Cyber Security of Smart Grids – concept for implementation

Киберсигурност на интелигентните мрежи - концепция за изпълнение

On line 9-та Международна енергийна конференция „Енергетика и киберсигурност – рискове и противодействие”
11/02/2021г.

- Панел 4: Интелигентни мрежи и кибер сигурност.

Предстояща Трансформация на енергийните сектори от конвенционални към интелигентни дерегулирани пазарни структури

Енергийният сектор се преструктурира в много части на света. Структурата му се трансформира от регулирана (правителствено-контролирана) до дерегулирана (пазарно контролирана).

Целият енергиен сектор е разделен на три основни подсектора:

1. компании за генериране на енергияGENCO);
2. преносна компания (TRANSCO) и
3. дистрибуторски компании (DISCOM).

В допълнение към тези три основни подсектора, различаваме още връзки към:

- независимия системен оператор (ESO);
- Българска независима електроенергийна борса;
- търговци на електро-енергия;
- крайни снабдители;
- потребители.

Киберсигурност на интелигентни /умни/ мрежи

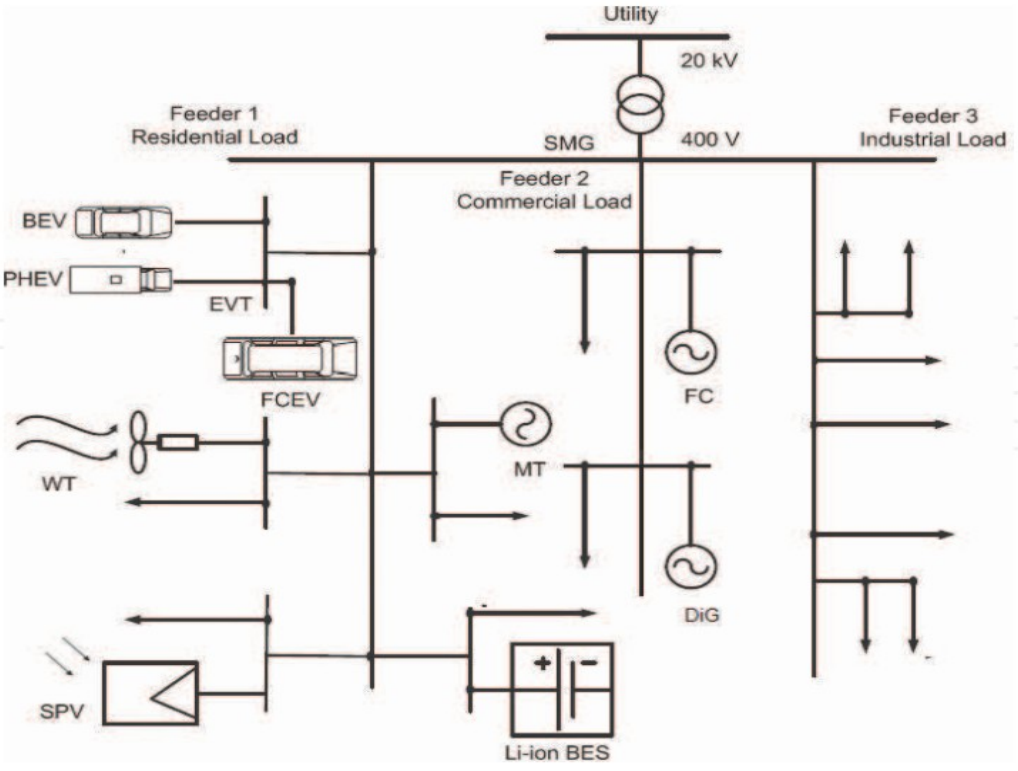
Конвенционалната мрежа може да бъде преобразувана в интелигентна мрежа с включване на следните характеристики:

- Самовъзстановяване при възникване на смущения и прекъсвания;
- Включване на програми за обратна връзка доставчик-клиент;
- Устойчивост срещу всякакъв вид кибер и физическа атака;
- Способна да доставя качествена енергия, според изискванията на клиента;
- Способна да включва всички източници на генерация, т.е. конвенционални и възобновяеми;
- Разрешава включването на устройства за съхранение;
- Разрешава преструктуриране за развитие на нови пазари, услуги и продукти;
- Обезпечава икономично снабдяване чрез оптимизиране на ресурсите.

1. Интелигентни технологии в електро-генериращия сектор

Някои от тези технологии са както следва:

1.1. Включване на разпределено генериране на енергия в микромрежи



Микромрежата може да включва:

1. фотоволтаичен източник SPV,
2. вятърна турбина WT,
3. микротурбина MT,
4. горивни клетки FC,
5. зарядни станции за електрически превозни средства EVT,
6. акумулаторна батерия BES,
7. дизелов генератор DG

и електрически товари.

1.2. Управление на микромрежата чрез честотно регулиране

Маховикът е в състояние да улавя енергия от периодични енергийни източници с течение на времето и да доставя непрекъсната мощност към мрежата.

1.3. Контрол на генерацията

За генериране и контрол на натоварването, надзорът се осъществява чрез използване на SCADA система.
SCADA системите - за директна комуникация и взаимодействие с различни устройства като сензори, клапани, помпи, мотори, задвижвания и т. н., посредством интерфейс човек-машина (HMI).

Съвременни SCADA системи

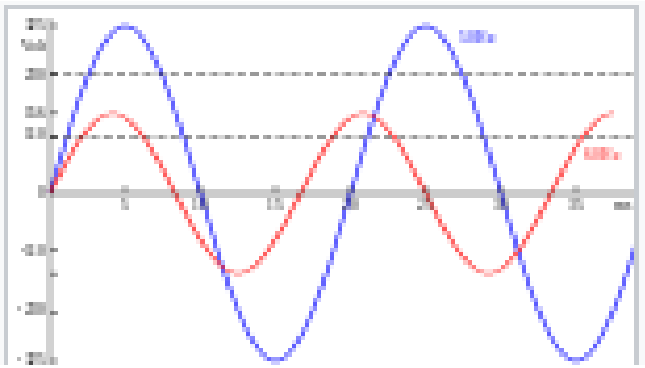
2. Интелигентни технологии в преносния сектор

Различните изграждащи елементи на една интелигентна и надеждна преносна система са, както следва:

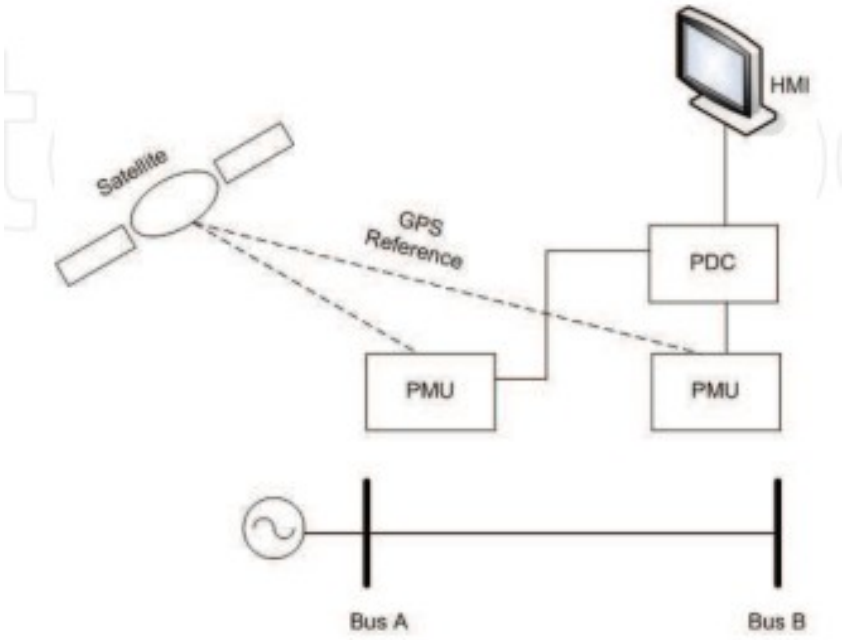
- широко обхватна комуникационна мрежа,
- фазоизмервателни модули (PMU),
- концентратори за фазови данни (PDC) и
- интелигентни подстанции.

2.2.1. Фазоизмерители

Това са устройства използвани за изчисляване на величината и фазовия ъгъл на напре-жение или ток в електричес-ката мрежа, използващи общ източник на време за синхронизация.



2.2. Фазови концентратори на данни (PDC)



Основната функция на концентратора е да събира и сортира фазови измервания, получени от фазоизмерителите, като сигналите се преобразуват в полезна информация, която е достъпна за интерфейса на системата човек-машина (HMI).

Колкото една система е по-напреднала във внед-ряването на цифровите технологии, толкова систе-мата е по-зависима от тях и толкова е по-уязвима към кибератака.

Днес основното предизвикателство пред инфра-структурата, сигурността и икономическото благополучие идва от заплахата от кибератака.

Рисковете за провеждане на кибер-саботаж срещу критичната инфраструктура съществува и ще се увеличива във времето. Това важи за цяла Европа, тъй като кибер инфраструктурата все повече обхваща границите. И нашето икономи-ческо бъдеще в Европа зависи от управлението на тези рискове.

Планиране на устойчивост на умните мрежи

Неочакваните нарушения на нормалния живот все още произтичат от аварии или природни явления и бедствия, като земетресения и наводнения, отколкото от умишлени саботажи.
Но съществуват по-взискателни сценарии, при които има вероятност, свързаните рискове да се окажат в ефект на домино, създаващи проблеми, които обхващат различни сектори от икономиката. Това може да се случи при напреднали кибератаки.

С планиране на сигурността се цели оценяване вероят-ните загуби като продукт от различни фактори:

- брой, умения и степен на мотивация на кибер-престъпниците;
- мащаб на първоначалното въздействие;
- продължителност на прекъсване на услугите;
- щетите от това прекъсване.

Планиране на устойчивост на умните мрежи

Възможности за противодействие:

- редуциране времето за възстановяване на засегнатите микромрежи;
- запазване способността на критичната информационна и комуникационна инфраструктура за самовъзстановяване на микромрежите;
- намаляване мащаба на първоначалното въздействие;
- споделяне с мрежова скорост на информация-та за кибератаки или очаквани такива между операторите на критични системи;
- намаляване на уязвимостта на умните мрежи;
- насърчаване на технологичен трансфер на най-добри практики, стандарти и доброволни насоки и изследвания в областта на приложната криптография и киберсигурност за микромрежи.

Планиране на устойчивост на умните мрежи

Кой ще плаща за способноста за защита на мрежите?

По-голямата част от инфраструктурата в Европа е в ръцете на частния сектор, въпреки че в отрасли, като електро и газоснабдяването, са регулирани от държа-вата.

Решението – всяка компания, която управлява крити-чни инфраструктури, трябва да й се разшири прите-жавания лиценз, че ще поддържа горецитираните възможности.

Регулаторните органи вече трябва да гарантират, че индустрията съответства на националното, европей-ското и международното законодателство за безопас-ност, а сега трябва да се добави киберсигурност към това. По този начин може да се осигурят равни усло-вия на конкуренция и да се приеме, че разходите в повечето случаи, трябва да бъдат прехвърлени на потребителя.

Киберсигурност на интелигентни /умни/ мрежи

ЗАКЛЮЧЕНИЕ

Киберсигурността на интелигентната мрежа трябва да се справя както с невнимателните компромиси на електрическата инфраструктура, поради грешки на потребителите, откази на оборудването и природни бедствия, така и от умишлени атаки, като например от недоволни служители, индустриален шпионаж и терористи.

БЛАГОДАРЯ ЗА ВНИМАНИЕТО

Димитър Куюмджиев
Енергиен експерт
БЕМФ