, hiszen valós idejű rendszerirányítást lát el mind normál, mind üzemzavaros állapotban. A villamosenergia-rendszer kiberfizikai biztonságának szempontjából kiemelt jelentőséggel bír a rendszerirányítás számítógépes támogatásának üzemeltetése, amely szintén TSO-i alapfeladat. [4]

3. ábra: A hazai villamosenergia-rendszer irányítási struktúrája [4]



1.3.2 Számítógépes támogatás

A rendszerirányítás során a hatékony működtetéshez rengeteg adatra van szükség a villamosenergia-rendszerről. Ezen óriási mennyiségű információ folyamatos fogadása, feldolgozása, továbbítása és tárolása szükséges, amely nagy erőforrást igénylő feladatnak bizonyul. Ebből kifolyólag alapvető fontosságú a megbízható és kielégítő számítógépes támogatás, amely mind az operatív üzemirányítást, mind az üzemelőkészítést és -értékelést hivatott segíteni. A rendszerről rendelkezésre álló adatokat online és offline is kezelni kell, erre nyújt megoldást a rendszerirányítás számítógépes infrastruktúrája. Bonyolultságuk és funkcionalitásuk szerint megkülönböztetünk SCADA és EMS rendszereket, melyek mindegyike az üzemirányítás szerves részét képzi. [5]

1.3.2.1 SCADA rendszerek

A SCADA egy olyan elosztott irányítórendszer, melynek legfőbb feladata - a nevéből adódóan is - a felügyeleti szabályozás és adatgyűjtés. Ez az online valós idejű rendszer képzi a számítógépes üzemirányítás alapját. Fontos megjegyezni, hogy a SCADA egy olyan struktúra, melyből többféle változat is létezik, és számos kritikus infrastruktúrában kerül alkalmazásra, például vízvezeték-hálózatoknál vagy a villamosenergia-rendszereknél. Segítségével nagy mennyiségű adatot lehet közel valós időben - másodperces bontással - olvasni, továbbítani, tárolni és feldolgozni. A SCADA rendszerekben futó algoritmusok jellemzően nem bonyolultak, a programok néhány miliszekundomos futási idejűek, és ciklikusan hajtódnak végre. Ezen funkciók főleg real-time futnak online, a rendszer pedig *VPN* (*Virtual Private Network*) hálózaton keresztül kapja az adatokat a telemechanikai alközpontoktól, azaz *RTU*-któl (*Remote Telemechanical Unit*). A SCADA-funkciók a teljesség igénye nélkül: távmérések és távjelzések fogadása, topológia-analízis, információ-dekódolás, hitelességvizsgálat, adatbázisba szervezés, információk megjelenítése, naplózás, határérték- és gradiensfigyelés, illetve távparancsadás az EMS által számított beállítási értékek segítségével. [5]

1.3.2.2 EMS rendszerek

A rendszerirányítás során alkalmazott adatkezelést és számításokat, illetve az ezek alapján történő energiaelosztást az EMS rendszer végzi. Főbb feladatai közé a tartozik az AGC, a topológiai feldolgozás, az állapotbecslés és üzembiztonsági analízis, a load-flow számítás, *DTS* (*Dispatcher Training Simulator*) és a real-time hálózatszámítás, mint például feszültség-meddő szabályozás vagy zárlatszámítás. Egységes szoftvercsomag nem alakult ki az EMS feladatok ellátására sem, hiszen az eltérő rendszerek más és más igényekkel rendelkeznek, viszont a főbb funkciók ettől függetlenül legtöbbször megegyeznek. Fontos látnunk, hogy a SCADA rendszerek kezelik és tartják nyilván az összes VER adatot, ezért a védelmük kiemelt hangsúlyt igényel, a legtöbb országban ugyanis kritikus infrastruktúraként tartják számon. [5]

1.3.3 A SCADA rendszerek felépítése

A komplex felépítésű infrastruktúrák nagy része irányításra szorul, és ahogyan azt korábban tárgyaltuk, ezek irányítását és ellenőrzésént főként a SCADA rendszerek végzik. Fontos megemlíteni, hogy a SCADA azonban nem egy konkrét irányítószerv, csupán egy rendszerstruktúra, melyből számos típus létezik attól függően, hogy milyen szerepet lát el. Különböző SCADA rendszerek végzik például a vízvezeték- és a villamosenergia-rendszerek irányítását, azonban felépítésüket tekintve sok közös tulajdonság is megállapítható. Általánosságban elmondható, hogy struktúrájukat tekintve 5 alrendszerre bonhatók, melyeket az ellátott funkciók alapján különböztetünk meg egymástól. Ez az 5 egység együttesen felel a SCADA működésért, ezért azt jellemzően elosztott irányítórendszernek is szokás nevezni. [5]

1.3.3.1 Fizikai alrendszer

A mindennapi életünkhöz legközelebb a fizikai alrendszer áll, amely magába foglalja a villamosenergia-rendszerben végbemenő folyamatok összességét, és az azokat megvalósító berendezéseket. A VER korábban ismertetett felépítését szem előtt tartva megállapíthatjuk, hogy mindhárom szegmens bőven rendelkezik ilyen elemekkel. A hálózaton végbemenő folyamatok közül a villamosenergia-termelés, szállítás, elosztás és felhasználás tartozik, azonban ezeknél kisebb volumenű események is ide sorolhatók, például a távvezeték melegedése vagy éppen egy megszakító működésbe lépése egy alállomáson. A folyamatok sokaságát és sokszínűségét tekintve azt a megállapítást tehetjük, hogy mind darab-, mind típusszámra óriási mennyiségben vannak jelen villamos berendezések és eszközök a hálózat minden területén. Ezek jellemzően olyan szenzorikák, automatikák és működtető eszközök, melyek végrehajtják a különböző fentebb bemutatott fizikai mechanizmusokat. A legtöbb ilyen berendezéssel az alállomásokon találkozhatunk, ezek azonban a működtetés mellett folyamatosan adatokat gyűjtenek; mérik például az áramerősséget, a feszültséget vagy a hőmérsékletet. Mivel ez a funkció leginkább a real-time monitoringhoz és irányításhoz szükséges, a mért értékeket olyan elektromos jelekké alakítják át, melyeket a rendszer más részeire továbbítani képesek úgy, hogy azok ott felhasználhatóak legyenek. [5]

1.3.3.2 Kiberfizikai alrendszer

A fizikai szintet a SCADA többi alrendszerével a kiberfizikai kapcsolatréteg köti össze. A különböző szenzorikákból és működtető berendezésekből származó adatokat valamilyen meghatározott szállítási platformon el kell juttatni azokra a helyekre, ahol az irányítás történik, hiszen ott ezek az adatok feldolgozásra kerülnek a számítások elvégzéséhez. A kiberfizikai jelző már önmagában is eléggé beszédes, árnyalja, hogy ezen réteg kulcsa a valódi kézzel fogható fizikai rendszer összekapcsolása a rendszerirányítás informatikai részével. Ezt a kapcsolatot a gyakorlatban többnyire egyszerű feszültség vagy áramerősség jeleket szállító villamos vezetékek segítségével valósítjuk meg, de egyre több helyen alkalmaznak modernebb megoldásokat is, például optikai szálas kábelt. [5]

1.3.3.3 Elosztott irányító-alrendszer

A kétirányú kommunikációra is képes elosztott irányító-alrendszer jelenti a SCADA rendszer gerincét. Struktúrálisan úgy képzelhetjük ezt el, hogy a rendszerirányítási folyamatot hierarchikusan szintekre bontjuk. A legalsó szinten néhány alállomást tartalmazó területet fog össze egy-egy alrendszer, majd a hierarchiában felfelé haladva egyre több és komplexebb irányító alegységet fogunk össze. Ezen logika mentén haladva a struktúra tetején egyetlen egy helyre kerül koncentrálva az egész irányítandó hálózat. Ennek tükrében állathatjuk, hogy a SCADA rendszer ezen szegmensébe ezek az alrendszerek tartoznak. Olyan terepi eszközöket sorolhatunk ebbe az alrendszerbe, melyek leggyakrabban beágyazott irányítási lehetőségekkel rendelkeznek, ezáltal képesek logikai műveletek elvégzésére. A működtető berendezésekből kapott jeleket feldolgozzák, majd előre meghatározott, esetleg dinamikusan változó programvezérelt logika szerint küldenek vissza valamilyen válaszjelet. A villamosenergia-rendszer esetében ebbe a szegmensbe tartoznak jellemzően a *PLC*-k (*Programmable Logic Controller*), az *RTU*-k és *MTU*-k (*Remote/Master Telemechanical Unit*), illetve az egyéb *IED*-k (*Intellgient Electric Devices*). [5]

1.3.3.4 Kommunikációs hálózat

A SCADA különböző alrendszerei közötti kapcsolatot komplex hálózati struktúra biztosítja. Az alacsonyabb szinten elhelyezkedő, egy-egy alállomásért, esetleg egy-egy nagyobb területért felelős elosztott irányítórendszerek felett természetesen áll egy a már fentebb bemutatott hierarchia alapján az egész hálózatot átfogó és mindent vezérelni képes ellenőrző rendszer. Ezt a felső szintű irányítást köti össze a kisebb irányítóegységekkel valamilyen igencsak komplex hálózati struktúra. A kommunikáció előre meghatározott protokollok alapján történik, melyek azonban a rendszer különböző szintjein akár eltérőek is lehetnek. A leggyakrabban alkalmazott szabványok a *TCP/IP*, *Ethernet/IP*, *ModBus* és a *DNP3*. Eltérő hálózati szintek eltérő protokolljai egymással csak protocol-gatewayen keresztül tudnak kommunikálni, amely emiatt védelmi szempontokból igencsak kritikus pontnak számít. A hálózati forgalomirányítás optimalizálásának érdekében szinte kivétel nélkül kerülnek alkalmazásra bridgek, switchek, routerek mint kiegészítő megoldások. Ezen eszközök feladata továbbá, hogy a fizikailag vagy logikailag egymástól elkülönített szegmensek között kapcsolatot teremtsenek, legtöbbször például *LAN* (*Local Area Network*) vagy *WAN* (*Wide Area Network*) által. [5]

1.3.3.5 Végrendszerek

Felhasználási szempontból természetesen az ember-gép kapcsolat megfelelői kialakítása a legfontosabb, amely biztosítja a lehetőséget a teljes rendszer folyamatos monitorozására és távvezérlésére. A külföldi irodalomban historianként ismert archívum és adatgyűtjő rendszer a felhasználói interakciók kezelésének egyik legfontosabb alapját képzik. Az al- és végrendszereken úgynevezett ember-gép interfészeken (*HMI - Human-Machine Interface*) keresztül kerül kapcsolatba a felhasználó a rendszerrel, melyek munkaállomásként kerülnek megvalósításra. Vezérlési szempontból külön egységként kezelhetjük az

irányítótermeket és -szobákat, ahol diszpécserek vagy ügyeletes rendszerirányítók végzik a munkát. Ezen HMI-k gyakran felhasználóbarát grafikus felülettel is rendelkeznek, melynek segítségével a legkomplexebb feladatok és vezérlések is viszonylag egyszerűen végezhetők el. A végrendszereken sokféle távvezérlési parancs adható ki, például megszakítók vagy szakaszolók irányítása, de számos alrendszerekről gyűjtött információt is megjeleníthetünk, melyek közül kiemelt fontossággal bírnak a visszajelzések, jelentések és az alarmok. [5]

Az ismertetett alrendszerekre bontott SCADA struktúrán kívül természetesen más megközelítés is létezik, azonban a rendszer főbb elemei adottak, így jelentős különbség nem áll fennt. Kiberfizikai biztonsági szempontból érdemes az irányítórendszereket a valódi rendszertől nem elkülönítve vizsgálni, hiszen egymáshoz nagyon közel állnak, illetve funkcionalitásukat tekintve sem javasolt szétválasztásuk a teljes hálózattól.

2 Okos hálózatok

2.1 A smart grid koncepció

A modernizált villamosenergia-rendszer egyre több és több digitális berendezést alkalmaz, elsősorban kommunikációra. A hatékonyabb működés reményében okosított hálózat a világ bizonyos részein már egészen jól kiépítésre került, túlnyomó részt azonban még csak közelítjük a smart grid koncepciót.

2.1.1 Hagyományos VS. okos hálózat

Napjaink egyre divatosabb kifejezésévé nőtte ki magát a smart gird, azaz az okos hálózat. Ez az egyszerűnek tűnő fogalom igencsak komplex jelentéssel bír, amely egyáltalán nem triviális. A hagyományos villamosenergia-rendszeren a jövő okos hálózata számos területen túlmutat, azonban ezen jellemzők vizsgálatához érdemes először sorra venni a tradícionális hálózat jellemzőit. Ahogy arról már korábban is szó volt, a villamosenergia-rendszer valós idejű szolgáltatást biztosít. Ennek gyakorlati következménye, hogy a fogyasztási igény jelentkezésekor azonnal rendelkezésre kell állnia a szükséges teljesítménynek, így annak előállítása és a felhasználási helyre való elszállítása az adott pillanatban biztosítva kell, hogy legyen. Ennek tükrében a hálózatba tápláló generátorokat a fogyasztói igényhez időben igazodva kell szabályozni, hogy a szükséges időszakban megfelelő mennyiségű villamos energiát szolgáltathassanak. [6]

A VER fontos különbsége az például infokommunikációs hálózatokhoz képest, hogy valós fizikai energia áramlik a rendszerben, nem pedig csak akár vezeték nélküli módon is szállítható analóg vagy digitális jel. Ezen hagyományos rendszer olyan problémáit hivatott megoldani a smart grid, mint például az ellátásbiztonság, elosztott energiatermelés vagy a megújuló energiaforrások integrációja. Az okos hálózat egy a tradícionális villamosenergia-rendszer továbbfejlesztett változata, melynek legfontosabb ismérvei, hogy jelentős kommunikációs infrastruktúra által igyekszik biztosítani a rendszer elemeinek hatékony együttműködését számos IT eszköz alkalmazása mellett.

2.1.2 Tulajdonságok és ismérvek

A hagyományos villamosenergia-rendszer olyan centralizált hálózat, melyet elektromechanikus komponensek alkotnak, és melyben az infrastruktúra monitorozása, illetve a hibák helyreállítása manuálisan történik. Ezzel szemben a smart gridben, azaz az okos hálózatban jelentősebb mértékű elosztott termelés és kommunikációs infrastruktúra jelenik meg. A koncepció alapja, hogy az intelligens energiatermelés, -elosztás, -felhasználás és tárolás, illetve a decentralizált adatfolyam segítségével megvalósítható bármely feszültségszintű hálózat optimális automatizálása a megújulók integrálásával együttesen. A smart grid valójában tehát nem más, mint real-time adatmonitorozás, és kétirányú digitális kommunikáció által megvalósított dinamikus microgrid-menedzsment különböző technológiai megoldások alkalmazása mellett.

Ebben rendszerben kapcsolatban állnak egymással a különböző irányítási egységekkel, és együttműködnek az olyan villamos szolgáltatások, mint például a megújuló-energiatermelés és -integráció, felhasználói fogyasztás, közlekedés vagy villamosenergia-piac. A hálózati egységek együttműködését robosztus információs irányítórendszer biztosítja, amely folyamatosan adatokat gyűjt és kezel. A smart grid komponensei egymástól nem elszigetelten működnek, hanem összehangolt, együttműködő egységekként. Egy ilyen fejlett hálózati infrastruktúra számos előnnyel bírhat a hagyományos rendszerrel szemben, amennyiben az infrastruktúra rendelkezésre áll és megfelelően működik; megbízható, rugalmas és biztonságos energiaelosztás és -szolgáltatás, folyamatos fogyasztás monitorozás, *DSM* (*Demand-Side Management*), optimalizált hálózati forgalom, rövidebb hibaidők és kiesések, csökkentett hálózati veszteségek és általánosan jobb, hatékonyabb rendszerszintű működés, illetve szolgáltatások. A smart gridet támogató technológiák között főként digitális eszközök és különböző szenzorok szerepelnek, melyek méréseket végeznek, adatot gyűjtenek, tárolnak, küldenek és továbbítanak. Összességében tehát egy ilyen összehangolt villamosenergia-hálózati struktúra lehetőséget biztosít a megbízhatóbb és jobb minőségű áramszolgáltatásra, az elosztott és megújuló energiaforrások alkalmazására, az előretervezhetőségre, automatizált működtetésre és karbantartásra, illetve szélesebb felhasználói lehetőségek biztosítására. Az alábbi ábra összefoglalja a korábban bemutatott tradícionális villamosenergia-rendszer és a smart grid közti főbb különbségeket, újításokat. [6]

Jelenlegi hálózat	Okos (smart) hálózat
Analóg- elektromechanikus	Digitális
Egyirányú kommunikáció	Kétirányú kommunikáció
Centralizált termelés	Elosztott termelés
Sugaras elosztóhálózat	Adaptív elosztóhálózati topológia
Nincs (kevés) mérés, érzékelő	Sok szenzor, sok mérés
On-line visszajelzések nélkül működik	Működését saját maga monitorozza
Hiba esetén „kézi" helyreállítás	Automatikus helyreállítás
Hiba esetén => kiesés	Adaptív, az ép rész szigetüzemben működik tovább
Készülékek időközi „kézi" diagnosztizálása szükséges	Folyamatos táv monitorozás, öndiagnosztika
Diszpécseri üzemirányítás	Automatikus, szakértői, döntéstámogató rendszerek
Load-flow by Kirchoff law	Aktív teljesítményáramlás szabályozás
Ár információk nem átláthatók a piaci minden szereplője számára	Teljes átláthatóság, szabad hozzáférés a hálózatokhoz, on-line piaci információkhoz
Fogyasztó passzív szereplő	Fogyasztó aktív (tudatos) közreműködő, DSM

4. ábra: A hagyományos és az okos hálózat tulajdonságai [6]

2.1.3 A smart grid definíciója

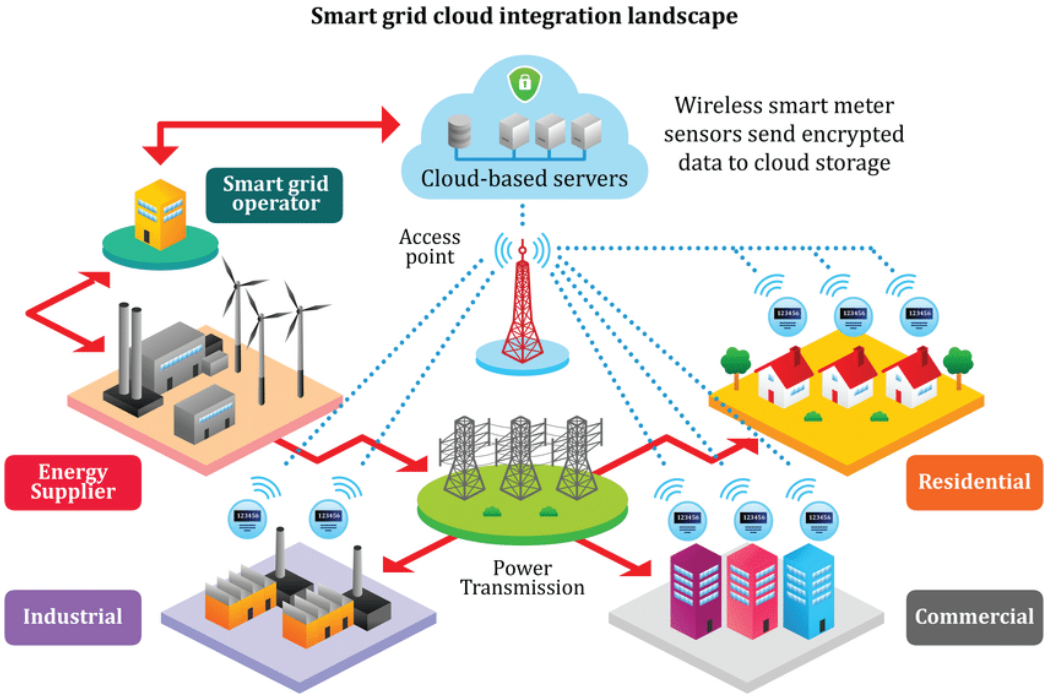
A smart gridnek, mint fogalomnak nincsen általánosan elfogadott pontos és hivatalos definíciója, azonban számos szervezet megkísérelte a maga módján meghatározni annak jelentését. Az *Európai Bizottság* a smart gridet úgy definiálta, mint *„továbbfejlesztett villamos hálózat, mely kétirányú digitális kommunikációval és intelligens mérő-monitorozó rendszerrel került kibővítésre”* [7]. A *The European Smart Grid Task Force* értelmezésében ez egy *„olyan villamos hálózat, amely hatékonyan építi be saját működésében a hozzá csatlakozó felhasználók és komponensek - pl. fogyasztók, termelők vagy akár olyanok, melyek mindegyikre képesek - viselkedését és tevékenységét azért, hogy költséghatékony, kis veszteséget produkáló, magas minőségű és biztonságú fenntartható energiaellátásra legyen képes”* [7]. Természetesen számos másik többé vagy éppen kevésbé eltérő meghatározás is létezik, viszont legtöbbjük egy jól jellemezhető struktúrát ír körül. A smart grid leegyszerűsítve és a lényeget kiragadva nem más, mint a villamos és információs infrastruktúra összekapcsolása. Ennek eredményeképp az okos hálózat képes a rendszer elemeinek állapotával folyamatosan összhangban lévő szabályozásra többirányú kommunikáció segítségével. A smart grid által biztosított szolgáltatás így nem más, mint kétirányú adat- és energiaáramlás a villamos hálózaton.

2.2 Az okos hálózat struktúrája

2.2.1 Modellek

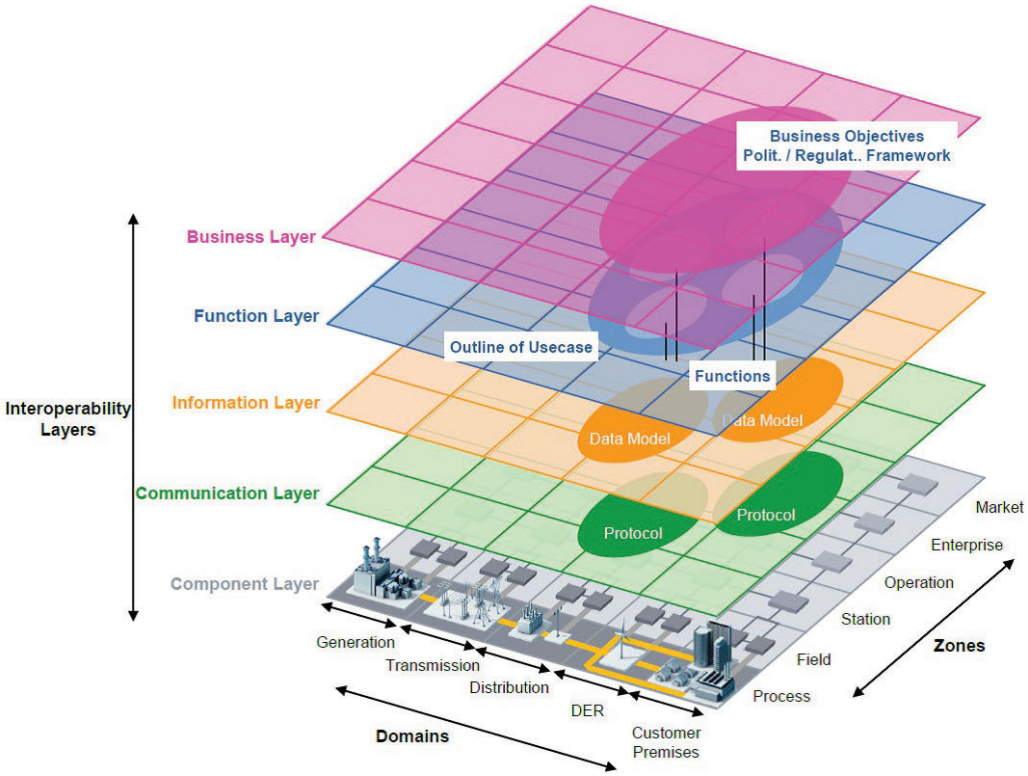
Az smart grid összetétele nagyon sokszínű, igazán változatos építőkövekből áll össze. Az okos hálózat modellezése érdekében ezen rendszerelemeket ismernünk kell, hogy az elképzelt modell a valósághoz a lehető legközelebb álljon. Az építőelemek nagy részét a szenzorrendszer képviseli; ide tartoznak például az áram- és feszültségváltók, a *PMU*-k (*Phasor Measurement Unit*), illetve a hőmérséklet, nyomás és okos mérők. A hálózat további szegmensei a gép-gép közötti kapcsolatokat biztosító kommunikációs infrastruktúra, a szabályozó algoritmusok és a fizikai rendszerhez tartozó beavatkozó elemek.

A smart grid felépítését modellezni sem egyszerű feladat, hiszen egy infrastruktúrákat átölelő komplex rendszert kifejező módon bemutatni nagy kihívás. Az irodalomban leggyakrabban a centralizált hálózathoz hasonló szerkezetet szemléltetik, azonban egyre szélesebb körökben terjed el a rétegzett struktúra is. Előbbi lényege, hogy a különböző szolgáltatások egy bizonyos hozzáférési ponton kapcsolódnak a felhő-alapú szerverekhez, melyek biztosítják a hálózati komponensek együttműködését. Ezt a struktúrát jót szemlélteti az alábbi ábra melyen látható, hogy a smart grid vezérlése külön szolgáltatási egységként jelenik meg az energiatermelés, -szállítás, -elosztás és a különböző célú felhasználások mellett. A felépítés gyenge pontja, hogy a rendszerben igencsak meghatározó nagy mértékű komplexitást és összefügést nem tükrözi hűen. A smart gridben minden mindennel összefügg, így képes az okos hálózat a komponensek optimalizált párhuzamos működtetésére.



5. ábra: Centralizált smart grid struktúra [8]

Sokkal beszédesebb az a moduláris megközelítés, mely szerint ez a fajta struktúra rétegekre bontható. A 6. ábrán látható a smart grid 5 szintje, melyeket az általuk ellátott feladatok és a hálózatban betöltött szerepük alapján különböztetünk meg: komponens, kommunikációs, információs, funkcionális és üzleti/ipari réteg. Ezen rétegekbe jól besorolhatók a fentebb ismertetett smart grid építőelemek, kiegészítésre csupán a legfelső, azaz az üzleti vagy ipari réteg szorul. Ez a hálózati szint a teljes rendszer irányítását, monitorozását és ellenőrzését reprezentálja a már korábban bemutatott SCADA végrendszerekhez hasonlóan. A két smart grid struktúrát összevetve levonhatjuk azt a következtetést, hogy a rétegzett moduláris felépítés sokkal közelebb áll a rendszer fizikai valójához, így a vizsgálataim további részében ezt a megközelítést fogom alkalmazni.



6. ábra: Rétegzett smart grid struktúra [9]

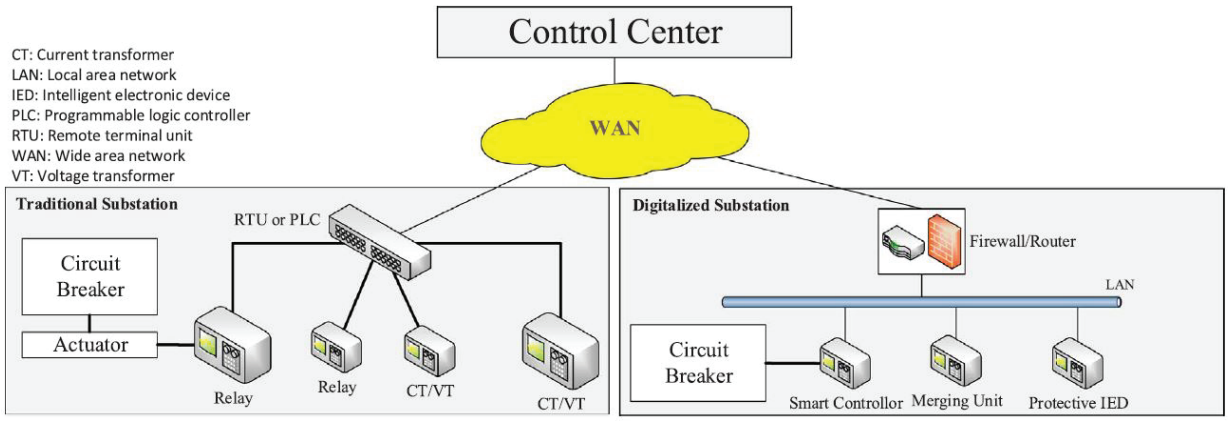
2.2.2 SCADA és SG integráció

Mint látható, a már korábban bemutatott EMS/SCADA rendszer funkciói teljes mértékben beleillenek a smart grid koncepcióba. A hatékonysághoz elengedhetetlen egy az egész hálózatot nyilvántartó irányítórendszer - SCADA -, melynek működését egy központi optimalizáló elosztó egység segíti, amely jelen esetben az EMS. Ezek szerint a két rendszert nem érdemes az *SG*-től (*smart grid*) külön vizsgálni, hiszen egy jól felépített hálózatban ezek egymással együttműködve, egymást kiegészítve léteznek. A fentebb ismertetett réteges smart grid felépítésbe jól beleillenek a SCADA/EMS szegmensek, ezért a két struktúrát érdemes összevetni, és lehetőség szerint egymásba integrálni.

Az SG komponens szintjébe tartozik a fizikai alrendszer egésze, illetve az összes hálózati működést biztosító berendezés. A kommunikációs réteg foglalja magába azokat a szabványokat, protokollokat, melyek alapján a hálózati kapcsolatok kiépítésre és működtetésre kerülnek. A rendszer jól láthatóan hatalmas mennyiségű adattal is dolgozik, melyet bizony valamilyen módon tárolni kell. Erre felhő-alapú adatbázisstruktúra a legalkalmasabb, amely megvalósítja az összes adatkezelést a teljes hálózati infrastruktúrában. Erre az információs vagy adatrétegre épülő funkcionális szintbe sorolhatók azok a számítások, műveletek és vezérlési logikák, vezérlések, melyek megvalósítják a rendszer irányíthatóságát. A felhasználói beavatkozást és távvezérlést biztosító ember-gép kapcsolatot biztosító végrendszer pedig egy az egyben megegyezik a SCADA végrendszerével, melyben HMI-ken és grafikus felületeken keresztül érhető el a teljes rendszer. A smart grid és SCADA integráció egy olyan komplex modellezési lehetőséget biztosít, amely több szempontból is kedvező kiberbiztonsági vizsgálatok során. Az így kialakított struktúra lehetővé teszi, hogy a rendszer egyetlen egészként kezelhessük, nem pedig külön részegységenként. Ellenkező esetben mind hiányosságok, mind nem létező problémák is előállhatnak, azonban az egyesített felépítés ezt a problémát kiküszöböli. Ezen felül megfelelő alapja lehet egy az egész hálózatot modellező szimulációs keretrendszernek, amilyet a kutatásom során magam is tervezek. [5]

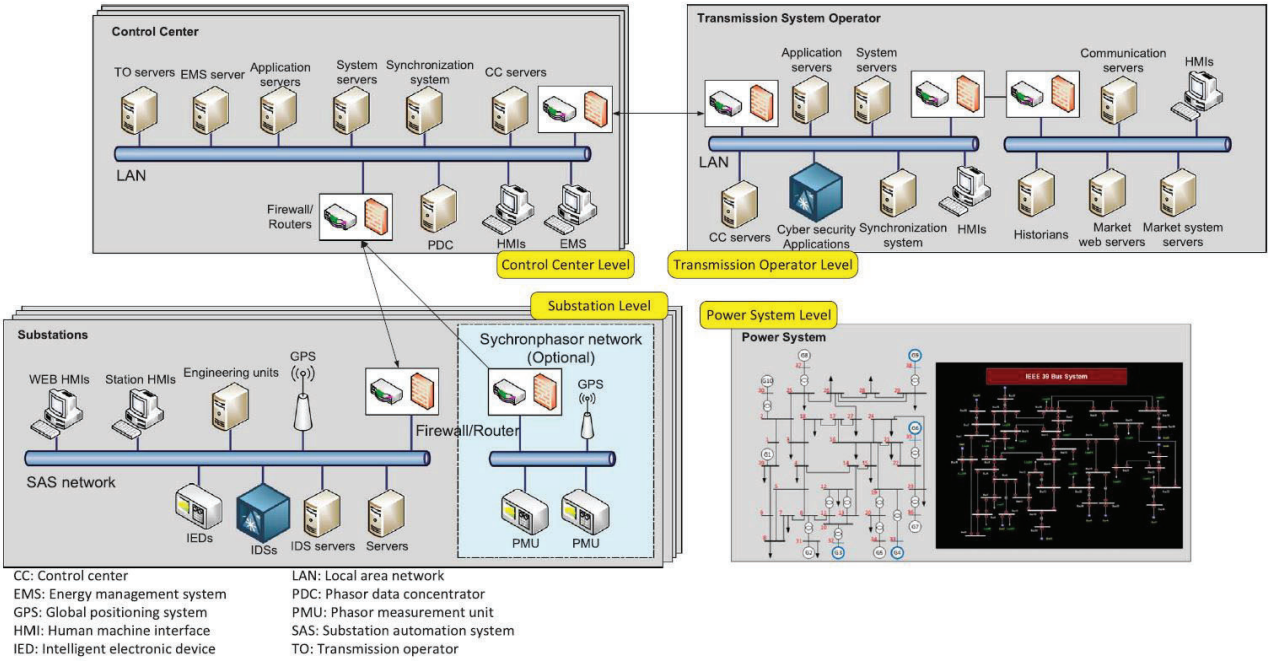
2.2.3 Hálózati kommunikáció

A hagyományos villamosenergia-rendszerre, főként annak alállomásaira leginkább az analóg kommunikáció volt jellemző, azonban az okos hálózat esetében előtérbe kerül annak digitális változata. Ez a protokollok által keretek közé zárt digitális kommunikáció lehetőséget biztosít több jel egyszerre történő továbbítására, így a rendszer információs hálózatán zajló adatcsere gyorsabbá és hatékonyabbá válhat. Ez a digitalizáltság természetesen nem csak az alállomásokon figyelhető meg, ugyanis LAN és WAN gatewayen keresztül a rendszer többi része felé is lehetőség nyílik a kommunikációra. Az alábbi ábra egy tradícionális és egy modernizált alállomás struktúráját mutatja be. [10]



7. ábra: Hagyományos és digitalitált alállomási struktúra [10]

Az online megvalósított adatcserét, monitorozást, ellenőrzést és irányítást – melyek során a rendszert leíró információk áramlanak – mind átviteli mind elosztóhálózati szinten *ICT* (*Information and Communication Technologies*) infrastruktúra segíti. Ennek legfőbb váza a korábban már tárgyalt SCADA, de fontos részét képzi a *SAS* (*Substation Automation System*) is. Ezt az alállomás automatizálási rendszer az *IEC 61850* szabvány specifikálja, célja pedig, hogy biztosítsa az *Ethernet* alapú kommunikációt, a különböző gyártmányú eszközök együttműködésének lehetőségét, illetve a kommunikációs topológia változása által okozott hatások minimalizálását. Ezen felül PMU-k alkalmazásával fejleszthetők tovább a szinkronfazor rendszerek, melyek segítségével a VER megfigyelhetősége sokkal hatékonyabbá és megbízhatóbbá válhat. Ezen PMU egységek akár 60-120 adatpontot is képesek másodpercenként rögzíteni, melyeket az *IEEE C37.118* protokoll alapján az irányítási központba továbbít a *PDC*-knek (*Phasor Data Concentrator*), ahol a rendszer nagy területi megjelenítésére és feszültségstabilitási vizsgálatra is lehetőséget biztosít. Az alábbi blokkvázlat egy tipikus átviteli hálózati ICT rendszert mutat be. [10]



8. ábra: Tipikus átviteli hálózati ICT struktúra [10]

3 Kiberbiztonság

A cybersecurity sajnálatos módon egyre közismertebb fogalommá válik, az élet egyre több területén találkozhatunk vele. Magyar fordítása a kiberbiztonság, amely az számítógépes rendszerek védelmét, támadásokkal szembeni ellenállóképességét jelenti. A modern IT infrastruktúrák szinte kivétel nélkül alkalmaznak internetes megoldásokat, így megfelelő védekezés nem csak fizikai, hanem kommunikációs szinten is szükséges.

3.1 Elméleti alapok

3.1.1 IoT és ipari IoT

A kritikus infrastruktúrákkal szemben olyan alapvető elvárásokat támasztunk, mint a megbízhatóság, hitelesség és információ-biztonság. Ezen három alappillér felel azért, hogy a rendszer folyamatosan biztonságos és minőségi ellátást nyújthasson [11]. Tipikus kritikus infrastruktúrák a mindennapi életünkhöz feltétlenül szükséges szolgáltatási rendszerek és alrendszerek, mint például a vízvezeték-rendszer a vízellátás miatt, vagy éppen a kutatás fókuszában lévő villamosenergia-rendszer, annak is a SCADA irányítórendszere. A hagyományoktól eltérő módon egyre inkább csökken a kritikus infrastruktúrák szegmentáltsága, melynek egyik fő oka, hogy az ellátás korlátlanságára törekedve célszerű minimalizálni, de lehetőség szerint inkább eltűntetni ezen rendszerek fizikai határait. [5]

Az Internet of Things – azaz a dolgok internete – egyre nagyobb teret nyer, életünk minden területén egyre több és több internethez csatlakozó eszközt használunk. Ezek a berendezések elsősorban kommunikációs céllal kapcsolódnak a világhálóhoz, hogy más okoseszközökkel összhangban hatékonyabban működjenek együtt. Másik fő előnyük, hogy a már-már világszerte korlátlan internetlefedettség miatt képesek vagyunk bárhonnan elérni ezeket az eszközöket, így a távvezérléssel járó minden előnyt – legyen az kényelem vagy gazdaságosság – kihasználhatunk. Jól megfigyelhető ez a trend mindennapi alkalmazásokban, mint például okosotthonokban, vagy modern irodai ICT infrastruktúrákban. Nem képez kivételt ez alól az ipar sem, hiszen a modern gyárak is egyre több okoseszközt alkalmaznak, így jelent meg az ipar 4.0 az egyre több *IIoT* (*Industrial IoT*) berendezés alkalmazásával. Ugyan ez igaz a villamosenergia-rendszerre is, hiszen a már korábban bemutatott – főként kommunikációs – hálózati komponensek nagy része rendelkezik internet eléréssel, legtöbbször pedig aktív kapcsolattal is. [5]

3.1.2 Kiberfenyegetettség, avagy biztonsági problémák

Az internet veszélyeit ma már jól ismerjük, azonban az IoT eszközök hordozta fenyegetettség kritikus hatással van az érintett infrastruktúrákra, jelen esetben a villamosenergia-rendszerre. A hálózat hatékonyságának és gazdaságosságának növelése mellet a biztonsági tényezőket sem szabad figyelmen kívül hagyni. Az alkalmazott internethez csatlakozó berendezések jóval nagyobb kockázatot jelentenek a rendszer számára,

hiszen ezek által nagyon sok hálózatba való potenciális belépési pont jelenik meg, melyekbe betörni nem könnyű, azonban megfelelően képzettség mellett nem is lehetetlen.

A témáról alkotott teljes körű látképhez érdemes sorra venni azokat a rizikófaktorokat, amelyek csökkentik a rendszerbiztonságot, vagy esetleg potenciális támadási pontot jelenthetnek. Egy kellően előkészített támadás során az elkövető hosszú időn keresztül tanulmányozza a célrendszert, megkeresi annak gyenge pontjait, előkészíti a stratégiát és a terepet, majd megfelelő előmunka után megkísérli a támadást. Ezen folyamatban a hálózat gyenge pontjainak feltárása a legfontosabb számunkra, ezért ezek általános vizsgálata szükségszerű. A legnagyobb fenyegetettségnek a villamosenergia-rendszer kommunikációs infrastruktúrája van kitéve. Ennek oka, hogy az alkalmazott protokollok és szabványok nagyon sokszínűek, és nincsenek egységesítve. Az eltérő használatuk inkonzisztenciát okozhat különböző szegmensek között, ami a kapcsolatuk sérülékenységét eredményezi. Az IoT eszközök sajnos nem minden esetben rendelkeznek megfelelő védelmi funkciókkal az internetes behatolások ellen, ezért ezek is nagy veszélyt jelentenek a hálózatra. Összességében azt a következményt vonhatjuk le, hogy az adatokért és távvezérlésekért felelős hálózatrészek vannak a legnagyobb fenyegetettségnek kitéve, hiszen a standardizáltság itt a legcsekélyebb, és itt okozhatók a legsúlyosabb károk is.

3.1.3 Lehetséges károk és kockázatok

A kiberveszélyek folyamatos kockázatot jelentenek a villamosenergia-rendszer számára, emiatt pedig érdemes tisztában lenni az esetleges támadások indítékaival, illetve a lehetséges következményekkel. Alapvetően megkülönböztethetünk szándékos és véletlen behatolást, károkozást, attól függően, hogy az elkövető direkt célpontként támadta-e meg a hálózatot, avagy sem. A ,,kiberbaleseteket” leggyakrabban hobbisták okozzák, akik otthonról teljes véletlenszerűen kerülnek bele a rendszerbe, ahol képzettség hiányában könnyen kárt tudnak tenni. Egyre gyakoribbak azonban szándékos behatolások, melyeket legtöbbször valamilyen terrorszervezetek követnek el, de előfordulhatnak politikai indíttatású támadások is. Összességében elmondhatjuk, hogy a kiberhadszíntér kiterjed már a kritikus infrastruktúrákra is, legjellemzőbben például a villamosenergia-rendszerre.

A támadások által számos fizikai kár is okozható a villamos hálózaton, melyek sokrétű következményekkel járhatnak. A rendszer megjavítása hatalmas összegeket emészthet fel, azonban ennél sokkal súlyosabb az okozható szolgáltatásmegszakadás. Ennek eredményeként sok ipari szegmensben következhetnek be leállások, a háztartási fogyasztók sem jutnak áramhoz, összességében tehát óriási gazdasági és szociális problémák keletkezhetnek. A politikai háborúk egyik új színtere sajnos szintén a kiberhadviselés, hiszen gyakran állami támogatással felvértezve következnek be a legújabb támadások és bűncselekmények.

3.2 Kibertámadások

3.2.1 Támadások kategorizálása

A támadásokat több csoportba sorolhatjuk aszerint, hogy a kritikus rendszer sebezhetőségét milyen irányból használják ki. Számos megközelítés létezik erre a kategorizálásra, de a valósághoz legközelebb a hardver, szoftver és kommunikáció szerinti bontás áll [12]. Természetesen ezen csoportosítások nem diszjunktak, így például az előbbit tökéletesen kiegészíti a következő csoportbontás: hagyományos IT-alapú, protokoll-specifikus, konfiguráció-alapú és az irányítófolyamatok elleni beavatkozások. [5]

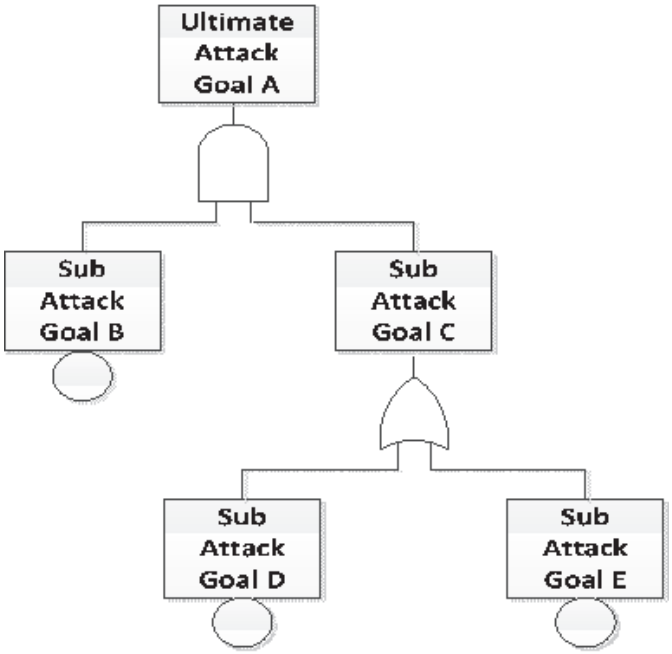
A hagyományos IT-alapú támadások leginkább az *ARP*, *DNS*, *NTP*, *DHCP* és *ICMP* hálózati szolgáltatásokat használják ki, leggyakoribb típusuk a *MIM* (*Man In the Middle*), melyet ARP poisoninggal valósítanak meg. A protokollspecifikus támadások a kommunikáló felek közti információt másítják meg leginkább, mindezt úgy, hogy a módosítják a protokoll szabályrendszerét, az üzenetek felépítését vagy a bennük található adatokat. Leggyakoribb támadási célpontjuk az Ethernet/IP, TCP/IP, ModBus, *UDP* és a DNP3. A konfiguráció-alapú támadások során általában SCADA alrendszerek végpontjai kerülnek célpontba, melyek berendezései hardveresen, szoftveresen vagy éppen a hálózati kommunikáció által kerülnek veszélybe. Konkrétan az irányítási folyamatokat célzó támadások középpontjában leginkább a már korábban említett RTU-k, MTU-k, IED-k és PLC-k állnak. Megfigyelhető, hogy ezen kategorizálás mentén a támadásokat aszerint különböztettük meg egymástól, hogy a rendszer mely szintjében tesznek kárt, nem pedig annak alapján, hogy milyen módszerrel teszik azt meg. Utóbbi szempont szerint a *DoS* (*Denial of Service*) jellegű és az adatbázist célzó kibertámadások fordulnak elő leggyakrabban [13]. Az megemlített módszerek és konkrét támadási típusok jelen dolgozatban nem kerülnek részletes bemutatásra, hiszen a vizsgálódásuk szempontjából működésük ismerete egyelőre nem szükséges. [5]

3.2.2 Modellezésük

A megfelelő mélységű vizsgálatokhoz és szimulációkhoz elengedhetetlen a támadások modellezése. A fentebb bemutatott kategóriákból már érezhető, hogy nagyon sokszínű támadási paletta áll az elkövetők rendelkezésére, amely ráadásul folyamatosan bővül. Amint sikerült bizonyos típusú behatolásokat kivédeni, máris jönnek létre újak, és ami a legsúlyosabb, hogy a létező támadásokat egymással folyamatosan kombinálják. Ezáltal teljesen új komplex módszerek alakulnak ki, melyek ellen igencsak nagy kihívás hatékonyan védekezni. Tekintettel arra, hogy a támadások ennyire sokszínűek lehetnek, olyan modellezési megközelítésre van szükség, amely kielégítő információt nyújt, azonban nem emészt fel túlzottan sok erőforrást. [5]

Az egyik legpraktikusabb modellezési forma a támadási fa. Ebben a struktúrában egy hierarchikusan felépített fagráf reprezentálja a folyamatot, melynek pontjai a támadás céljait, illetve részcéljait jelentik. Ezekből logikai kapuk – leginkább AND és OR – segítségével áll elő a teljes támadási szerkezet, illetve a végső cél. A modell

működését az alábbi ábra szemlélteti. A megközelítés nagy előnye, hogy viszonylag egyszerűen elemezhetők vele a támadások, azokról kellő logikai és strukturális ismereteket nyújt, és nem igényel nagy erőforrást. Hátránya viszont, hogy a támadás mély működési mechanizmusairól nem szolgáltat információt, azonban ez a kutatásom keretein belül megengedhető veszteség. [5]



9. ábra: Támadási fa [14]

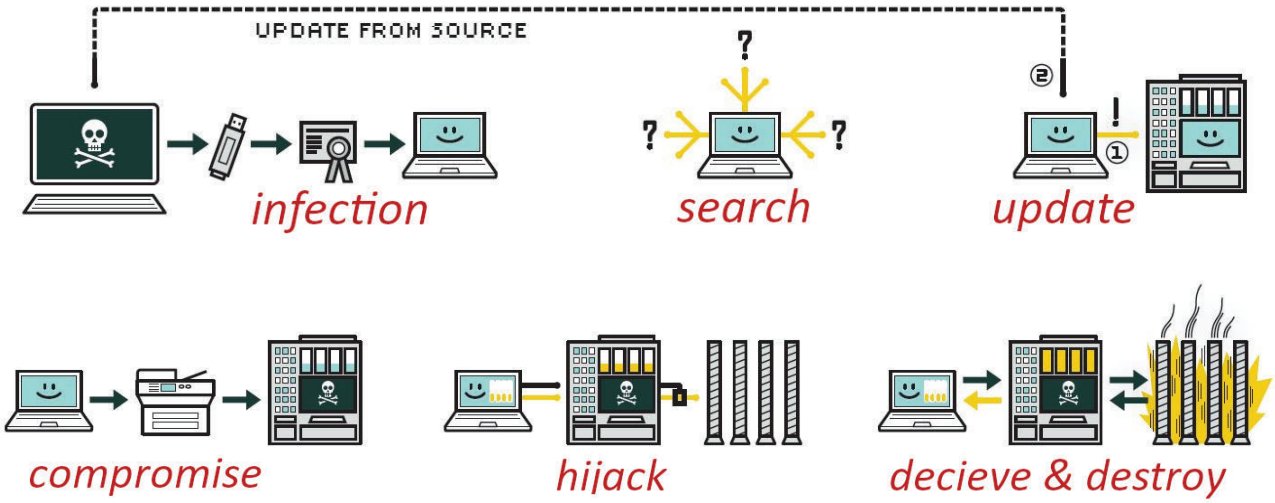
3.2.3 Esettanulmányok

Kibertámadások már régóta léteznek, az első *malware* (értendő: *malicious software*) 1971-ben készült el kísérleti céllal. A kártékony szoftverek fejlődése nagy ütemben indult meg ezután, ugyanis a 2003-ban a *Sapphire* névre keresztelt féreg 15 perc alatt bezúzta az internetet. Az első jelentős irányítórendszerek, konkrétabban SCADA rendszerek ellen elkövetett támadás 2010-ben történt, amikoris a méltán híres Stuxnet okozott károkat egy iráni nukleáris üzemanyagdúsító gyárban. A következő években egyre fejlettebb malware-ek láttak napvilágot, mint például a *Duqu* vagy a *Flame*. Az elmúlt időszak legnagyobb figyelmet kapott támadása azonban mégis csak az Ukrán villamosenergia-rendszer elleni, amely többszázezer fogyasztó számára okozott áramkimaradást. Az alábbi bekezdésekben a Stuxnetet, mint korszakalkotó támadást nyílik lehetőségünk jobban megismerni, majd az ukrajnai esetet is rövid bemutatásra kerül. [15]

3.2.3.1 Stuxnet

A Stuxnet működése hat részfolyamatra bontható, melyeket az 10. ábra szemléletet. A féreg első életszakaszában aktívan hatását nem fejti ki, csupán megfigyelés és a károkozás előkészítése a célja. A vizsgált eset során USB driveon (pendrive) keresztül került be a hálózatba a malware, ahol minden Microsoft Windows operációs rendszert futtató számítógépet megfertőzött. Ezt úgy tudta megtenni észrevétlenül, hogy magának digitális megbízhatósági tanúsítványt hamisított, melynek segítségével a detektáló

rendszereket át tudta verni. Ezután a Stuxnet olyan további számítógépeket keresett, melyek a megcélzott irányítási rendszerhez tartoznak, esetünkben például a nagy forgási sebességű urándúsító centrifugák irányítórendszeréhez. Ha egy adott gép nem célpont, akkor a féreg nem tesz semmit, amennyiben viszont igen, úgy megkísérli az internethez való csatlakozást, hogy saját maga legfrissebb verzióját letölthesse. Ezt követően megtámadja a célrendszer logikai kontrollereit *zero-day* – meglévő, de nem ismert biztonsági rések – sebezhetőségek kihasználásával. Ezután a Stuxnet először türelmesen kivár, aktívan kémleli a megcélzott rendszerek folyamatait, arról adatokat és információkat gyűjt. [15]



10. ábra: A Stuxnet működésének folyamatábrája [15]

Érdemes megfigyelni, hogy a malware eddig semmiféle konkrét kárt nem okoz, tehát az első életszakasz célja a fertőzés, terjedés, megfigyelés és előkészítés. A begyűjtött információk segítségével átveszi a Stuxnet az irányítást a centrifugák felett, majd meghibásodásig túlvezérli őket. Mindeközben a féreg meghamisított visszajelzéseket küld a külső platformokra, hogy a hibás, nem üzemszerű működés továbbra is észrevétlen maradjon. Ezáltal képes megfelelő időt biztosítani arra, hogy a folyamat visszafordíthatatlan legyen, így a károkozás végzetessé válik. [15]

3.2.3.2 Black Energy 3 (BE3)

2015. december 23-án az ukrán elosztóhálózatot ért kibertámadás következtében mintegy 225 000 fogyasztó szenvedett áramkimaradást több órán keresztül. A történet azonban ennél sokkal korábban kezdődik, hiszen ahogyan azt a Stuxnetnél már láttuk, a Black Energy 3 is jóval a károkozás előtt belekerül a célpontként kiválasztott rendszerbe. Először is a kiszemelt villamos hálózat több számítógépes munkaállomása kerül *e-mail spear phishing* áldozatává, amely nem más, mint károkozókat tartalmazó, ám hitelesnek tűnő levelek küldése a célszemélyeknek. [16]

Ilyen támadás ért el sikereket a BE3-ban is, így a féreg egy Microsoft dokumentum makróiban megbújva bekerült a rendszerbe. A malware a hálózatot észrevétlenül felderíti, majd a biztosított csatornákba való bejutáshoz szükséges adatokat kinyeri és közvetíti azokat az elkövető felé. Ezután az irányítórendszerbe történő bejutás is lehetségessé válik, ahol a Black Energy 3 *FDI* (*False Data Injection*) támadást alkalmazva kezdi el a konkrét károkozást. A módszer lényege, hogy a SCADA-ban valódi értékek helyett olyan módosított adatok kerülnek kijelzésre, melyek becsapják a rendszer. Ennek megvalósulása jelen esetben úgy történt, hogy a hamis adatok ellenőrzésekor az alállomási felügyelő a jelzett értékeknek megfelelően az irányítórendszer parancsára kinyitotta a megszakítót, amely azonban hibához vezetett. Mind a SCADA, mind a szakember helyesen végezte munkáját, azonban mind a kettő hamis adatok alapján dolgozott, fizikai meghibásodást okozva eláltal a villamosenergia-rendszeren, melynek következménye a kiesés is volt. [16]

3.3 Védelmi módszerek

3.3.1 Védekezési megközelítések

Mint már tudjuk, az igencsak komplex villamosenergia-rendszer nagy kiberfenyegetettségnek van kitéve, ráadásul az összetett szerkezetű hálózatnak hasonlóan bonyolult támadások esetén kell megfelelően ellenállnia. A VER kibervédelmére többféle megközelítés létezik, melyek rendre más stratégiát követnek. A legkézenfekvőbb módszernek a hálózat kellően biztonságosan történő kialakítása tűnik, azonban a villamosenergia-rendszer a világon mindenhol már kiépített és aktívan használt infrastruktúra. A meglévő hálózat optimalizálása lehet megoldás az elavult, biztonsági résektől hemzsegő rendszer védelmére, azonban ez óriási beruházásokkal, költségekkel és munkával járna, így már-már kivitelezhetetlennek tűnik. Gyakori cél ezen felül a rendszer elleni aktív támadások megszakítása, tehát az azonnali beavatkozás. Ez az eliminálás alapuló megközelítés ugyan hatékony lehet, ám a sikerhez a támadások működésének pontos ismerete szükséges. Ez azt jelenti, hogy újszerű, még nem ismert támadás esetén közel hatástalan a védelmi mechanizmus, ezen felül pedig nagy erőforrásokat is igénybe vehetnek ezen eliminációs algoritmusok.

A preventív védelmi módszerek lényege, hogy nem várjuk meg, míg egy támadás aktívvá válik, azaz elkezdi kifejteni a hatását, hanem már azt megelőzően kiiktatjuk a rendszerből. Érdekesség, hogy a kibertámadások nagy része sokkal a behatolás ideje után történik, ugyanis ebben az időszakban az elkövető adatot gyűjt, elemzi a rendszert abba beolvadva, és vár a tökéletes időzítésre. Ennek tudatában nagy remények fűzhetők ehhez a megközelítéshez, hiszen, ha már behatoláskor képesek vagyunk észlelni egy leendő támadást, akkor elkerülhető a konkrét károkozás.

3.3.2 Detektálórendszerek

A prevención alapuló védekezésnek két módja létezik, melyek az anomália- és behatolás-detektálás. Az angol irodalomban *ADS* (*Anomaly Detection System*) és *IDS* (*Intrusion Detection System*) rendszerekként emlegetett platformok képesek felismerni a rendszerben megjelenő anomáliákat és behatolásokat, ezáltal a kártékony hatás kifejtése előtt tudjuk megfelelően lereagálni a támadást. Az IDS rendszereket három szempont szerint csoportosíthatjuk; a detektáló módszer, az IDS típusa, és passzív/aktív felismerés alapján.

A tudás-alapú IDS rendszerek rendelkezésére áll egy ismert támadásokból és azok mintáiból, előre definiált viselkedéseiből alkotott adatbázis. A működése során vizsgálja a kommunikációs hálózatot, melynek forgalmán folyamatos mintaillesztést végez, és így azonosít esetleges támadásokat. Ezzel szemben a viselkedés – vagy anomália – alapú detektálás mintakeresés helyett folyamatosan profilozza a hálózati forgalmat. Ebben az esetben nehéz előre definiálni, hogy milyen viselkedési formák jelentsenek veszélyt, azonban nagy előnye ennek a módszernek, hogy nem csak ismert támadások detektálhatók vele. A két rendszer közötti jelentős eltérés még a passzív és aktív felismerés során mutatkozik meg. Míg a korábbi esetben anomália-detektálás esetén riasztások generálódnak, melyek emberi beavatkozás szükségességét jelzik, addig az aktív rendszerek úgy vannak konfigurálva, hogy szükség esetén kapcsolat megszakítására is képesek legyenek önállóan. [10]

4 A szimulációs keretrendszer prototípusa

4.1 Testbedek

Tesztelési keretrendszereket – továbbiakban testbedek – a műszaki tudományok minden területén használunk új technológiák, algoritmusok, eszközök és elméletek tesztelésére és vizsgálatára. Ezek olyan környezetek, melyben lehetőségünk nyílik modellezni, illetve szimulálni az elemzendő folyamatokat és technológiákat, tehát lényegében kísérletezési lehetőséget biztosítanak. Felépítésük alapján négy fő típusú testbedet különböztethetünk meg: hardver, szimuláció, valós-idejű szimuláció alapúakat és hibrideket. [17]

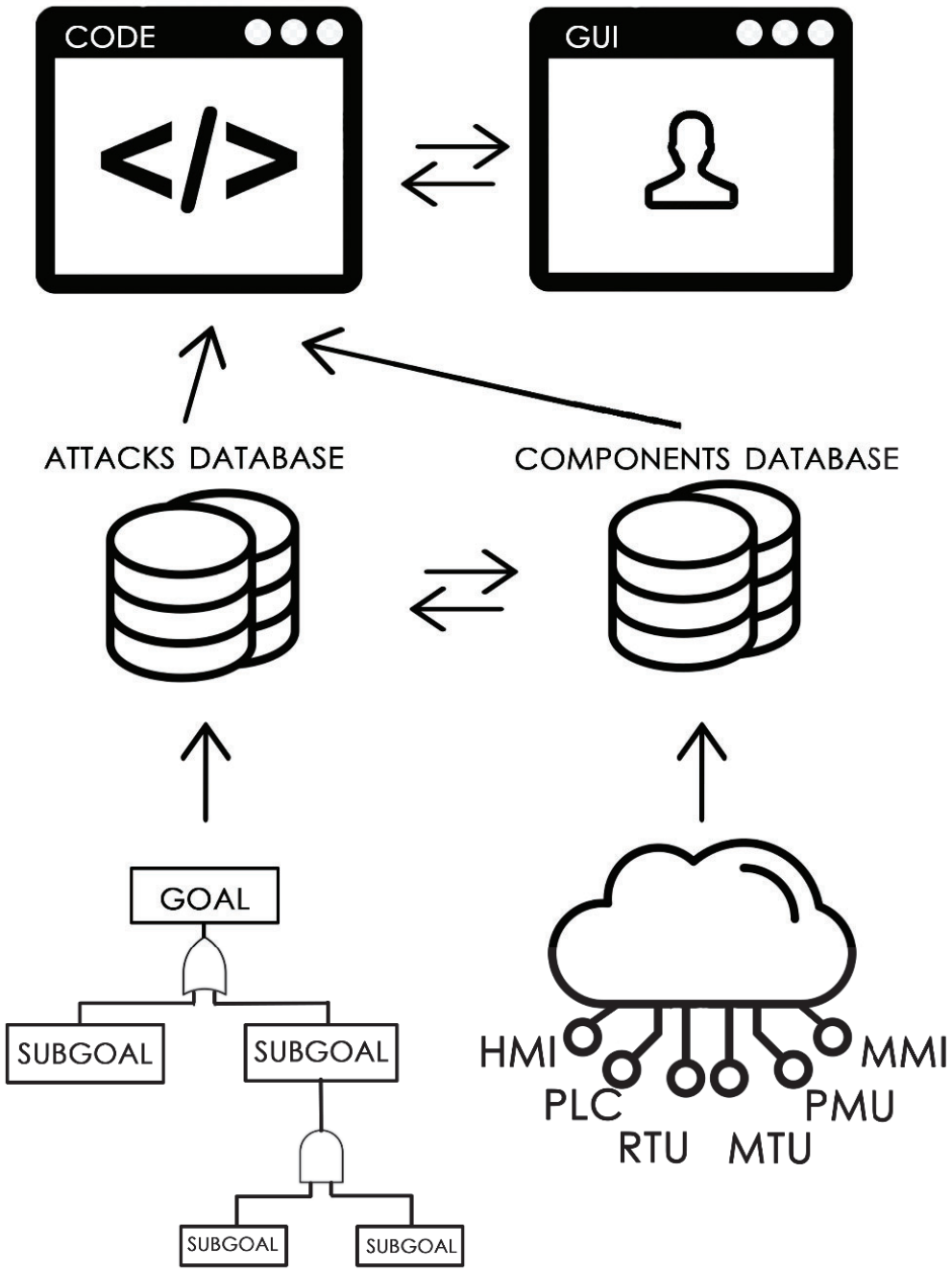
Míg a hardver alapú keretrendszerek valódi fizikai eszközöket és berendezéseket használ, ezért fejlesztésük és kivitelezésük nagyon drága. Sokkal költséghatékonyabbak a tisztán szimulációs alkalmazó testbedek, hiszen ebben az esetben nem szükséges hardverekre beruházni. Fejlesztésük és kivitelezésük viszonylag egyszerű, azonban hátrányuk, hogy mivel nem real-time működésűek, sokkal kevésbé valósághűek, illetve pontosak a többi rendszerhez képest. Mivel hardverek alkalmazására az ilyen típusú testbedek nem alkalmasak, illetve a valós-idejű funkciók hiányában nem képesek lehetőséget biztosítani a kommunikációs hálózat modellezésére és vizsgálatára. Ezzel szemben, a valós-idejű keretrendszerek alkalmasak valósághű szimulációkra is, hiszen akár kommunikációs vagy hardverszintű anomáliákat is elemezhetünk segítségével. A hibrid testbedek értelemszerűen az eddig bemutatott három típust ötvözi; fő előnye, hogy az alapvetően real-time szimulációban bármikor helyettesíthetők a felhasznált hardverek azok megfelelői szimulációjukkal. A négy alaptípuson kívül népszerű még az úgynevezett *HIL* (*harware-in-the-loop*) megközelítés is. Ennek lényege, hogy olyan környezetet hozunk létre, melyben a hardvert valós időben szimuláljuk, a szoftvert pedig a szimulátorban vizsgáljuk offline. [17]

A villamosenergia-rendszer szimulációjára jónéhány platform elérhető, mint például a *PowerFactory*, *MatLAB/Simulink*, vagy a *PowerWorld*. Többségük ráadásul rendelkezik *API* (*Application Program Interface*) integrációs lehetőséggel is. Kommunikációs hálózat szimulációjára alkalmas platformok az *Opnet*, *Omnet++*, *Ns2* és *Ns3*, melyeket érdemes a testbedek kiegészítéseként használni. [17]

Az általam tervezett platform szimuláció alapúként kerül kivitelezésre, majd azt hálózati szimulátorral kiegészítve hibriddé szeretném továbbfejleszteni. A távlati célokat szem előtt tartva a fejlesztés során a HIL megközelítés szerint építem fel a keretrendszert.

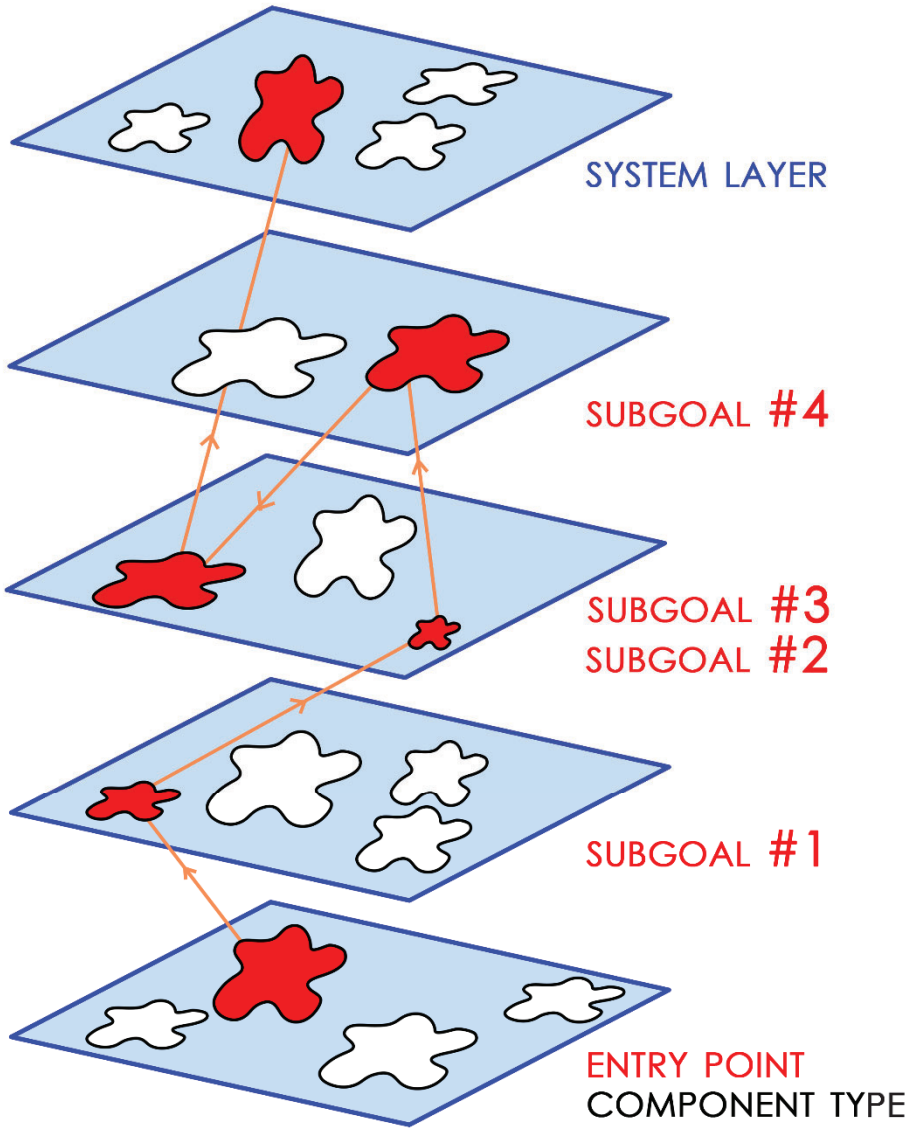
4.2 A platform felépítése

A teljes keretrendszer struktúráját az alábbi blokkvázlat szemlélteti. A platform több egységből áll össze, melyek részletesebben a következő alpontokban kerülnek bemutatásra. Mint látható, a szóban forgó négy szegmens a két adatbázis, a működtető program, illetve a grafikus felhasználói felület.



11. ábra: A testbed struktúrája

A rendszer a korábban említett integrált SCDG struktúrát alkalmazza. Ebben a felépítésben 5 rétegre bontjuk a modellezendő villamosenergia-rendszer, majd ezeket a rétegeket feltöltjük a megfelelő komponensekkel. Az építőelemek közül egy adott támadásban érintetteket működés közben piros színnel jelzi a szoftver, és kirajzolja az általuk alkotott útvonalat. Ebben a routing üzemmódban meghatározásra kerül a VER-be történő behatolási pont (*entry point*), illetve támadás végső célja is. Ez a modell az alábbi ábrán mutatható be szemléletesebben.



12. ábra: VER és támadás modellezés

4.2.1 Támadások adatbázis

A keretrendszer egyik mögöttes adatbázisa a támadások nyilvántartására szolgál. A korábban bemutatott modellezési lehetőségek közül a támadási fa megfelelő megoldást jelent, hiszen strukturális információkat biztosít, amely esetünkben kielégítő. A hatékony tárolás és felhasználhatóság érdekében ezen modell szerint a támadásokat subgoalokra bontjuk, és ezeket felvezetjük az adatbázisba. A konkrét támadások ezekből fognak építkezni, így minimálisra csökkenthető a szükséges erőforrás. A rendszer bővíthetőségét is biztosítja ez a módszer, hiszen új, például kombinált támadás esetén fel tudunk használni korábban eltárolt entitásokat. Minden egyes támadásról – pontosabban subgoalról – nyilvántartjuk, hogy a rendszer mely pontján képes behatolni, illetve hogyan és hol fejti ki hatását. Ez a két attribútum a vizsgált hálózaton történő szimulációhoz szükséges, ugyanis így lehetőségünk nyílik a támadások útvonalát követni, illetve hatásukat elemezni.

4.2.2 Komponensek adatbázis

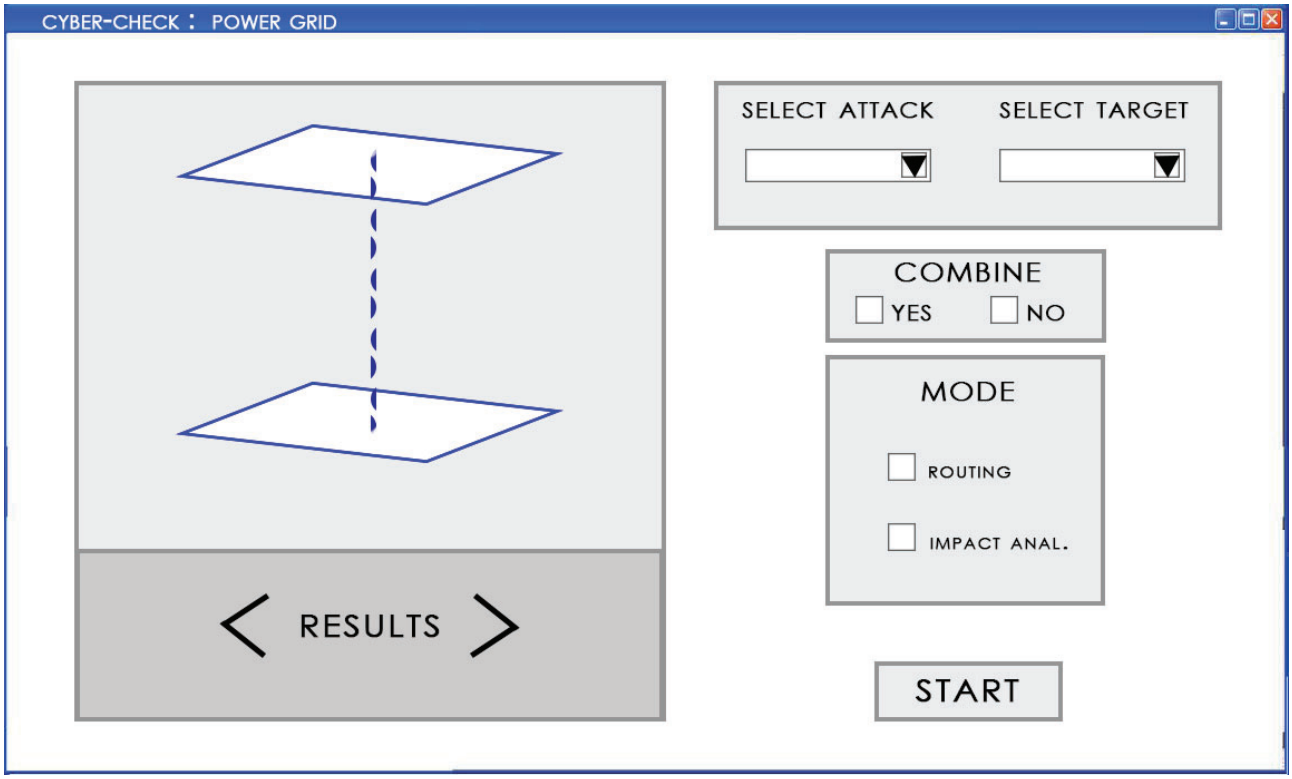
A másik adattömb a rendszert alkotó komponenseket tartja nyilván. Tetszőleges építőelemeket felvehetünk az adatbázisba, a hálózatmodell mindig ezek függvényében változik. Fontos kiemelni, hogy ebben a megközelítésben nem egy konkrétan felépített rendszer vizsgálata válik lehetővé, hanem egy általános struktúra lesz elemezhető modulárisan. Ehhez elengedhetetlen, hogy a korábban bemutatott integrált *SCADA+SG* (továbbiakban *SCDG*) rendszer pontosan definiálva legyen, ezért minden egyes komponens esetén a legfontosabb attribútum, hogy a hálózat mely szintjén helyezkedik el. Másik fontos jellemzője ezen entitásoknak, hogy mely másik egyedekkel működnek együtt, illetve, hogy ez az együttműködést milyen protokollt használ – ha használ. Tekintettel arra, hogy ez az együttműködés általában kommunikáció alapú, ezért szükséges lehet egy azt szimuláló segédplatform is, amely megtervezésére azonban a kutatás ezen szakaszában még nem került sor.

4.2.3 Szoftver

A két adattábla közötti kapcsolatot a működtető szoftver biztosítja. Ennek segítségével hozhatjuk továbbá létre a villamos hálózatot is, melyen a szimulációkat szeretnénk végezni. A program biztosítja továbbá a grafikus felülettel való kommunikációt, illetve a szimulációs számítások és algoritmusok is itt kerülnek implementálásra és futtatásra. A funkciókat és módszereket később tárgyaljuk részletesebben.

4.2.4 Grafikus felhasználó felület

A grafikus felhasználói felület (*GUI* - *Graphical User Interface*) biztosítja a szoftver külvilággal (userrel) való kommunikációját. A GUI fő eleme egy szimulációs ablak, melyen keresztül nyomon követhetők az éppen futó szimulációk, illetve a futtatás eredményei. Ezen a felületen a rétegzett rendszer látható, és azok a komponensek, melyek a kiválasztott szimulációban érintettek. A felhasználónak lehetősége nyílik választani, hogy impact-analysis vagy routing módban szeretné futtatni a kiválasztott támadást. Opcionálisan választható még a megcélzott komponens, illetve a két szimulációs módot kombinálhatjuk is. A menürendszer és a felület prototípusa az alábbi ábrán látható.



13. ábra: GUI

4.3 Szimulációs elvek

A programot elindítva az SCDG rendszer normál üzemállapotában mutatkozik, a menürendszerben pedig számos lehetőség kínálkozik a felhasználó felé. Kiválaszthatjuk, hogy a rendszer ellen milyen támadást szeretnénk ,,elkövetni", illetve, hogy melyik szimulációs módszer kerüljön futtatásra.

Ezek egyike a támadások útvonalának követése. Ebben a szimulációs módban a behatolástól egészen a végső célkomponensig megfigyelhetjük a támadás haladását a rendszerben. A kijelzés úgy történik, hogy a behatolási ponttól kezdődően folyamatosan haladó nyilak kezdenek el mozogni a többi réteg komponensei felé. Minden egyes érintett hálózati elem esetében a program tárolja, hogy milyen módon jutott be a komponens, majd a futtatás végén szöveges formában is megkapjuk az útvonalat.

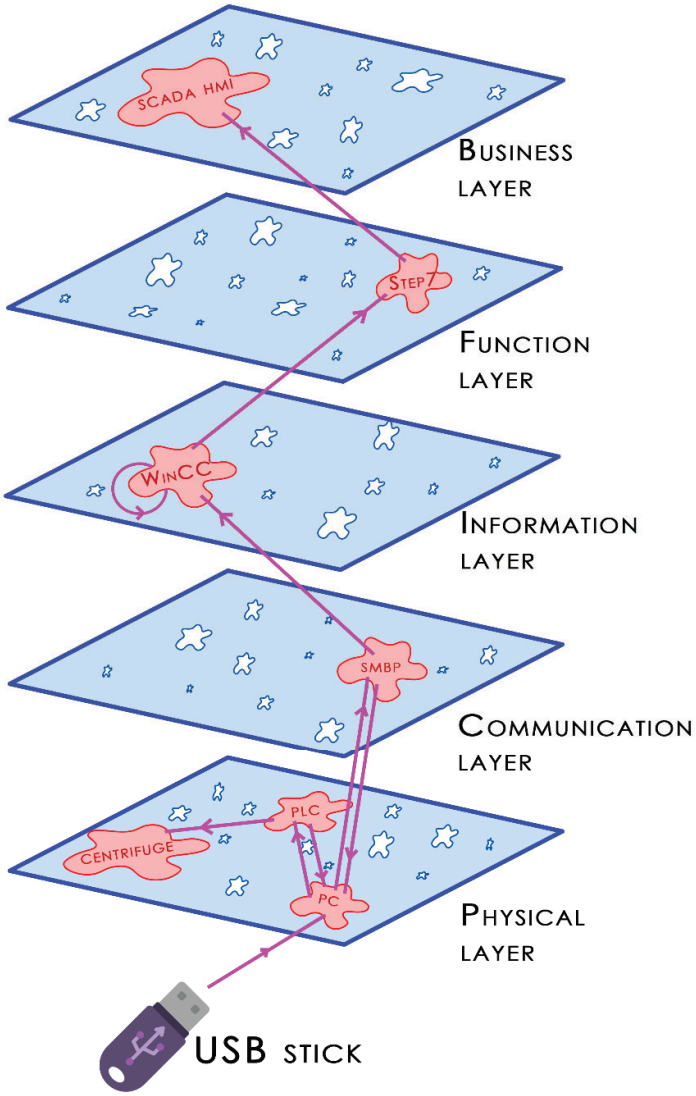
A másik szimuláció – impact-analysis – segítségével a támadások hatását figyelhetjük meg és vizsgálhatjuk a hálózaton. Ennél a módszernél az SCDG modell megrongált komponensei piros színnel jelölődnek ki, és lehetőségünk nyílik ezek közelebbi vizsgálatára. Egy-egy érintett építőelemre ,,rá tudunk nagyítani", amely által megnézhetjük, hogy milyen kár keletkezett benne. A futtatás eredményeként szöveges formában leírva is megjelenik, hogy a rendszer mely részében milyen hatást fejtett ki az indított támadás.

4.4 A működés bemutatása

A prototípus környezet működése az alábbi koncepció ábrán látható. A bemutatott támadás a korábban már elemzett Stuxnet, amely egy iráni urándósító üzemben okozott károkat. Érdemes megfigyelni, hogy a fentebb részletezett működés nem nyújt információt a támadás struktúrájáról, illetve a rendszerben megtett útjáról. Ezzel ellentétben ez a testbed pontosan ezekről ad majd felvilágosítást. Nézzük meg tehát, hogy mit is láthatunk a szimuláció futtatásának eredményeként.

4.4.1 Stuxnet routing

A malware egy pendriveon keresztül felkerült a kiszemelt rendszer egy Windows operációs rendszert futtató számítógépére, melyről LAN-on keresztül az *Server Message Block Protocolt* használva átterjedt a többi *PC*-re is. Ezután sikeresen bemásolta magát *SQL injectionnel* a Siemens *WinCC* adatbázisszervereibe, majd befolyásolta a szintén Siemens gyártmányú *Step7* SCADA rendszert. Az itt történt hamisítás eredményeként valótlan adatok jelentek meg a végrendszereken futó HMI-ken, melynek következtében a PC-k és PLC-k között észrevétlenül kialakult a fertőzött kapcsolat. A PLC-k felett átvette a vírus az irányítást, melynek segítségével a centrifugák forgási sebességét túlterhelésig módosította.



14. ábra: A Stuxnet szimulációja

Jól nyomon követhető a behatolás és a terjedési út, az eredményes befolyásolásig. A testbed alkalmazásával ha nem is feltétlen elkerülhetők, de a gyenge pontok kimutathatóvá válnak, és egy nem éles betörés szimulálásával a rendszer megbízhatósága, biztonsága, robosztussága érdemben növelhető.

5 Zárszó

A korábban bemutatott működési koncepció megerősíti azt a feltételezést, mely szerint a támadások strukturális ismerete kielégítő információt hordoz azok rendszerben történő vizsgálatához. Ezen funkciók alkalmazásával képesek lehetünk rámutatni, hogy a gyakorlatban a villamosenergia-rendszer mely elemei vannak kitéve a legnagyobb veszélynek, illetve, hogy melyek a főbb gyenge pontok. A routing és impact-analysis szimulációs módszerek lehetőséget biztosítanak ADS/IDS rendszerek tesztelésére és vizsgálatára, ezen felül pedig a testbed oktatási és demonstrációs célokra is felhasználható lehet. Az általam tervezett testbed segítségével a teljes villamosenergia-rendszer komplex vizsgálatára nyílik lehetőség az irodalomban fellelhető platformokkal ellentétben. Az ismertetett példa rámutat, hogy a rendszer egyszerű és jól-strukturált módon képes szimulálni a támadásokat, ezáltal valós-időben alkalmazva ADS/IDS funkciókat is képes ellátni.

A platform jelenleg prototípus szintjén alkalmas pontosabban specifikált kutatási célok által motivált irányokba való módosításra is. A megtervezett rendszer hasznos lehet a hazánkban a villamosenergia-rendszer kiberbiztonsága érdekében nemrég megalakult *SeConSyS* együttműködés általi felhasználásra és továbbfejlesztésre. A *BME Villamos Energetika Tanszék FIEK Smart Grid Laboratóriumában* hamarosan telepítésre kerülő kisfeszültségű alállomási kommunikációs rendszer vizsgálatára is alkalmas lehet a platform, melyet akár a laboratóriumi igények szerint testre is szabhatunk.

A kutatás során a legnagyobb kihívást a célplatform megtervezéséhez szükséges komplex háttértudás megismerése és megszerzése volt. Egy tesztelői keretrendszerhez feltétlenül ismerni kell minden érintett tudományterületet, amely jelen esetben a villamosenergia-rendszer felépítésétől kezdődően a rendszerirányításon és digitalizáción keresztül egészen a hálózati kommunikációig és kiberbiztonságig kiterjedt. Az irodalom alapos tanulmányozása során gyakran felmerülő probléma volt az az inkonzisztencia, amit a korábban már említett standardizáltság hiánya okozott. Ennek tudatában potenciális kutatási terület lehet egy teljeskörű szabványrendszer kialakítása a villamosenergia-rendszer minden szegmensére.

Jelen dolgozatomban a fejlesztés előkészületeit és a testbed prototípusának megtervezését mutattam be. Kutatásom következő szakaszában a támadások és rendszerkomponensek gyűjtésének folytatása, tanulmányozása és az adatbázisnak megfelelő formába való öntése lesz a fő célom, melyet majd a következő generációs program megírásával párhuzamosan a jelenleg rendelkezésre álló ADS és IDS rendszerek tanulmányozása fog követni.

6 Irodalomjegyzék

[1] https://techjury.net/blog/how-many-iot-devices-are-there/

[2] https://index.hu/techtud/2019/10/20/conficker-virus-fereg-microsoft-zombihalozat-evfordulo-kiberbiztonsag/

[3] Al-Ameri, Ahmed.: Méthodes analytiques d'étude pour la diminution des pertes de puissance dans les réseaux électriques maillés en utilisant des techniques d'optimisation pour le dimensionnement et l'emplacement des générateurs décentralisés, 2017

[4] Dr. Vokony I.: Átviteli hálózat üzemvitele – SCADA, EMS alapok, Villamosenergia-rendszer üzeme és irányítása, 15. előadás, BME Villamos Energetika Tanszék

[5] Molnár M.: A villamosenergia-rendszer kiberfizikai biztonsága, IX. Mechwart András Ifjúsági Találkozó – Magyar Elektrotechnikai Egyesület, 2019. szept. 17., Debrecen

[6] Prikler L.: Smart Grid, A jövő energetikája – víziók és valóság, 5. előadás, BME Villamos Energetika Tanszék

[7] Leszczyna R.: A Review of Standards with Cybersecurity Requirements for Smart Grid, Computers & Security, 2018

[8] Khalil I., Atiquzzaman M., Kumarage H., Abdulatif A.: Privacy-preserving cloud-based billing with lightweight homomorphic encryption for sensor-enabled smart grid infrastructure, IET Wireless Sensor Systems, 7, July 2017

[9] An introduction to the Smart Grid Architecture Model, Energy Networks, Australia, https://www.energynetworks.com.au/sgam/hybrid/index.htm?goto=1:8

[10] Sun C-C., Hahn A., Liu C-C.: Cyber security of a power grid: State-of-the-art, Electrical Power and Energy Systems, 99, 2018, 45-56.

[11] Otuoze O. A., Mustafa M. W., Larik R. M.: Smart grid security challenges: Classificiation by sources of threats, Journal of Electrical Systems and Information Technology, 5, 2018, 468-483

[12] Irmak E., Erkek I.: An overview of cyber-attack vectors on SCADA systems, 6th International Symposium on Digital Forensic and Security, Antalya, Turkey, 22-25 March 2018

[13] Rodofile N. R., Radke K., Foo E.: Extending the Cyber-Attack Landscape for SCADA-based Critical Infrastructure, International Journal of Critical Infrastructure Protection, 2019

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

[15] Kushner D.: The real story of stuxnet, IEEE Spectrum, 50(3), 48–53., 2017

[16] Whitehead, D. E., Owens, K., Gammel, D., & Smith, J.: Ukraine cyber-induced power outage: Analysis and practical mitigation strategies, 2017, 70th Annual Conference for Protective Relay Engineers (CPRE)

[17] Gunduz, M. Z., & Das, R.: A comparison of cyber-security oriented testbeds for IoT-based smart grids. 2018, 6th International Symposium on Digital Forensic and Security

Köszönetnyilvánítás

Végezetül pedig szeretnék köszönetet mondani az *Energetikai Szakkollégium* PR alosztályvezetőjének, kedves szakkollégista társamnak, *Schlosser Ilonának*. A prototípus keretrendszer bemutatására szolgáló ábrák elkészítésében vállalt elévülhetetlen érdemeiért nagyon hálás vagyok.

Köszönöm szépen a segítségedet, Babszi!