REZUMAT

Analiza siguranței în funcționare a sistemului electroenergetic național și implementarea de măsuri de protecție împotriva factorilor de risc

Conducător de doctorat,
Prof. univ. dr. ing. Horia Leonard Andrei

Doctorand,
ing. Ioan Marinescu

TÂRGOVIȘTE
2019

Cuprins

I SISTEME ELECTRONERGETICE. RELAŢIA PRODUCĂTOR-DISTRIBUITOR-CONSUMATOR

I.1 SISTEMUL ELECTROENERGETIC ÎN ROMÂNIA 4
I.1.1 Contextul temei de cercetare 4
I.1.1.1 Actualitatea temei 4
I.1.1.2 Structura generală 4
I.1.2 Repere ale producerii, transportului, distribuţiei şi furnizării de energie electrică în România 5
I.1.3 Principalele facilităţi de producere a energiei electrice prezente în România 5
I.1.3.1 Termocentrale 5
I.1.3.2 Centrale nuclearelectrice (Atomocentrale) 5
I.1.3.3 Hidrocentrale 6
I.1.3.4 Energia solară 6
I.1.3.5 Centrale eoliene 6
I.2 RELAŢIA PRODUCĂTOR – DISTRIBUITOR – CONSUMATOR 7
I.2.1 Distribuţia şi furnizarea energiei electrice în România 7
I.2.2 România ca parte integrantă a sistemului energetic european 8
I.2.3 Perspectivele strategiei energetice 8
I.2.4 Analize şi previziuni ale Autorităţii Naţionale de Reglementare în domeniul Energiei 8

II IDENTIFICAREA PARAMETRILOR INFRASTRUCTURILOR CRITICE DIN SISTEMELE ELECTROENERGETICE ŞI MANAGEMENTUL RISCURILOR 9

II.1 INFRASTRUCTURILE CRITICE ASOCIATE REŢELELOR ELECTROENERGETICE ŞI IDENTIFICAREA PARAMETRILOR ACESTORA 9
II.2 MODELAREA INFRASTRUCTURILOR CRITICE ASOCIATE REŢELELOR ELECTROENERGETICE 11
II.2.1 Sistemul electroenergetic inteligent (Smart Grid) 11
II.2.2 Microreţele 11
II.2.3 Situaţii de criză în sisteme electroenergetice 12
II.3 ANALIZA MANAGEMENTULUI RISCURILOR DIN INFRASTRUCTURILE CRITICE. TEHNICI DE MICŞORARE A RISCURILOR 15
II.3.1 Riscuri naturale 19
II.3.1.1 Cutremur de pământ (seism) 19
II.3.1.2 Manifestări meteorologie extreme 19
II.3.1.3 Fenomene solare cu interferenţă în magnetosfera Pământului 20
II.3.2 Riscuri antropice 21
II.3.2.1 Energia nucleară 21

III METODE ŞI MĂSURI DE PROTECŢIE PENTRU CREŞTEREA SIGURANŢEI ÎN FUNCŢIONARE SISTEMELOR ELECTROENERGETICE

III.1 INFLUENŢA FACTORILOR DE RISC ASUPRA SISTEMULUI ELECTROENERGETIC 21

III.1.1 România în sistemul european de transport al energiei electrice 22
III.1.1.1 Compania Națională de Transport al Energiei Electrice "TRANSELECTRICA", Dispecerul Energetic Național....22
III.1.1.2 Tensiunile de transport, distribuție și furnizare....22
III.1.1.3 Serviciul de sistem, sistemele de reglaj al frecvenței....22
III.1.1.4 Politica națională de eficiență energetică....23
III.1.1.5 Calitatea energiei electrice....23
III.1.1.6 Compatibilitatea electromagnetică....24
III.1.2 Factori de risc și influența acestora asupra sistemului electroenergetic național....24
III.1.2.1 Sistemul electroenergetic național din perspectiva fiabilității și a siguranței în funcționare 24
III.1.2.2 Riscuri și vulnerabilități ale sistemului electroenergetic național din perspectiva sistemelor de monitorizare, control și achiziție a datelor....25
III.2 METODE ȘI MĂSURI DE PROTECȚIE A SISTEMULUI ELECTROENERGETIC 27
III.2.1 Securitatea cibernetică din punct de vedere al siguranței naționale, în România și în cadrul partenerilor strategici....27
III.2.2 Sisteme criptografice pentru securizarea comunicațiilor....28
III.2.2.1 Cifrări prin substituție....29
III.2.2.2 Transpoziții....29
III.2.2.3 Metode criptografice de actualitate....29
III.2.2.4 Sisteme decriptate și utilizate în prezent pentru telecomunicații (text, voce, imagini, video, documente) prin intermediul Internetului....30

IV SIMULĂRI ȘI MODELĂRI ALE INFLUENȚELOR FACTORILOR DE RISC....

IV.1 ANALIZE DE MANAGEMENT....30
IV.2 COMPONENTE ALE SISTEMULUI ELECTROENERGETIC NAȚIONAL CA POSIBILE ȚINTE ALE UNUI ATACATOR....32
IV.2.1 Comutatorul de transfer automat....32
IV.2.2 Transformatorul electric....32
IV.3 STUDIU DE CAZ....32
IV.3.1.1 Ipoteza....32
IV.3.1.2 Amplasarea stației de transformare....33
IV.3.1.3 Date rezultate din modelarea incendiului la un transformator din stația de transformare 34
IV.3.1.4 Date rezultate din modelarea parametrilor electrici la transformatorul supus atacului în simularea precedentă....41
IV.3.1.5 Exemplu de criptare a unor parametri electrici vehiculați prin intermediul SCADA 46

V CONCLUZII ȘI CONTRIBUȚII ORIGINALE....

V.1 CONTRIBUȚII ORIGINALE....50
V.2 PERSPECTIVE DE DEZVOLTARE ULTERIOARĂ....51
V.3 LUCRĂRI DEZVOLTATE PE PARCURSUL CERCETĂRII DOCTORALE....51

BIBLIOGRAFIE SELECTIVĂ (DIN TOTALUL DE 260 DE LUCRĂRI):....

Cuvinte cheie: *riscuri, amenințări, vulnerabilități, reziliență, infrastructuri critice, Smart Grid, monitorizare, control, achiziții de date, criptare.*

I Sisteme electronergetice. Relaţia producător-distribuitor-consumator

I.1 Sistemul electroenergetic în România

I.1.1 Contextul temei de cercetare

Energia reprezintă motorul societății contemporane fără de care existența noastră ar regresa către un nivel similar perioadei medievale dar în același timp producerea acesteia reprezintă una dintre principalele surse de poluare și cauza principală a încălzirii globale. Accesul la energie reprezintă o prioritate pentru individ iar asigurarea acesteia în mod neîntrerupt și în parametri de calitate reprezintă în prezent o prioritate pentru orice stat, fiind nominalizată ca obiectiv strategic fundamental al țării noastre.

România dezvoltă o politică energetică bazată pe interesele sale strategice, dar în același timp, ca stat cu drepturi depline în cadrul Uniunii Europene aplică principiul solidarității și contribuie la crearea și dezvoltarea rețelelor transeuropene de interes pentru subiectul tezei, respectiv energie și telecomunicații, cuprinse în Tratatul de Funcționare al Uniunii Europene.

I.1.1.1 Actualitatea temei

Viitorul apropiat presupune implementarea standardului de telecomunicații de generația a cincea cunoscut ca International Mobile Telecommunications Standard 2020 (IMT-2020 sau 5G), sens în care Autoritatea Națională pentru Administrare și Reglementare în Comunicații a anunțat că intenționează să acorde licențele aferente până la sfârșitul anului 2019 cu posibilitatea utilizării de către operatori de la începutul anului 2020. Comisia Europeană recomandă o abordare comună a statelor membre UE referitoare la securitatea noilor rețele din perspectiva Internet of Things (IoT) și a interconectării echipamentelor din sectoare considerate infrastructuri critice, precum cel energetic iar Statele Unite ale Americii tratează cu prudență noua evoluție a rețelelor de telecomunicații din perspectiva vulnerabilităților de tip culegere de informații și sabotaj cauzate de un stat/organizație concurent/ă sau ostil/ă.

I.1.1.2 Structura generală

Lucrarea a fost structurată pe 5 capitole astfel:

Capitolul I prezintă o introducere în apariția și dezvoltarea sistemului electroenergetic național, o trecere în revistă a principalelor modalități de producere a energiei electrice, transportul acesteia și interconectările regionale aferente precum și perspectivele strategiei energetice.

În capitolul II este prezentată evoluția prognozată a sistemelor electroenergetice și sunt identificate, clasificate și analizate riscurile la adresa acestora atât din perspectivă națională cât și pe plan global.

Capitolul III prezintă sistemul electroenergetic național din perspectiva interconectării cu cele europene, parametrii de funcționare și de calitate ai acestuia,

exemple de conducere prin intermediul sistemelor de monitorizare, control și achiziție de date (SCADA), perspectiva noilor amenințări cibernetice apărute concomitent cu evoluția către sistemul electroenergetic inteligent, 5G și IoT și o evoluție a modalităților de criptare a informațiilor în vederea securizării sistemului electroenergetic digital prin criptarea parametrilor energiei electrice.

Capitolul IV prezintă un model de analiză de management pentru o infrastructură critică electroenergetică, modelări software ale consecințelor unui atac reușit asupra unei componente a sistemului electroenergetic național (variația parametrilor electrici și incendierea transformatorului) și 2 modalități de criptare.

Capitolul V prezintă concluziile lucrării, contribuțiile originale, perspectivele de dezvoltare ulterioară și lucrările științifice întocmite pe durata cercetării doctorale.

I.1.2 Repere ale producerii, transportului, distribuției și furnizării de energie electrică în România

Producătorul generează energia electrică, operatorul de transport și de sistem operează rețeaua de înaltă tensiune și echilibrează cererea cu oferta, distribuitorul gestionează rețeaua electrică de medie și joasă tensiune până la consumatorul final iar furnizorul îl reprezintă pe consumator în relația contractuală cu distribuitorul, încasează facturile aferente consumatorului și achită serviciile către producător, transportator și distribuitor.

I.1.3 Principalele facilități de producere a energiei electrice prezente în România

I.1.3.1 Termocentrale

Termenul de termocentrală sau centrală termoelectrică se referă la capacitățile de producere a energiei electrice, pe baza conversiei energiei termice obținută prin arderea unor combustibili precum: cărbune, gaze naturale, păcură, deșeuri sau biomasă.

Putem clasifica termocentralele după destinație, astfel:

- **centralele electrice de termoficare (CET)**;
- **centralele termoelectrice (CTE).**

Termocentralele moderne se construiesc având la bază un ciclu combinat abur-gaz, iar cogenerarea (în unele cazuri tri-generarea) prin folosirea căldurii reziduale de la primul proces tehnologic în care primul generator este acționat de gazele de ardere iar al doilea de energia recuperată de la aceste gaze fierbinți pentru a genera abur, a cărui presiune acționează al doilea generator. Acest proces îmbunătățește randamentul termocentralei, ce ajunge la ~85% [1].

I.1.3.2 Centrale nuclearelectrice (Atomocentrale)

Centrala nuclearelectrică reprezintă un ansamblu de instalații și construcții reunite în scopul producerii energiei electrice și/sau termice, pe baza reacției de fisiune nucleară în lanț, controlată.

Cantitatea de energie liberă conținută într-un combustibil nuclear, termenul de combustibil fiind folosit prin analogie deoarece nu arde ci este supus unui proces de fisiune în cazul producerii de energie sau fuziune în cazul celor mai puternice arme nucleare, este cu mult mai mare decât energia liberă conținută într-o masă similară de combustibil convențional, acest lucru făcând fisiunea nucleară o sursă tentantă de energie [2].

I.1.3.3 Hidrocentrale

Hidrocentrala reprezintă o centrală electrică în care energia hidraulică produsă de mișcarea apei este transformată în energie electrică, cu ajutorul unei turbine.

Turbinele reprezintă componenta principală a unei hidrocentrale. Turbinele sunt conectate printr-un ax la un generator, energia electrică produsă în acest fel fiind transmisă către un transformator ridicător de tensiune, apoi prin linii electrice de înaltă tensiune către distribuitori și apoi consumatori, prin Sistemul Energetic Național.

I.1.3.4 Energia solară

Energia solară reprezintă radiația Soarelui care ajunge la Pământ însă doar o parte din aceasta ajunge la sol în timp ce restul se reflectă în straturile superioare ale atmosferei, este absorbită de aceasta sau este reflectată din nori. Această radiație poate fi convertită în energie electrică cu ajutorul **panourilor fotovoltaice** folosite în diverse implementări sau într-o centrală de tip **energie solară concentrată** fezabilă în zone puternic însorite.

În contextul încălzirii globale cauzată de poluare se pune accent tot mai mult pe sursele de energie curată, nepoluantă. În acest sens, compania Tesla a dezvoltat țigle solare pentru reducerea costului construcției; acest design îmbină rolul de protecție împotriva intemperiilor al acoperișului cu generarea energiei electrice, oferind în același timp un aspect vizual plăcut deoarece nu se pot deosebi de țiglele clasice.

Analizând din punct de vedere economic panourile fotovoltaice, rata de recuperare a investiției (ROI – return of investment) a acestora este redusă din perspectiva costului ridicat și a randamentului scăzut, ceea ce în lipsa unor subvenții guvernamentale implică o investiție cu rentabilitate scăzută, dar susținută de stat prin certificate verzi [3].

I.1.3.5 Centrale eoliene

Energia eoliană, sau energia vântului este o formă de energie nepoluantă, folosită din antichitate de omenire pentru transport (ambarcațiuni cu propulsie asigurată de forța vântului) și agricultură (pentru măcinarea cerealelor sau pentru irigații).

Mișcarea maselor de aer se datorează încălzirii neuniforme a acestora (zona ecuatorială primește mai multă energie de la Soare față de zona polară), aerul cald este mai ușor, se ridică și începe să se deplaseze către zonele mai reci.

România are cel mai mare potențial energetic eolian din toate țările Europei continentale, estimat la 14 GW iar regiunea cu cel mai bun randament este Dobrogea, unde sunt instalate majoritatea turbinelor eoliene din țara noastră.

Conversia energiei eoliene în energie mecanică și apoi în energie electrică se realizează cu ajutorul turbinelor eoliene. Astfel, vântul antrenează palele, fixate pe arborele turbinei, în mișcarea de rotație iar energia mecanică obținută prin rotația arborelui este convertită în energie electrică de către un generator de curent electric [4].

I.2 Relația producător – distribuitor – consumator

I.2.1 Distribuția și furnizarea energiei electrice în România

Producția de energie electrică trebuie să fie în orice moment similară consumului din acea perioadă, pentru a nu destabiliza rețeaua. De aceasta se ocupă societatea **Transelectrica**, operatorul de transport și de sistem pe piața de energie electrică din Romania, cu un rol de administrator și operator al sistemul electric de transport, ce asigură inclusiv schimburile de electricitate între țările Europei Centrale și de Est, ca membru al ENTSO-E (Rețeaua Europeană a Operatorilor de Transport și Sistem pentru Energie Electrică).

Transelectrica este singurul operator care asigură serviciul de transport al energiei electrice, de conducere tehnică operațională a Sistemului Electroenergetic National precum și de administrare a pieței de energie electrică.

Rețeaua Electrică de Transport reprezintă o infrastructură critică de interes național și strategic și operează la tensiunea de linie nominală mai mare de 110 kV (înaltă tensiune). Conform datelor publicate de companie, aceasta operează o infrastructură ce constă în:

- 81 de stații electrice, astfel: o stație la tensiunea de 750 kV, 38 de stații la o tensiune de 400 kV, 42 de stații la o tensiune de 220 kV.
- 8834.4 km linii electrice aeriene (din care linii de interconexiune - 486,2 km) , astfel: 3,1 km la o tensiune de 750 kV, 4.915,2 km la o tensiune de 400 kV, 3.875,6 km la o tensiune de 220 kV, 40,4 km la o tensiune de 110 kV.
- 216 unități principale de transformare, totalizând 38058 MVA, după cum urmează: două de 1250 MVA, două de 500 MVA, 22 de 400 MVA, 31 de 250 MVA, 81 de 200 MVA, una de 100 MVA, două de 63 MVA, 9 de 40 MVA, 24 de 25 MVA, una de 20 MVA, 32 de 16 MVA și 9 de 10 MVA.

Acțiunile de mentenanță se stabilesc ținând cont de programele de investiții (retehnologizare, modernizare, dezvoltare, înlocuire) și sunt corelate cu acestea atât la nivelul stațiilor cât si al liniilor electrice.

In Rețeaua Electrică de Transport se efectuează, după caz, servicii / lucrări de mentenanță cu caracter corectiv sau preventiv.

I.2.2 România ca parte integrantă a sistemului energetic european

În cadrul Rețelei Europene a Operatorilor de Transport și Sistem pentru Energie Electrică au fost create șase grupuri regionale, în cadrul cărora se analizează și se finalizează planul european de dezvoltare a rețelei. Transelectrica face parte din grupurile regionale Continental Centru-Est și Continental Sud-Est și reprezintă un jucător important al piețelor regionale de electricitate.

Constituirea Rețelei Europene a Operatorilor de Transport și Sistem pentru Energie Electrică ca grup de cooperare al Operatorilor de Transport și de Sistem europeni are ca scop promovarea finalizării și funcționării pieței interne a energiei electrice și a comerțului transfrontalier, precum și în asigurarea unei gestionări optime, a unei exploatări coordonate și a unei evoluții tehnice sănătoase a rețelei europene de transport de energie electrică, constituit sub denumirea „Ten Year Network Development Plan" - TYNDP.

I.2.3 Perspectivele strategiei energetice

Din analiza Strategiei Energetice a României 2016 – 2030, cu perspectiva anului 2050 reiese conceptul de rețele inteligente ce permit controlul în timp real, schimburi de informație și energie sistem-consumator în dublu sens, cu optimizarea instantanee a producției și consumului de energie.

Se preconizează că interacțiunea dintre rețelele de energie electrică, internet și rețelele de comunicații se va amplifica, facilitând câștiguri de eficiență energetică și de flexibilitate. Noile tehnologii vor fi adoptate treptat, la un cost cât mai redus, cu protecția datelor cu caracter personal și cu un grad sporit de securitate în fața atacurilor cibernetice, o problemă deja din ce în ce mai prezentă, cu o gravitate a consecințelor proporțională cu adoptarea din ce în ce mai profundă a tehnologiei informației în aspectele vieții cotidiene.

Rețelele inteligente vor facilita tranziția consumatorului către rolul de **prosumator**, care injectează în rețea din producția proprie de energie electrică. Pe termen lung, acesta va avea impact asupra arhitecturii rețelelor, în special atunci când dispune și de o capacitate de stocare a energiei electrice, pentru a limita interacțiunea cu rețeaua. Urmează să scadă astfel și numărul gospodăriilor fără acces la rețelele de energie, inclusiv prin adoptarea de microrețele și soluții autonome ce vor deveni mai accesibile economic, scutind distribuitorul de investiții nerentabile, executate exclusiv din perspectiva accesului la energie electrică pentru toți consumatorii ca obiectiv strategic al politicii energetice.

I.2.4 Analize și previziuni ale Autorității Naționale de Reglementare în domeniul Energiei

Autoritatea Națională de Reglementare în domeniul Energiei (ANRE) reprezintă autoritatea administrativă autonomă, cu personalitate juridică, sub control parlamentar, finanțată integral din venituri proprii, independentă decizional, organizatoric și funcțional, având ca obiect de activitate elaborarea, aprobarea și monitorizarea aplicării reglementărilor obligatorii la nivel național și

necesare funcționării sectorului și pieței energiei electrice, termice și a gazelor naturale în condiții de eficiență, concurență, transparență și protecție a consumatorilor.

Conform datelor ANRE, furnizorii de energie electrică sunt următorii:

- Electrica Furnizare;
- ENEL Energie;
- CEZ Vânzare transformat în Distribuție Oltenia din 01.2017;
- E.ON Energie Rumânia, devenit din 01.01.2017 Delgaz Grid.

II Identificarea parametrilor infrastructurilor critice din sistemele electroenergetice și managementul riscurilor

II.1 Infrastructurile critice asociate rețelelor electroenergetice și identificarea parametrilor acestora

Există o puternică legătură între sistemul electroenergetic, mediul înconjurător, riscurile de orice tip și managementul lor. Continua criză energetică și efectele sistemelor electroenergetice asupra mediului au condus la identificarea și analiza factorilor de risc, ceea ce a constituit și va constitui subiectul pe care numeroși cercetători din întreaga lume îl abordează în lucrările lor.

Când ne referim la managementul riscului vorbim despre aplicarea sistematică a politicilor, procedurilor și practicilor de management la activitățile de **comunicare, de consultare, de stabilire a contextului, precum și la identificarea, analiza, evaluarea, tratarea, monitorizarea și revizuirea riscului.**

Revenind la definiția riscului ca fiind o funcție de probabilitate și gravitate, coroborat cu dependența tot mai mare a populației, industriei și mai ales a majorității infrastructurilor critice de accesul continuu la energie electrică de calitate, riscul unui colaps al sistemului electroenergetic are o probabilitate mare să antreneze disfuncționalități în lanț în celelalte infrastructuri critice, situație inacceptabilă din punct de vedere al consecințelor.

Prin securitate fizică se înțelege siguranța sistemului electroenergetic față de atacuri fizice desfășurate de indivizi sau organizații, cu intenția de a distruge puncte cheie ale acestuia, a-i întrerupe funcționarea sau a sustrage părți valoroase (de exemplu conductorii din cupru); securitatea cibernetică se referă la protejarea sistemului electroenergetic față de amenințările privind furtul/distrugerea/manipularea datelor companiei sau a bazelor de date privind informațiile clienților sau manipularea senzorilor și echipamentelor cu scopul întreruperii activității. Deși sunt diferite, cele două domenii se interconectează, vulnerabilitățile fiind complexe, iar un atac având ca scop disfuncționalitatea sistemului electroenergetic va fi derulat pe ambele planuri simultan (de exemplu atacurile din Ucraina dezvoltate în cuprinsul lucrării).

În ceea ce privește evoluția tehnologică din punct de vedere al rețelei electroenergetice, aceasta îmbunătățește fiabilitatea dar adaugă simultan

vulnerabilități în cazurile unde se introduc (noi) modalități de acces la distanță sau acolo unde redundanța este redusă.

Printre avantajele evoluției tehnologice regăsim posibilitatea simulării funcționării echipamentelor și implicit localizarea și îndepărtarea erorilor din faza de proiectare precum și automatizarea îmbunătățită ce reduce posibilitatea apariției erorilor umane.

Abordarea protecției infrastructurilor critice în cadrul NATO este diferită față de cea a Uniunii Europene, fiind privită din perspectiva situațiilor de urgență (protecție civile), motiv pentru care nu sunt stabilite reguli și norme comune în domeniu.

Comparativ, directiva Consiliului UE nr.114/2008/CE definește infrastructura critică națională ca „un sistem sau o componentă a acestuia, aflat pe teritoriul național, care este esențial pentru menținerea funcțiilor vitale ale societății, a sănătății, siguranței, securității, bunăstării sociale ori economice a persoanelor și a cărui perturbare sau distrugere ar avea un impact semnificativ la nivel național ca urmare a incapacității de a menține respectivele funcții".

Ordinul 1178/2011 al Ministrului economiei, comerțului și mediului de afaceri pentru stabilirea criteriilor sectoriale și a pragurilor critice aferente sectorului ICN/E — infrastructură critică națională/europeană — „Energetic" identifică infrastructurile critice din sistemul electroenergetic național.

Directiva Consiliului Uniunii Europene nr. 114/2008 privind identificarea și desemnarea infrastructurilor critice europene și evaluarea necesității de îmbunătățire a protecției acestora reglementează activitățile pe această direcție în sensul unei abordări care identifică și acoperă toate riscurile, dar acordă prioritate amenințărilor de natură teroristă. Conform acesteia, calamitățile provocate de om, cele naturale, precum și amenințările tehnologice ar trebui luate în considerare în procesul de protecție a infrastructurilor critice, dar se acordă prioritate luptei împotriva terorismului.

Conceptul de reziliență a evoluat în mod considerabil de la definiția fundamentală a lui Holling (Holling, 1973) ca „o măsură a capacității unui sistem de a continua să funcționeze făcând față modificărilor variabilelor de stare, de conducere, precum și ale parametrilor".

Caracteristicile cheie ale rezilienței infrastructurilor critice, concepute inițial de către Stephen Flynn și definite ulterior (2010) de NIAC sunt următoarele:

- **Robustețea** – capacitatea de a menține operațiunile și funcțiile critice în cazul unei crize: reflectată în construcția fizică și proiectarea infrastructurii (clădiri de birouri, poduri, baraje, diguri) sau în redundanța și capacitatea de substituție a sistemelor (rețele de transport, de alimentare cu energie electrică și de comunicații);
- Capacitatea de **reacție** – abilitatea de a se pregăti corespunzător, de a răspunde și de a gestiona activitățile în cazul apariției unei crize sau perturbări: presupune identificarea modului de evoluție a crizei sau perturbării, planificarea continuității afacerii, managementului lanțului

de aprovizionare, prioritatea acțiunilor pentru controlul și reducerea pagubelor;

- Capacitatea de **recuperare rapidă** – abilitatea de a reveni la și / sau reconstitui operațiunile normale cât mai repede și mai eficient posibil, după o întrerupere. Aceasta include planuri de urgență atent elaborate, operațiuni de urgență corespunzătoare, precum și modalitățile de a avea resursele necesare la locul potrivit;
- **Adaptabilitatea** – modul de absorbție a noilor lecții care pot fi extrase dintr-o catastrofă. Implică revizuirea planurilor, proceduri de modificare și introducerea de noi instrumente și tehnologii necesare îmbunătățirii robusteții, capacității de reacție și a celei de recuperare rapidă înainte de următoarea criză [5].

Energia electrică face parte din tipurile de energie cruciale nu doar pentru buna funcționare, ci chiar pentru existența societății contemporane; sistemul electroenergetic este supus unor riscuri variate (cu predominanță cauze naturale, accidente sau acțiuni săvârșite cu rea intenție) a căror apariție poate duce la perturbarea grava a operării sistemului.

II.2 Modelarea infrastructurilor critice asociate rețelelor electroenergetice

II.2.1 Sistemul electroenergetic inteligent (Smart Grid)

Institutul Național de Standardizare și Tehnologii (NIST) a propus un model de **sistem electroenergetic inteligent(**inteligență artificială, IoT, comunicații**)**, adaptat evoluțiilor din sectoarele tehnologia informației și telecomunicații, distribuit în componenta de sistem și cea de rețea.

Schimbările din spectrul amenințărilor asupra sistemului electroenergetic precum și evoluția componentelor acestuia demonstrează importanța implementării măsurilor de fiabilitate, siguranță în funcționare și interoperabilitate încă din stadiul de proiectare [6].

II.2.2 Microrețele

Sistemele electroenergetice contemporane au implementat parțial și greoi noile tehnologii din electronică, automatizări, tehnologia informațiilor și telecomunicații. Este prezentată evoluția sistemelor electroenergetice în timp, împreună cu tendința de evoluție contemporană către rețeaua electroenergetică inteligentă (Smart Grid), bazată pe descentralizare și schimb bidirecțional de energie și informație.

Evoluția de la sistemul electroenergetic tradițional bazat pe un număr relativ redus de centrale de mare putere, către descentralizare și soluții Smart Grid îmbunătățește reziliența și renunță la necesitatea acelor centrale care funcționează doar pe timpul zilei pentru a susține vârfurile de consum prin descentralizarea unei părți din generarea la nivel național către consumatorii finali deveniți **prosumatori** (ex: soluții solare și eoliene coroborate cu stocare în baterii).

Caracteristica de bază a unei microrețele o reprezintă posibilitatea de a funcționa în regim izolat atunci când în sistemul electroenergetic național apare o defecțiune dar și de a-l proteja pe acesta în cazul improbabil în care a o defecțiune a apărut în interiorul microrețelei, fără să îi permită acesteia să se propage în sistemul electroenergetic național și să afecteze alți utilizatori în cascadă.

Suplimentar față de protecția față defecte ce pot cauza pene de energie electrică, microrețelele preiau din soluțiile de generare și stocare proprii (panouri fotovoltaice, stocare în baterii) vârfurile de consum din timpul zilei, iar prin sistemele bidirecționale de telecomunicații si management al energiei, utilizatorii plătesc pentru cât consumă și pot lua cele mai bune decizii în funcție de prețul dictat de încărcarea sistemului [7].

II.2.3 Situații de criză în sisteme electroenergetice

Poluarea și încălzirea globală cauzează din ce în ce mai multe îmbolnăviri iar manifestările extreme ale vremii cresc în gravitate și rată de apariție, motiv pentru care considerentele legate de protecția mediului înconjurător sunt din ce în ce mai prezente în viața noastră (conștientizare) și în reglementările autorităților. Transportul a depășit zona conceptelor electrice, producătorii au înțeles că viitorul apropiat al mobilității este electric și au în portofolii autoturisme PHEV(hibrid ce combină motorizare termică, electrică, soluții de stocare a energiei și de regenerare a energiei la frânare și desigur posibilitatea de alimentare a bateriilor cu energie electrică de la priză) sau integral electrice. Totodată autoritățile impozitează din ce în ce mai mult automobilele cu ardere internă (din perspectiva poluării) și oferă subvenții pentru achiziționarea celor „verzi" – funcționarea autoturismelor electrice nu implică emisii poluante.

Sunt necesare modelări ale interdependențelor infrastructurilor critice la nivel național și la nivelul Uniunii Europene precum și conștientizarea și clasificarea vulnerabilităților, riscurilor și amenințărilor pentru a preveni apariția unor situații de criză, precum:

- la scurt timp după cutremurul de pământ ce a devastat România în 04.03.1977, o pană de energie electrică datorată unei erori umane s-a propagat în sistemul electroenergetic național, având consecințe economice importante;
- în anul 2005, vremea extremă a sistat pentru 5 zile energia electrică în stat din Vestul continentului;
- în 2006 s-a produs un efect în cascadă, de pe teritoriul Germaniei spre alte unsprezece state europene, afectând 15000000 persoane timp de 3 zile;
- Seismul din 2010 și uraganul din 2016 au afectat grav Haiti inclusiv în ceea ce privește sistemul electroenergetic național;
- în iunie 2019, o pană de energie electrică ce a afectat ~48.000.000 de oameni în America de Sud (Argentina, Uruguay și parțial Paraguay) datorită fenomenelor meteo extreme;

- pe 14 august 2003 a avut loc cea mai însemnată pană de electricitate care a afectat America de Nord, cu efect asupra 50.000.000 de persoane [8].

Sabotajul, terorismul sau alte activități criminale îndreptate către rețelele electroenergetice pot produce rezultate de o gravitate cel puțin similară penei nord-americane, dacă nu vor fi implementate măsuri de protecție corespunzătoare.

Prezentăm în continuare alte amenințări cibernetice, care deși la prima vedere par mai puțin grave, nu sunt vizibile sau tratate uzual în mass-media au capacitatea de a fi cel puțin la fel de periculoase ca un atentat terorist sau alt fel de atac fizic.

Analizând acțiunile de sabotaj, putem descrie evenimentele ce au afectat **Ucraina** în 2015 și 2016, care a fost atacată cibernetic cu ceea ce entitățile de profil denumesc APT (advanced persistent threat) – un atac cibernetic complex, executat de obicei cu resurse disponibile la nivel statal, prin care atacatorul urmărește să se infiltreze nedetectat în sistemele cibernetice țintite, să preia controlul, să sustragă date de interes, să afle modul de funcționare și vulnerabilitățile ce pot fi exploatate la momentul oportun și să creeze alte porți de acces în eventualitatea în care atacul este detectat înainte ca atacatorii să își atingă total obiectivele.

O altă țară ce se confruntă recent cu amenințări la adresa stabilității sistemului electroenergetic național este **Venezuela**.

Sintagma **malware** folosită internațional pentru amenințările cibernetice provine din "malicious software" (soft programat intenționat pentru infiltrarea într-un sistem informatic pentru deteriorarea sistemului și/sau furtul datelor);

Stuxnet este considerat prima armă cibernetică, a fost descoperit în 2010 de soluția antivirus Kaspersky și se speculează că a fost dezvoltat timp de mai mulți ani de către serviciile de informații din SUA și Israel cu scopul de a îngreuna avansarea programului nuclear iranian.

Acesta a acționat prin modificarea parametrilor de funcționare la automatizarea produsă de Siemens și folosită de centrifugele pentru îmbogățirea uraniului, cauzând distrugerea fizică a acestora. Arhitectura sa nu este specifică doar acestui atac ci poate fi folosit împotriva oricăror sisteme de control industrial sau sisteme SCADA, fiind un pericol inclusiv pentru orice infrastructuri critice țintite, inclusiv din România.

Cel mai recent atac grav asupra infrastructurii critice electroenergetice s-a produs la sfârșitul anului 2017 cu ajutorul malwareul intitulat "**Triton**" - dezvoltat cu scopul de a ataca sistemele de control industriale. Acesta acționează asupra sistemelor autonome de control fabricate de Schneider Electric, care monitorizează independent starea sistemelor critice și ia măsuri automat în cazul în care detectează o situație periculoasă [9].

Malwareul cu cea mai rapidă rată de infectare și cele mai mari pagube (~ 10.000.000.000$) este asociat cu entități statale din Rusia, este intitulat **NotPetya**.

Infractorii cibernetici au mers pe obținerea de foloase materiale prin accesarea și criptarea informațiilor, denumite generic **ransomware** (cod malițios ce criptează datele utilizatorului și cere o sumă, de obicei în criptomonedă pentru a evita urmărirea banilor de autorități, în schimbul codului de descifrare), cel mai elocvent exemplu pentru anul 2017 fiind intitulat **WannaCry** iar pentru 2018 **GandCrab** în mai multe versiuni, pentru toate fiind dezvoltate gratuit soluții de către Bitdefender.

Multe sisteme de control industriale aflate în uz sunt proiectate în anii 1960-1990, perioadă în care nu a fost luată în calcul posibilitatea ca cineva să încerce un atac asupra acestora. Pentru că nu au implementate protocoale de securitate (autentificare, criptare, etc.) acestea sunt considerate nesigure.

Orice sistem electroenergetic este imposibil de protejat împotriva tuturor amenințărilor fizice, dată fiind dimensiunea acestuia precum și a faptului că anumite obiective sunt amplasate în zone izolate sau greu accesibile, cel puțin în anumite perioade ale anului. Astfel, ca și în cazul combaterii altor forme de criminalitate, *cea mai eficientă metodă de protecție o reprezintă colectarea **proactivă** a informațiilor de către structurile de resort, coroborată cu acțiunea forțelor de ordine privind prevenirea, descurajarea și anihilarea acțiunilor ostile asupra sistemului electroenergetic înainte ca acestea să fie puse efectiv în aplicare.*

Un scenariu violent de sabotaj deja a avut loc în Statele Unite ale Americii în 16 aprilie 2013 iar atacul, numit generic "atacul lunetist Metcalf" nu și-a atins scopul iar subiectul nu a fost tratat cu seriozitate de mass-media, acesta este de o **gravitate deosebită**. Atacatorii au tăiat în prealabil fibra optică pentru a face imposibile telecomunicațiile între stația de transformare Metcalf a companiei de gaz și electricitate "Pacific", situată în Coyote - California și autorități. Ulterior, aceștia au deschis focul asupra celor 17 transformatoare din cadrul stației, care au pierdut uleiul de răcire, supraîncălzindu-se [10].

Precedentul creat indică ușurința cu care poate fi destabilizat un domeniu vital societății moderne - infrastructura critică electroenergetică. Atacatorii nu ar fi reușit o asemenea eficiență fără informații din interior, așadar atacul lunetist Metcalf nu poate fi considerat un simplu atac fizic, ci unul combinat în care atacatorii au exploatat punctele vulnerabile ale sistemului electroenergetic american, cu ajutor din interior (spionaj industrial) sau accesând ilegal sistemul cibernetic al companiei de electricitate (atac cibernetic).

Țara noastră s-a confruntat cu o defecțiune a unui transformator de mare putere din cauza unei defecțiuni tehnice care a dus la un incendiu și la pierderea echipamentului. În zilele noastre, un astfel de scenariu poate fi implementat de către un stat sau o organizație ostilă, dacă nu sunt implementate și actualizate constant măsuri adecvate de protecție cibernetică.

În documentele evenimentului preluate din arhiva RENEL, referitoare la evenimentul produs în stația 400/110/20 kV Smârdan din județul Galați în data de

17.07.1997, se analizează explozia urmată de incendiu la transformatorul nr. 2 (250 mVA, 400/110 kV).

Față de locul și natura defectului, protecțiile au funcționat corect și au izolat rapid defectul iar instalația fixă de stingere a incendiilor a pornit și funcționat corespunzător. Din ancheta evenimentului reiese cauza evenimentului: cedarea izolației trecerii electroizolante – faza R 110 kV deasupra transformatorului de curent și amorsarea arcului electric între fază și cuvă (oala suport a fazei R). Urmare a defectului intern s-a produs o degajare puternică de gaze care a creat o suprapresiune în cuvă ce a avut ca efect dislocarea trecerilor electroizolante 400 kV fazele R și S cu tot cu oalele suport, forfecarea șuruburilor de prindere a acestora și declanșarea incendiului.

II.3 Analiza managementului riscurilor din infrastructurile critice. Tehnici de micșorare a riscurilor

Putem clasifica riscurile cu probabilitate de apariție în România, astfel:

a) naturale:

- cutremure;
- alunecări de teren;
- vreme severă (temperaturi extreme, inundații, incendii cauzate de secetă, furtuni însoțite de descărcări electrice, căderi masive de zăpadă, vânt puternic, uragan, tornadă, avalanșe);
- interferențe în câmpul magnetic al Pământului (furtuni geomagnetice sau ejecții de masă coronală);

b) umane (antropice):

- accidente de muncă sau erori umane;
- uzură tehnologică;
- război (armă cu puls electromagnetic sau armă nucleară);
- acțiuni săvârșite cu rea intenție (atentat terorist, sabotaj).

Conform prevederilor HGR 718/2011 privind aprobarea Strategiei naționale privind protecția infrastructurilor critice, se definesc 7 categorii de vulnerabilități iar conform deciziei primului-ministru al României nr. 166/2013, prin Normele metodologice pentru realizarea, echivalarea sau revizuirea planurilor de securitate ale proprietarilor/operatorilor/administratorilor de infrastructură critică națională/europeană, se identifică 7 categorii de amenințări, însă acestea nu au un caracter general valabil ci se adaptează la specificul infrastructurii critice, analizând elementele relevante ale acesteia, detaliile tehnice ale echipamentelor, utilizatorii autorizați să le opereze direct sau de la distanță, identificând punctele critice ale sistemului.

Simultan cu dezvoltarea sistemelor de generare a energiei electrice pe baza surselor regenerabile, sisteme identice replicate la ordinul mii - sute de mii, operate prin dispozitive inteligente de comunicații, pot fi afectate de o singură

amenințare. Actualizările de securitate reprezintă o componentă importantă a securității cibernetice, dar se aplică cu întârziere și dificultate în sistemul electroenergetic datorită diversității echipamentelor.

Din punct de vedere al vulnerabilităților cauzate de operarea de la distanță a activelor prin dispozitive inteligente de comunicații, atacul din decembrie 2015 asupra sistemului electroenergetic ucrainian s-a axat pe obținerea datelor de acces în programele SCADA, apoi a urmat preluarea controlului operațiilor de la distanță, dereglarea sistemului și instalarea de malware pentru a îngreuna revenirea la starea de funcționare normală.

Deficiențele constatate în urma acestui atac sunt:

- Conștientizarea fenomenului phising și instruirea personalului în scopul detectării acestuia, scanarea și filtrarea e-mail-urilor, protejarea datelor de acces la stațiile de lucru;
- Conexiunile trebuie să fie configurate și controlate corespunzător;
- Comunicațiile se execută doar prin protocoale criptate;
- Apelurile din call-center trebuie filtrate în funcție de sursă;
- Trebuie prevăzută posibilitatea fizică de a opri managementul activelor de la distanță precum și posibilitatea de a instala actualizări de la distanță;
- Implementarea de soluții tehnice care să nu permită întreruperea alimentării cu energie electrică;
- Existența unui canal secundar de comunicații.

Evaluarea riscurilor și vulnerabilităților precizate anterior se realizează cu ajutorul matricei riscurilor.

Securitatea și reziliența infrastructurii critice din domeniul electroenergetic reprezintă o prioritate atât pentru deținătorii și operatorii acestora precum și pentru autorități.

Pentru a ajuta organizațiile care lucrează cu sisteme industriale de control sa identifice potențiale vulnerabilități, experții companiei specializată în produse antivirus “Kaspersky Lab” au realizat o analiză bazată pe informații din surse publice și de tip Open Source Intelligence, pentru anul 2015.

Pentru a reduce vulnerabilitățile unui atac cibernetic, sistemele industriale de control trebuie să funcționeze într-un mediu fizic izolat. În analiza din domeniul industrial menționată anterior au fost identificate 13.698 de servere prin care sisteme industriale de control sunt conectate la Internet. Acestea aparțin unor organizații mari din domenii variate (energetic, aerospațial, transporturi, petrol și gaze naturale, industria chimică, auto, alimentară și de băuturi, etc.), operatori de infrastructuri critice, instituții guvernamentale, financiare si medicale iar în 91,1% din aceste cazuri au fost identificate vulnerabilități care pot fi exploatate de la distanță. Cele mai vulnerabile componente industriale de control au fost interfețele om-mașină, dispozitivele electrice și sistemele SCADA.

În anul 2013, în Statele Unite ale Americii, doi cercetători au identificat și documentat vulnerabilități cibernetice, în cazul a 20 de operatori de infrastructuri critice, care, dacă ar fi fost exploatate, ar fi permis sistarea alimentării cu energie electrică prin modificarea parametrilor sau oprirea echipamentelor ce asigură distribuția energiei electrice.

În articolul "Vulnerabilitățile rețelei electroenergetice îndeamnă companiile de utilități să colaboreze", se prezintă situații din Statele Unite ale Americii precum: investigația publicației USA Today din care reies 362 de atacuri asupra rețelei electroenergetice între anii 2011 – 2014, majoritatea fiind clasate cu autor necunoscut sau studiul Comisiei Federale de Reglementare în Energie (FERC) din martie 2014 care atrage atenția asupra faptului că un atac reușit asupra a cel mult 10 stații de transformare din cele 55.000 răspândite pe teritoriul american ar cauza o pană de proporții.

Conform celor prezentate anterior, există deja numeroase cazuri de atacuri reușite, cum ar fi explozia de la un combinat siderurgic din Germania; atacul cibernetic a avut succes fiindcă a păcălit angajații să deschidă e-mailuri virusate cu ajutorul cărora atacatorii au furat datele de intrare în sistem, au modificat parametri proceselor tehnologice, cauzând explozia unui furnal, conform datelor Biroului Federal pentru Securitatea Informațiilor din Germania, citat de BBC.

Accesarea sistemelor industriale de control prin intermediul Internetului prezintă avantaje dar ridica numeroase probleme de securitate, oferind părților interesate (infractori din domeniul cibernetic, organizații statale sau teroriste, etc.) posibilitatea să controleze de la distanță componente vitale, ceea ce reprezintă din punctul nostru de vedere un risc situat în domeniul inacceptabil datorită probabilității mare de apariție și a consecințelor grave pentru întreaga infrastructură critică.

Utilizarea deep și dark web (Internetul ascuns), soluțiile de comunicare criptată la îndemâna oricui și metodele de plată în criptomonede aduc cu ușurință la îndemâna persoanelor/organizațiilor interesate aceste organizații de criminalitate informatică și în același timp le fac foarte dificil de identificat și adus să răspundă în fața legii, inclusiv din perspectiva unor organizații globale, cu membri care nu se cunosc în viața reală și locuiesc în țări diferite, ceea ce implică un efort major pentru instituțiile de aplicare a legii.

Specialiștii în securitate cibernetică ce dezvoltă soluția antivirus Kaspersky prognozează, în ceea ce privește securitatea cibernetică în domeniul industrial din care face parte și sistemul electroenergetic din România, următoarele tendințe:

- **Creșterea infecțiilor malware generale și accidentale:** infractorii cibernetici nu au descoperit încă scheme simple și fiabile pentru a genera bani de la atacurile asupra sistemelor informatice industriale, tendința fiind atacarea rețelelor corporative în timp ce sistemele informatice industriale sunt

infectate în majoritatea cazurilor neintenționat, ca o consecință a unei culturi de securitate cibernetică slabă, nu cu malware țintit.

- **Risc crescut de atacuri direcționate care solicită răscumpărarea**: ransomware precum WannaCry au demonstrat că tehnologiile operaționale (OT) sunt mai vulnerabile la atacuri decât sistemele informatice și sunt adesea expuse accesului prin Internet, după cum am citat anterior din studiul Kaspersky.
- **Incidente de cyber-spionaj industrial:** furtul datelor din sistemele informatice industriale în scopul pregătirii și implementării atacurilor (ransomware pentru a bloca activitatea companiei până la obținerea de foloase materiale, sau malware pentru a-i întrerupe activitatea).
- **O nouă ramură a criminalității s-a axat pe dezvoltarea serviciilor de atac și a instrumentelor de hacking:** se conturează o creștere a cererii pe piața neagră pentru exploatarea vulnerabilităților sistemelor informatice industriale așadar tendința în viitor este spre campanii de atac direcționate.
- **Noi tipuri de viruși:** urmând arhitectura Stuxnet, noi forme de malware sunt dezvoltate și folosite pentru a viza rețelele și bunurile industriale; acestea vor fi dezvoltate cu caracteristici precum capacitatea de a rămâne inactiv în rețeaua informatică a țintei pentru a evita detectarea.
- **Infractorii cibernetici vor profita de analizele asupra vulnerabilităților sistemelor informatice industriale de control publicate de furnizorii de securitate**: specialiștii din domeniul securității cibernetice au identificat și publicat date despre diverse atacuri asupra infrastructurilor industriale privind modul de operarea al acestora și vulnerabilitățile exploatate. Această abordare permite o mai bună înțelegere și conștientizare a fenomenului de către cei ce ar putea fi vizați (inclusiv operatorii de infrastructuri critice din domeniul electroenergetic) însă ca dezavantaj infractorii cibernetici au acces și înțeleg mai bine vulnerabilitățile industriale și pot dezvolta viruși specifici, greu sau imposibil de detectat de soluțiile se securitate din prezent.
- **Reglementări în materie de securitate cibernetică** - reprezintă primul pas spre creșterea protecției și conștientizării amenințărilor, vulnerabilităților și a modului de protejare împotriva acestora.
- **Asigurări industriale:** asigurarea împotriva riscurilor cibernetice devine parte integrantă a gestionării riscurilor pentru întreprinderile industriale; anterior, riscul unui incident de securitate cibernetică era exclus din contractele de asigurare, la fel ca riscul unui atac terorist. Totuși, pentru a fi despăgubiți, operatorii industriali trebuie să îndeplinească anumite cerințe, ceea ce sporește gradul de conștientizare în rândul acestora iar măsurile întreprinse cu siguranță vor spori siguranța și reziliența.

Un sistem diversificat se destabilizează global mai dificil dar un sistem modular are avantajul flexibilității iar în cazul unor probleme în puncte cheie (de exemplu transformatoare de mare putere) se pot înlocui rapid părțile afectate, la costuri mai mici, deoarece compania își permite să mențină un stoc de rezervă,

nefiind implicate costuri logistice mari datorită diversității pieselor și producătorilor.

II.3.1 Riscuri naturale

II.3.1.1 Cutremur de pământ (seism)

În categoria fenomenelor naturale distructive regăsim seismul, care la magnitudini medii întrerupe utilitățile publice iar la cele mari provoacă distrugeri ample în arealul în care se manifestă, printre acestea regăsindu-se și pagube în infrastructura electroenergetică.

În România, ca bază legală regăsim HGR nr. 372/2004 pentru aprobarea Programului Național de Management al Riscului Seismic iar cercetarea seismologică intră în atribuțiile Institutului National de Cercetare-Dezvoltare pentru Fizica Pământului. Instituția definește cutremurele ca fenomene naturale cauzate de eliberarea de energie în interiorul Pământului, în urma fracturării rocilor supuse tensiunilor acumulate de acestea iar suprafața de-a lungul căreia se produce ruptura și produce deplasarea se numește *plan de falie*.

II.3.1.2 Manifestări meteorologie extreme

În această secțiune sunt analizate amenințările naturale din perspectivă globală, europeană și națională.

România se situează pe harta riscurilor în domeniul mijlociu, pe poziția 102 din 172 de state, indicat un coeficient de risc de 5,4618 [11].

Conform articolului referitor la sistemul electroenergetic italian *Analysis and visualization of natural threats against the security of electricity transmission system*, datelor meteorologice preluate de la serviciul global de meteorologie AccuWeather **inundațiile** reprezintă riscul natural cu cea mai mare probabilitate de apariție, care produce daune maximale raportate la produsul intern brut.

Ultimul raport al Organizației Meteorologice Mondiale atrage atenția asupra creșterii impactului socioeconomic al încălzirii globale, aflată în creștere datorită gazelor cu efect de seră.

Din punct de vedere al siguranței sistemelor electroenergetice, schimbările climatice cauzate de încălzirea globală au condus la manifestarea de fenomene meteo extreme cu o rată de apariție și o gravitate accelerate, care au produs efecte pe fiecare continent.

Astfel, doar în 2018 aproximativ 62.000.000 persoane au fost afectate de amenințări asociate fenomenelor meteorologice extreme sau ca urmare a modificărilor climatice.

Deși un eveniment similar s-a petrecut de curând (Laos), cel mai grav dezastru natural pe care am putut să îl identific în categoria colapsului unui baraj s-a petrecut în 1975 în China. Ca răspuns la inundațiile grave și pentru a asigura generarea de energie electrică în anii cincizeci, China a construit Barajul Banqiao (finalizat în 1952) în bazinul râului Huai din provincia Henan care a cedat în urma unor inundații catastrofale și a antrenat ruperea a alte 62 de baraje din aval și peste

10.000.000 de oameni din întreaga regiune au fost grav afectați, 26.000 de persoane au murit din cauza inundațiilor iar alte 145.000 au murit în urma unor epidemii sau de foamete, aproximativ 6.000.000 de clădiri s-au prăbușit iar inundațiile au afectat peste 1.000.000 de hectare, însă regimul conservator a mușamalizat tragedia, făcând dificilă obținerea datelor conforme cu realitatea.

În prezent în România conform Registrului Român al Marilor Baraje sunt înregistrate 246 de asemenea structuri, cu înălțimi de la 5 la 168 m și cu volum al lacului de acumulare de la 100.000 m^3 la 2.400.000.000 m^3.

Analizând fenomenele meteorologice extreme ale anului curent, o furtună a lovit peninsula Halkidiki din Grecia în 11.07.2019 și a provocat distrugeri extinse la clădiri, ambarcațiuni și infrastructură, iar mai mulți oameni și-au pierdut viața, între care și 2 cetățeni români prinși sub o clădire distrusă de vântul puternic.

În contextul acestor manifestări pe continent, nici România nu a fost ocolită de furtuni; astfel, din comunicatele de presă ale Administrației Naționale de Meteorologie și a Inspectoratului General pentru Situații de Urgență, în anul curent vântul de intensitate ridicată asociat furtunilor a produs pagube (acoperișuri, autoturisme, etc.) și printre acestea regăsim inclusiv sistarea alimentării cu energie electrică prin ruperea liniilor electrice.

Clasificările fenomenelor meteorologice distructive cauzate de vânt se determină empiric prin scara Beaufort a vitezei vântului elaborată în 1805 din perspectiva efectelor acestuia asupra mării și adaptată ulterior și la efectele produse pe sol, conform datelor Royal Meteorological Society. Aceasta are 12 poziții, dintre care cele mai importante se clasifică:

- 9 – vânt puternic;
- 10 – furtună;
- 11 – furtună puternică;
- 12 – uragan.

Politehnica din Torino, cu sprijinul Comisiei Europene și al societății de distribuție a energiei electrice "Terna" din Italia, a realizat un model geo-referențial bazat pe riscurile natural asupra rețelei de distribuție a energiei electrice.

Modelul anterior coroborat cu cel din citare au potențialul de a fi folosite cumulat pentru îmbunătățirea rezilienței prin analiza riscurilor, planificarea, managementul, monitorizarea și consolidarea sistemelor de distribuție a energiei electrice. Analiza spațială este foarte utilă pentru formularea scenariilor, determinarea necesarului optim de generare, studierea impactului asupra mediului înconjurător și gestionarea activelor instalației.

II.3.1.3 Fenomene solare cu interferență în magnetosfera Pământului

Curenții geomagnetici induși sunt reprezentarea la nivelul solului a consecințelor modificărilor în magnetosfera și ionosfera Pământului din cauza exploziilor solare sau a exploziilor nucleare de mare putere și detonate în straturile superioare ale atmosferei [12].

Curentul geomagnetic indus ce curge prin înfășurările unui transformator electric produce o magnetizare suplimentară care, în timpul jumătății de ciclu când magnetizarea curentului alternativ este în același sens, poate conduce la saturarea miezului feromagnetic al transformatorului și cauzează încălzirea înfășurărilor acestora, cu potențial distructiv. Acest fenomen conduce la o formă a sinusoidei cu armonice abrupte, conduce la pierderi prin transmiterea ineficientă și probabilitatea mărită de declanșare eronată a sistemelor automate de protecție precum situația din Canada – 1989 când o întrerupere în cascadă cauzată de o furtună solară a sistat alimentarea cu energie electrică pentru 6.000.000 de persoane.

II.3.2 Riscuri antropice

II.3.2.1 Energia nucleară

Accidentele nucleare au fost evenimente rare, însă au marcat puternic omenirea. Scara Internațională a Evenimentelor Nucleare și Radiologice a fost introdusă în anul 1990 de către Agenția Internațională a Energiei Atomice cu scopul de a comunica prompt informațiile relevante în cea ce privește siguranța în cazul accidentelor nucleare [13].

În urma revenirii în atenția publică a accidentului nuclear de la Cernobîl, conducerea Nuclearelectrica a anunțat că reactoarele 1 și 2 ale centralei nuclearelectrice Cernavodă au fost construite și sunt operate respectând principii de protecție pe adâncime, au anvelopă, iar timpul de oprire a unui reactor în caz de urgență este de maxim 2 secunde, prin intermediul a 4 sisteme de protecție dintre care 2 independente de sistemul central; această cultură de securitate a condus la un rating bun în urma auditării externe.

Dat fiind faptul că reactoarele 1 și 2 ale centralei nuclearelectrice Cernavodă produc ~15-20% din consumul țării iar reactoarele 3 și 4 sunt construite parțial, apreciez oportunitatea continuării demersului de finalizare a acestor reactoare atât din perspectiva securității energetice a țării cât și din cea de exportator de energie (din păcate, în urma impredictibilității legislative, consecințele Ordonanței de Urgență nr. 114/2018 a condus, conform datelor Institutului Național de Statistică, la creșterea importurilor de energie electrica cu 78,5% în primul trimestru al anului 2019 față de perioada similară a anului 2018); cât despre alegerea partenerilor, instituțiile abilitate ale statului judecă oportunitatea nu doar din perspectivă financiară cât și din perspectivă geopolitică și strategică.

III Metode şi măsuri de protecţie pentru creşterea siguranţei în funcţionare sistemelor electroenergetice

III.1 Influența factorilor de risc asupra sistemului electroenergetic

III.1.1 România în sistemul european de transport al energiei electrice

III.1.1.1 Compania Națională de Transport al Energiei Electrice "TRANSELECTRICA", Dispecerul Energetic Național

Autoritatea Națională de Reglementare în domeniul Energiei(ANRE) a fost creată în anul 1998 și este o autoritate administrativă autonomă având ca obiect de activitate elaborarea, aprobarea și monitorizarea aplicării reglementărilor obligatorii la nivel național, necesare funcționării sectorului și pieței de energie electrică în condiții de eficiență, concurență, transparență și protecție a consumatorilor.

Transelectrica administrează, operează sistemul electric de transport al energiei electrice și asigură schimburile de electricitate între țările Europei Centrale si de Est, ca membru al ENTSO-E.

III.1.1.2 Tensiunile de transport, distribuție și furnizare

Nivelurile de tensiune au fost standardizate și în prezent se folosesc următoarele:

- **750 kV** – tensiune de interconectare și transport la mare distanță (înaltă tensiune);
- **400 kV** – tensiune de transport și interconectare (înaltă tensiune);
- **220 kV** – tensiune de transport (înaltă tensiune);
- **110 kV** – tensiune de distribuție (înaltă tensiune);
- **20 kV** – tensiune de distribuție locală (medie tensiune);
- 400/230 V – pentru utilizatorii casnici și micii utilizatori (joasă tensiune).

Ca și operator de transport, Transelectrica gestionează și operează rețeaua de înaltă tensiune (până la 110 kV inclusiv, considerată infrastructură critică națională) și conduce funcționarea sistemului electroenergetic național, realizând serviciul de sistem prin Dispecerul Energetic Național [14].

III.1.1.3 Serviciul de sistem, sistemele de reglaj al frecvenței

Serviciul de sistem reprezintă serviciul asigurat pentru menținerea nivelului de siguranță în funcționare a sistemului electroenergetic național, precum și a calității energiei electrice conform normelor în vigoare. Serviciile de sistem funcționale sunt asigurate de Transelectrica și reprezintă activitatea curentă a operatorului de transport și sistem în timp ce serviciile de sistem tehnologice sunt asigurate de utilizatorii rețelei electrice de transport (de regulă de către producători) la solicitarea Transelectrica și sunt realizate cu următoarele resurse:

a) sistemele de reglaj primar al frecvenței;
b) sistemul de reglaj secundar frecvență-putere;
c) rezervele de putere;
d) sistemele locale de reglare a tensiunii;

e) sistemele automate de izolare pe serviciile proprii și de autopornire a grupurilor în vederea restaurării funcționării sistemului electroenergetic național după un colaps total sau al unei zone;

f) consumatorii dispecerizabili care își reduc sarcina sau pot fi deconectați, la solicitarea Transelectrica.

III.1.1.4 Politica națională de eficiență energetică

Eficiența energetică este reglementată în România de Legea 121 din 2014 ce creează cadrul legal pentru elaborarea și aplicarea politicii naționale în domeniul eficienței energetice în vederea atingerii obiectivului național de creștere a eficienței energetice, cu o țintă națională indicativă de reducere a consumului de energie cu 19% până în 2020.

III.1.1.5 Calitatea energiei electrice

Calitatea energiei electrice poate fi analizată din punct de vedere

- al tensiunii de alimentare
- al serviciului de alimentare
- comercial

și necesită examinarea întregului lanț electroenergetic: producere, transport, distribuție, utilizare. Normele actuale ce reglementează calitatea energiei electrice sunt stabilite în funcție de daunele medii în cazul abaterilor de la indicatorii de calitate.

Calitatea serviciului de alimentare cu energie electrică este determinată de următorii factori:

- siguranța în funcționare a instalației;
- calitatea energiei electrice la punctul de delimitare dintre consumator și furnizor;
- compatibilitatea electromagnetică a instalațiilor cu mediul în care funcționează, în punctul comun de racord.

În funcție de responsabilitatea luării deciziei, indicatorii de calitate se clasifică astfel:

A. Indicatori primari (în responsabilitatea operatorului de distribuție)

a) Calitatea produsului
- frecvența tensiunii (reglaj P - f)
- amplitudinea tensiunii (reglaj Q - U)
- goluri de tensiune (protecție prin relee)
- supratensiuni (sisteme de protecție contra acestora)

b) Calitatea serviciului reprezentă de: întreruperi de scurtă (<3 minute) sau lungă durată.

Caracteristicile întreruperilor acceptate de utilizator se stabilesc prin convenție între furnizor și acesta.

B. Indicatori secundari (se referă la perturbațiile determinate de tipurile de sarcină ale utilizatorului final și sunt în responsabilitatea acestuia)

A. Rezerva de reglaj primar reprezintă rezerva de putere care în cazul abaterii frecvenței (±200 mHz) de la valoarea de referință (50 Hz) va fi mobilizată automat și integral în 30 de secunde având capacitatea de a rămâne în funcțiune pentru cel puțin 15 minute, toți producătorii de energie electrică având obligația de a asigura acest serviciu;

B. Rezerva de reglaj secundar va fi mobilizată automat și integral într-un interval de cel mult 15 minute, având rolul de a reface rezerva de reglaj primar;

C. Rezerva terțiară

- **rapidă** (cel mult 15 minute);
- **lentă** (cel mult 7 ore) [15].

III.1.1.6 Compatibilitatea electromagnetică

Compatibilitatea electromagnetică constă în abilitatea sistemelor sau echipamentelor de a opera în mediu fără să sufere sau să cauzeze degradări inacceptabile ale funcționării din cauza influențelor electromagnetice și reprezintă, în accepțiunea Comisiei Electrotehnice Internaționale, aptitudinea acestora de a funcționa satisfăcător în mediul lor electromagnetic, fără a induce perturbații inacceptabile în orice alt echipament sau sistem existent in acel mediu.

III.1.2 Factori de risc și influența acestora asupra sistemului electroenergetic național

III.1.2.1 Sistemul electroenergetic național din perspectiva fiabilității și a siguranței în funcționare

Sistemele de control și automatizare implică riscuri majore din partea atacatorilor deoarece toate echipamentele sunt interconectate, acoperă un areal vast, inclusiv în zone accesibile cu dificultate sau inaccesibile în condiții meteorologice defavorabile și integrează fluxuri de date privind monitorizarea și luarea deciziilor și executarea acțiunilor necesare pentru menținerea stabilă a frecvenței sistemului electroenergetic național (**50 Hz**) precum și integritatea acestuia în orice codiții, de-a lungul traseului energiei electrice de la sursă la receptor.

Prin lucrarea de față recunoaștem fără echivoc progresul adus prin implementarea noilor sisteme tehnologice (IT, telecom, SCADA) și dorim să atragem atenția asupra vulnerabilităților apărute o dată cu implementarea noilor tehnologii astfel încât beneficiile (viteză de răspuns mult îmbunătățită, localizarea instantanee a oricărei erori/întreruperi, sisteme automate de protecție, flexibilitate, etc.) să nu permită un atac relativ ușor dar având consecințe deosebit de grave.

Conectivitatea între toate structurile ce alcătuiesc sistemul electroenergetic național integrează funcții digitale avansate din domeniul

telecomunicațiilor și tehnologiei informațiilor care au ca scop evoluția acestuia către Sistemul Electroenergetic Național Inteligent (Smart Grid) în vederea câștigului de durabilitate, flexibilitate și reziliență în fața noilor amenințări, în special a celor din spațiul cibernetic. Un exemplu eficient al descentralizării Sistemului Electroenergetic Național îl reprezintă Danemarca în timp ce evoluția prognozată a Sistemului Electroenergetic Național în România și arhitectura Sistemului Electroenergetic Național în vederea tranziției către varianta inteligentă (Smart Grid) sunt prezentate de Transelectrica.

Această tranziție, de la o rețea electrică tradițională (unidirecțională) către Sistemul Electroenergetic Național Inteligent, se bazează pe fluxuri de energie și telecomunicații în ambele sensuri [16].

III.1.2.2 Riscuri și vulnerabilități ale sistemului electroenergetic național din perspectiva sistemelor de monitorizare, control și achiziție a datelor

A. SCADA din perspectivă legislativă și a reglementărilor

Din punct de vedere al automatizării industriale, am ales să detaliez DCS, SCADA și EMS ca fiind reprezentante pentru procesele tehnologice ale oricărui sistem electroenergetic național.

Sistemele de control distribuit (**DCS**) sunt utilizate în mod obișnuit într-un proces, o instalație sau o uzină, de obicei cu un număr mare de bucle de control, în care controllerele autonome sunt distribuite pe tot sistemul, dar există un control central de supraveghere cu ajutorul unui operator uman. Acestea cresc fiabilitatea și diminuează costurile de instalare prin localizarea funcțiilor de control în apropierea procesului tehnologic, instalației, uzinei, etc. cu monitorizare și supraveghere centralizată la fața locului și sunt preferate în domeniile unde siguranța și fiabilitatea sunt prioritare.

Sistemele de management energetic (**EMS**) monitorizează, controlează și optimizează utilizarea energiei utilizând componente fizice (hardware) pentru a colecta date privind consumul de energie și aplicații software pentru a citi și analiza aceste date, oferă o imagine a consumului de energie al unei clădiri și evidențiază zone pentru îmbunătățirea eficienței. Cu sisteme din ce în ce mai inteligente, sistemele de management al energiei avansează spre un control și o optimizare mai mare a energiei în clădiri și aplicații civile și industriale.

Sistemele de monitorizare, control și achiziție de date (**SCADA**) sunt utilizate în mod obișnuit pentru medii de mari dimensiuni, care pot fi dispersate pe o anumită zonă geografică. Acestea cuprind un centru de comandă care monitorizează și controlează un întreg proces tehnologic, un sistem de distribuție, o uzină, etc. iar cea mai mare parte a operațiunilor se executa automat de către Unități Comandate de la Distanță (**R**emote **T**erminal **U**nit) sau de către Unități Logice de Control Programabile (**P**rogrammable **L**ogic **C**ontroller) în timp ce în centrul de comandă sunt luate decizii de administrare pe baza interfeței grafice a sistemului de monitorizare, control și achiziție de date [17].

Transelectrica recunoaște necesitatea implementării unei soluții noi EMS/SCADA în viitorul apropiat, utilizând capacitățile de telecomunicații și

tehnologia informației din prezent iar în opțiunea strategică de modernizare a inclus:

- înființarea unei structuri organizatorice dedicată pentru prevenirea, analiza, identificarea și reacția la incidentele de securitate cibernetică;
- adaptarea arhitecturii sistemului EMS/SCADA conform cu cerințele de securitate din domeniul infrastructurilor critice (NERC CIP) și a ultimelor standarde de securitate specifice (IEC 62351, ISO/IEC 27001);
- necesitatea unor canale securizate de comunicații
- necesitatea implementării soluțiilor Smart Grid.

În prezent, acestea au evoluat de la câteva implementări construite local, la sisteme complexe, cu hardware și software standardizate (în sensul construirii pe baza unor componente construite în regim de linie de asamblare, nu unicat la comandă și comercializării ca produs/serviciu adaptat fiecărei companii) despre care orice poate găsi detalii, făcându-le vulnerabile către amenințările cibernetice din ce în ce mai prezente și mai eficiente în prezent. SCADA nu a fost proiectat utilizând metode de criptare (deoarece se considera a fi un sistem închis), astfel că odată ce un atacator a intrat în sistem, poate cauza pagube de exemplu prin suprascrierea limitelor de siguranță ala unui proces tehnologic sau poate trimite date false, de exemplu pot modifica parametrii de tensiune sau frecvență într-un sistem electroenergetic în urma cărora sistemele automate de control sau operatorii de serviciu pot decupla zonele țintite de atacator de la alimentarea cu energie electrică.

Din punct de vederea al reglementărilor, în România securitatea sistemelor informatice din sistemele de management energetic/sistemele de monitorizare, control și achiziție de date (EMS/SCADA) este tratată în *Strategia de securitate energetică* și impune adaptarea arhitecturii acestor sisteme conform cu cerințele de securitate din domeniul infrastructurilor critice (NERC CIP) și a ultimelor standarde de securitate specifice sistemelor de proces EMS/SCADA (IEC 62351, ISO/IEC 27001).

În document se specifică necesitatea înființării unei structuri organizatorice dedicată pentru prevenirea, analiza, identificarea și reacția la incidentele de securitate cibernetică ale sistemelor informatice din sistemele menționate anterior și din alte sisteme asociate infrastructurilor critice; această structură urmează să implementeze obiectivele și direcțiile de acțiune prevăzute în baza legală națională, respectiv **HGR nr. 271/2013 pentru aprobarea Strategiei de securitate cibernetică a României și a Planului de acțiune la nivel național privind implementarea Sistemului național de securitate cibernetică.**

B. Exemple de arhitectură a sistemelor de monitorizare, control și achiziție de date, din reglementări și din practică

Sistemele moderne de monitorizare, control și achiziție de date înlocuiesc forța de muncă manuală pentru a efectua sarcini electrice de distribuție

și procese manuale în sistemele de distribuție prin intermediul echipamentelor automatizate. Implementarea acestui sistem mărește eficiența sistemului de distribuție a energiei prin furnizarea de funcții cum ar fi vizualizarea în timp real a operațiilor, dinamica sistemului, înregistrarea datelor, menținerea tensiunilor dorite, a curenților, a factorului de putere, a frecvenței precum și generarea de avertizări în situațiile ce excedă parametrilor normali pre-determinați.

Sistemele de monitorizare, control și achiziție de date efectuează monitorizarea automată, protejarea și controlul diverselor echipamente din sistemele de distribuție cu ajutorul dispozitivelor electronice inteligente comandate de la distanță (RTU). Prin intermediul acestora se urmărește restabilirea serviciului de alimentare cu energie electrică în timpul unei defecțiuni dar mai ales, cum am detaliat anterior se urmărește localizare unei potențiale defecțiuni și luarea măsurilor necesare evitării acesteia, înainte ca aceasta să apară, în vederea menținerii condițiilor de funcționare normale [18].

C. Arhitectura de securitate cibernetică SCADA

Arhitectura de securitate cibernetică a sistemelor de monitorizare, control și achiziție de date este clasificată de Robert Radvanovsky în *Arhitectura metrică a unui sistem SCADA*, conform următoarelor categorii, în timp ce arhitectura unui sistem de securitate cibernetică este descris în normativele americane:

1. Nivelul/cunoștințele structurii de securitate;
2. Nivelul potențialilor adversari;
3. Accesul/autentificarea;
4. Vulnerabilitățile;
5. Potențialul distructiv;
6. Detecția;
7. Recuperarea.

D. Amenințări de natură cibernetică

Un atacator va încerca toate căile posibile pentru a intra în sistem, căutând dispozitive care au integrate antene și procesoare de rețea fără fir (WWAN), căutând în vederea conectării, acele dispozitive care au fost identificate cu breșe de securitate și care nu au încă instalate actualizările necesare [19].

III.2 Metode și măsuri de protecție a sistemului electroenergetic

III.2.1 Securitatea cibernetică din punct de vedere al siguranței naționale, în România și în cadrul partenerilor strategici

- Comandamentul Apărării Cibernetice;
- Centrul Național de Răspuns la Incidente de Securitate Cibernetică (CERT-RO;
- Centrul de Coordonare a Protecției Infrastructurilor Critice (CCPIC);

- Centrul Național Cyberint;
- Centrul Operațional de Răspuns la Incidente de Securitate (CORIS-STS);
- Centrul de Excelență NATO pentru Cooperare în Domeniul Cibernetic (CCDCOE);
- Agenția NATO pentru Comunicații și Informatică (NCIA);
- Divizia cibernetică a FBI
- Serviciul Central de Securitate din cadrul Agenției Naționale de Securitate
- Agenția pentru Securitatea Cibernetică și a Infrastructurilor (CISA);
- Agenția Uniunii Europene pentru Securitatea Rețelelor și a Informațiilor (ENISA)

III.2.2 Sisteme criptografice pentru securizarea comunicațiilor

Anterior, am identificat o vulnerabilitate în cadrul automatizărilor industriale ce ar putea fi exploatată ușor de un atacator și propunem rezolvarea prin securizarea comunicațiilor ce au loc între componentele unor sisteme de monitorizare, control și achiziție de date; în continuare sunt prezentate câteva soluții ce pot fi implementate mai simplu sau mai costisitor, în funcție de nivelul de protecție dorit.

Din punct de vedere al securității cibernetice, aceasta este constituită pe 3 caracteristici de bază:

- **Disponibilitate** (datele sunt accesibile oricând);
- **Integritate** (informațiile nu au fost modificate);
- **Confidențialitate** (datele sunt inteligibile doar persoanelor destinate) [20];

dar și pe următoarele caracteristici adăugate ulterior dar nu mai puțin importante:

- **Autentificare** (metodă de a verifica identitatea utilizatorului și a stabili implicit dacă are acces la respectiva informație);
- **Responsabilitate** (orice tip de acțiune asupra informației poate fi asociat persoanei responsabile);
- **Autenticitate** (datele sunt cele originale, nu fabricate să semene cu originalul);
- **Non-repudiere** (expeditorul primește dovada livrării iar destinatarul primește dovada identității expeditorului; astfel, niciunul nu poate invoca faptul că nu a procesat informația);
- **Fiabilitate** (comportare și rezultate dorite) [21].

Criptografia își derivă denumirea din Grecia antică, unde *kryptos* înseamnă ascuns iar *graphe* se referă la scriere și este ramura științelor matematice care se ocupă cu elaborarea sistemelor criptografice (de cifru) prin care se

intenționează ca informația inițială să nu aibă sens pentru altcineva în afară de emițător și receptor. **Descifrarea** reprezintă procesul invers cifrării, cu condiția de a cunoaște sistemul și cheia de cifrare în timp ce **decriptarea** reprezintă procesul de analiză a criptogramelor în situațiile în care nu se cunosc sistemul și cheile de criptare, în scopul identificării informațiilor în forma lor inteligibilă. Știința care se ocupă cu decriptarea se numește **criptanaliză** și alături de criptografie formează **criptologia** [22].

III.2.2.1 Cifrări prin substituție

- **Codul lui Cezar** (cifrul lui Cezar, deplasarea lui Cezar sau cifru cu deplasare)**.**
- **Cifrul Vigenere** este o evoluție a cifrului Cezar, care fiind foarte ușor de decriptat a evoluat către
- **Substituție polialfabetică.**

III.2.2.2 Transpoziții

În criptografie, transpozițiile se referă la metodele de criptare prin care pozițiile deținute de unități de text sunt deplasate conform unui sistem predefinit, astfel încât textul cifrat constituie o permutare a textului simplu, în speță caracterele textului la vedere sunt reordonate și generează textul cifrat.

III.2.2.3 Metode criptografice de actualitate

A. Metode de criptare simetrică

Criptarea simetrică folosește aceeași cheie atât pentru criptare cât și pentru decriptare, numită *PSK* – Pre-Shared Key:

- ***DES*** (***Data Encryption Standard*** cu o cheie de 56 biți) și ***3DES***;
- ***Blowfish***;
- ***AES*** **(*Advanced Encriptyon Standard*)** [23].

B. Metode de criptare asimetrică

Criptarea asimetrică oferă o complexitate mult sporită, oferă securitate superioară dar și un consum de resurse pe măsură, diferența semnificativă față de criptarea simetrică fiind folosirea încă unei chei suplimentare (private) astfel:

În scopul **păstrării confidențialității datelor**, se criptează prin cheia publică și se descifrează prin cea privată;

În vederea **autentificării**, se criptează prin cheia privată și se descifrează prin cea publică, rezultatul fiind semnătura digitală;

Dintre algoritmii de criptare asimetrică, cei mai folosiți sunt:

- ***RSA***;
- ***DSA*** (*Digital Signature Algori*thm);
- ***DH*** *(Diffie-Hellman key exchange)*;
- ***ECC*** **(***Elliptic Curve Cryptography)* [24].

C. Hash sau funcția de integritate

Confidențialitatea datelor a fost prezentată anterior în modalități variate urmând cursul cunoscut al acestei discipline de-a lungul istoriei însă avem nevoie

ca pachetele de date criptate să ajungă fără modificări (pierderea parțială a datelor sau schimbări ale conținutului) de la destinatar la destinație. În acest scop (asigurarea **integrității** datelor) există *algoritmi de stabilire a integrității datelor* sau conform denumirii de specialitate, *de hash.* Când emițătorul transmite receptorului date, hash-ul generează (matematic) un cod unic de identificare care este de asemenea trimis receptorului. După ce datele au ajuns la receptor, acesta recalculează codul unic de identificare iar dacă cele două sunt identice, datele au ajuns la destinație fără a le fi afectată integritatea [25].

D. Protocoale criptografice pe Internet

Protocolul **Hyper Text Transfer Protocol** este folosit pentru accesarea informațiilor din World Wide Web; pentru a securiza această transmitere a informațiilor se pot folosi:

- **Secure Hyper Text Transfer Protocol** (S-HTTP);
- **Hyper Text Transfer Protocol Secure** (HTPPS) [26].

III.2.2.4 Sisteme criptate utilizate în prezent pentru telecomunicații (text, voce, imagini, video, documente) prin intermediul Internetului

Problema intimității în lumea digitală a condus la criptarea comunicațiilor mobile, prin Internet iar cele mai populare soluții din domeniu, criptate inițial sau pe parcurs, sunt:

A. ***WhatsApp***
B. ***Telegram***
C. ***Threema***
D. ***Signal***
E. Rețeaua Virtuală Privată (VPN) [27]
F. Implementarea soluțiilor blockchain [28]

IV Simulări și modelări ale influențelor factorilor de risc

IV.1 Analize de management

Analiza SWOT, acronime din limba engleză pentru **puncte forte(S), puncte slabe(W), oportunități(O) și amenințări(T)** în cazul unui operator de infrastructură critică din sectorul electroenergetic [29]:

	Benefice	**Periculoase**
Mediul intern al organizației	**S** **PUNCTE FORTE**	**W** **PUNCTE SLABE**
	Din ce puncte de vedere suntem cei mai buni	Din ce puncte de vedere suntem slabi și necesităm măsuri urgent
	Ce resurse financiare avem la dispoziție	Cu ce lipsuri din punct de vedere financiar ne confruntăm
	Care este nivelul personalului	Ce fel de instruire lipsește angajaților
	Ce avantaje oferim pentru	Cum se raportează angajații la

	atragerea resursei umane de calitate	companie din punct de vedere al satisfacţiei profesionale şi personale
	Ce tehnologii folosim	Care sunt greşelile din trecut
		S-au luat măsurile necesare şi suficiente pentru a evita situaţii similare
		Suntem în urmă cu implementarea noilor tehnologii
Mediul extern	**O** **OPORTUNITĂŢI**	**T** **AMENINŢĂRI**
	Ce schimbări ale mediului pot fi exploatate	Cunoaştem concurenţa
	Cunoaştem obiceiurile de consum ale utilizatorilor noştri şi ne adaptăm permanent dinamicii pieţei	Am testat temeinic noile tehnologii înainte de a le implementa
	Cunoaştem punctele slabe ale competitorilor	Anticipăm ce ar putea face concurenţa în detrimentul nostru
	Mediu de lucru pozitiv şi salarizare motivantă	Migrarea forţei de muncă
	Plan de continuare a afacerii, de livrare a serviciilor şi de operaţii în caz de urgenţă	Zone vulnerabile în cazul unui atac fizic
	Plan de acţiune în urma unui dezastru	Vulnerabilităţile faţă de dezastre naturale şi manifestări severe ale vremii
	Plan de răspuns în cazul unui incident de securitate	Sisteme, reţele şi componente vulnerabile în cazul unui atac cibernetic
	Departament IT puternic, cu resursă umană specializată în securitate cibernetică	Lipsa soluţiilor de securitate cibernetică
		Nerespectarea de către personal a indicaţiilor de securitate cibernetică
		Implementarea cu întârziere a pachetelor de actualizare privind vulnerabilităţile identificate
		Căi de acces la distanţă nesecurizate pentru sisteme de monitorizare, control şi achiziţii de date
	Colaborarea cu agenţii de stat specializate în securitate	Disponibilitatea şi accesul facil la date tehnice privind componentele

	cibernetică, companii specializate în astfel de soluții și cu mediul academic implicat în cercetarea acestui domeniu	diverselor soluții de monitorizare, control și achiziții de date din piață
	Care sunt oportunitățile de implementare ale noilor tehnologii fizice sau cibernetice	Am testat integritatea și politicile de securitate ale partenerilor, furnizorilor, celor care prestează servicii externalizate în vederea identificării unor amenințări/vulnerabilități
	Cum, unde și în ce fel putem fi cu un pas înaintea atacatorilor și concurenței prin implementarea tehnologiilor *Blockchain*	

IV.2 Componente ale sistemului electroenergetic național ca posibile ținte ale unui atacator

IV.2.1 Comutatorul de transfer automat

Un comutator de transfer automat cunoscut în domeniu sub acronimul ATS este un dispozitiv ce face parte din sistemele electroenergetice și servește la transferul energiei electrice, în mod automat, de la sursa primară la o sursă de rezervă dacă detectează o defecțiune la sursa primară sau o altfel de întrerupere sau modificare a parametrilor energiei ce provine de la sursa primară [30].

IV.2.2 Transformatorul electric

Transformatorul electric este un aparat electromagnetic static ce transformă parametrii energiei electrice (uzual tensiunea) din circuitul primar în circuitul secundar, pe baza legii inducției electromagnetice. Curentul electric alternativ din circuitul primar străbate înfășurarea primară și produce un câmp magnetic în miezul feros, care la rândul său produce tensiune electrică alternativă în înfășurarea secundară [31].

IV.3 Studiu de caz

IV.3.1.1 Ipoteza

În conținutul ultimei variante la momentul redactării tezei (Planului de dezvoltare a Rețelei Electrice de Transport 2018-2027) Transelectrica pune la dispoziție o listă cu 80 de transformatoare (tabelul 8.8) de putere mare, tipul constructiv, fabrica și anul fabricației, stația de transformare unde este instalat și starea tehnică, de unde reiese inclusiv nevoia urgentă de retehnologizare sau

înlocuire în cazul unor echipamente (ex: transformator 110kV-20kV produs în 1976, în stare tehnică deficitară -32%).

Coroborat cu detaliile infrastructurii EMS/SCADA și de telecomunicații, fără prea mare efort, un atacator interesat (individ sau organizație) obține open-source, foarte rapid și facil numeroase informații care îi sunt de folos în alegerea unei ținte și planificarea unui atac de succes, fizic, cibernetic sau combinat.

Ca scenariu de risc am ales să implementăm un astfel de atac, ce urmărește modificarea parametrilor de siguranță ai unei stații de transformare și o modelare a efectelor acestui atac. Sistemele de apărare împotriva incendiilor în cazul unui transformator de putere, a cărui răcire se realizează cu ulei electroizolant (întâlnit și sub denumirile de ulei electrotehnic sau ulei de transformator) pot fi cu releu de gaze (Buchholz) sau cu sistem de stingere cu gaze inerte [32].

Pentru studiul de caz am ales o stație MT/JT 20kV-400V în care, printr-un atac cibernetic reușit, unul dintre transformatoare este supraîncărcat. Din această cauză, izolația cedează și se creează un arc electric, ce are temperaturi cuprinse între 4000 și 20000^{o}C. Din fișa tehnică disponibilă pe site-ul producătorului, am ales ca exemplu un ulei mineral care are punctul de inflamabilitate la 170^{o}C, temperatura de autoaprindere la 280^{o}C și căldura specifică (cantitatea de căldură necesară unui corp pentru care 1 kg din masa sa își modifică t^{o} cu un grad) de 1860J/kg*^{o}K. Din cauza temperaturii arcului electric, uleiul prin care acesta se transmite se vaporizează și creează o undă de presiune care se propagă cu ~1200m/s în cuva transformatorului și poate cauza ruperea acesteia.

Releul de gaze este ineficient la o creștere bruscă a presiunii, în timp ce sistemul de detectare, semnalizare, avertizare și stingere cu gaze inerte menționat anterior a fost proiectat pentru a minimaliza impactul acestui fenomen, prin integrarea unui vas de expansiune pentru uleiul transformat în stare gazoasă și a unui sistem cu gaze inerte, de suprimare a incendiului rezultat din combustia uleiului în stare gazoasă [33].

Studiul de caz este alcătuit din 3 componente, astfel:

- un model ipotetic de amplasare a unei stații de transformare ce deservește un cartier format din zone rezidențiale, tehnologice și de relaxare;
- caracteristicile unui incendiu produs la unul din transformatoarele stației descrise anterior;
- modelarea parametrilor electrici;
- exemplificarea practică a unei modalități de criptare a parametrilor electrici.

IV.3.1.2 Amplasarea stației de transformare

Am dezvoltat, utilizând aplicația on-line SketchUp și resursele open source 3D Warehouse, un model de plan urbanistic zonal ce cuprinde funcțiuni

mixte precum locuințe, spații de producție, circulație și servicii de transport, instituții publice de învățământ și sănătate și intervenție în situații de urgență, spații destinate cumpărăturilor și spații de recreere, conform figurii 1.

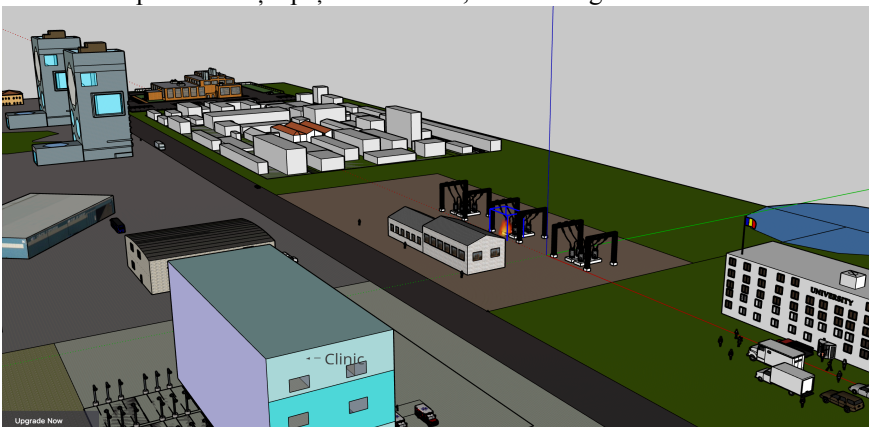

Fig. 1. Plan urbanistic zonal privind studiul de caz, cu stația trafo în centru

IV.3.1.3 Date rezultate din modelarea incendiului la un transformator din stația de transformare

Am creat, utilizând software dedicat pentru simularea incendiilor (PyroSim) și cu ajutorul resurselor open-source GrabCAD community, un model al unei stații de transformare compus dintr-o clădire P+2 cu 5 camere pe fiecare nivel.

Am amplasat la o distanță de 4 metri de fațada clădirii și 10 metri distanță unul față de celălalt, 3 transformatoare (MT/JT). Am ales transformatorul nr. 2 (din mijloc) cu dimensiunile 2,75x2x1,85 m în jurul căruia am creat un mesh de 500.000 de celule (o plasă din mici obiecte geometrice în jurul obiectului supus modelării, cu scopul de a avea o suprafață finită asupra cărora softul va efectua calculele și prin intermediul căreia va afișa grafic dinamica fluidelor).

La fiecare etaj am setat câte 8 termocupluri pe fațadă iar la parter am setat 4 termocupluri în interiorul camerei, conform figurii 2.

Pentru realism și în scopul agravării consecințelor acestui scenariu am setat viteza vântului, care bate dinspre transformator spre clădirea stației, la 6,4 m/s (25 Pascal).

Adaptând scenariul la posibilitățile softului, am considerat cuva transformatorului spartă în urma undei de șoc, uleiul se scurge în partea de jos unde ia foc pe o suprafața egala cu amprenta la sol a transformatorului (burner sau inițierea incendiului).

În vederea rulării acestei simulări am setat softul să indice degajarea de fum și de flăcări, din care am extras capturi de ecran (**simulare cantitativă**) prezentate în figurile 3 și 4, cu scopul de a prezenta vizual efectele incendiului asupra transformatorului și posibila evoluție a acestuia către clădire.

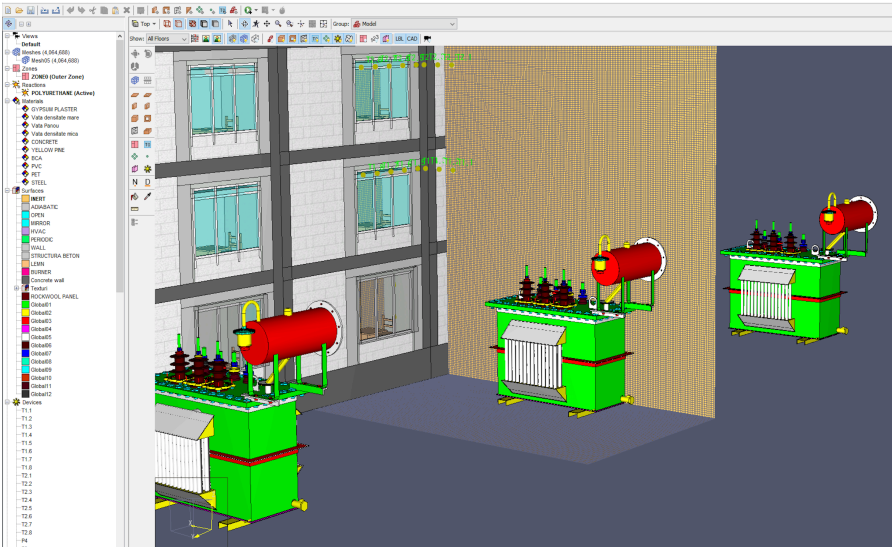

Fig. 2. Mesh şi termocupluri pentru simularea incendiului la transformatorul nr.2

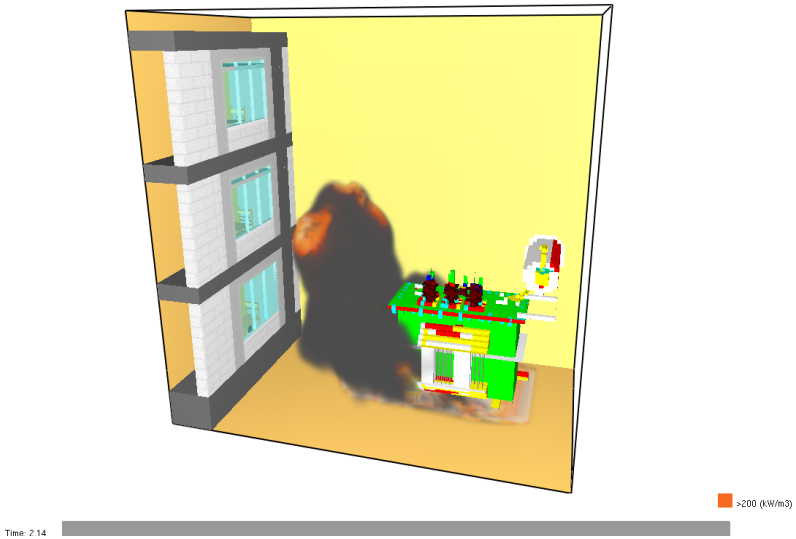

Fig. 3. Incendiu generalizat (cantitativ)

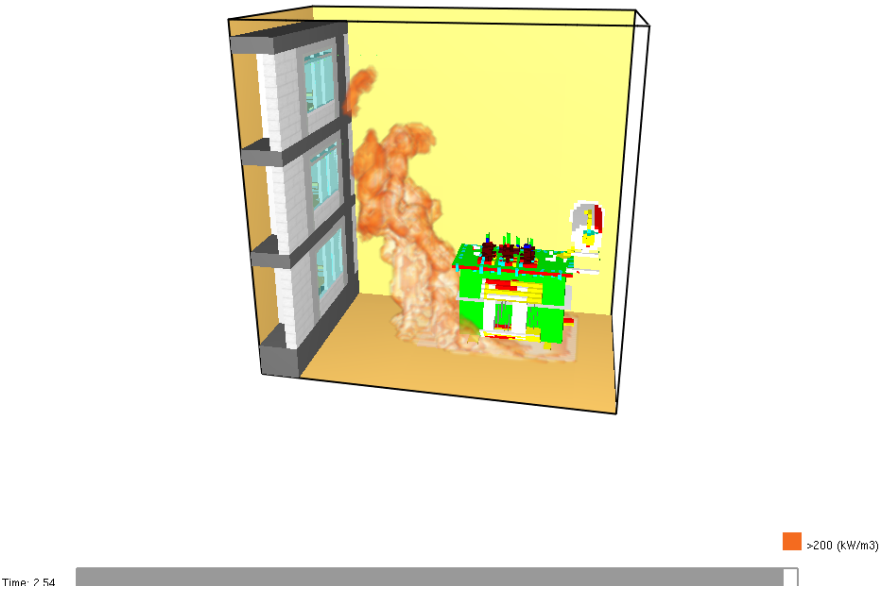

Fig. 4. Dezvoltarea incendiului spre clădire cu prezentarea flăcărilor și fără fum (cantitativ)

În scopul unei simulări care prezintă din punct de vedere **calitativ** rezultatele scenariului prezentat anterior redăm în continuare în figurile 5-9 și prezentăm un extras al parametrilor rezultat din primele 627 de secunde ale unei simulări de incendiu ce s-ar fi stins prin ardere completă în 10 ore (doar transformatorul, fără dezvoltare spre clădire) dacă nu s-ar fi luat măsuri de stingere.

Spre deosebire de cea cantitativă care a returnat rezultate în câteva zeci de minute, aceasta a necesitat 2 săptămâni de calcul pe un computer specializat. Am luat în calcul următorii parametri: 1600 kg de ulei electrotehnic care în urma spargerii cuvei se scurge pe o suprafață de $2m^2$, acesta are capacitatea calorică de 46.000kJ/kg, eliberează o energie totală de 73.600 MJ și o rată de eliberare a căldurii de 2045kW. Materialele din care a fost construită clădirea au fost considerate inerte(nu reacționează, nu transferă căldură și nu iau foc din cauza transferului termic de la transformator). Am ales această abordare datorită timpilor de calcul nerezonabili în cazul folosirii unor materiale combustibile pentru clădire cât și datorită subiectului de interes pentru lucrare, în speță efectele fizice ale unui atac cibernetic asupra unui transformator din perspectiva unei vulnerabilităților unei componente importante în sistemul electroenergetic național.

Uleiul se scurge printr-o breșă în carcasa transformatorului și la contactul cu aerul se autoaprinde datorită temperaturii ridicate în contact cu oxigenul din atmosferă în calitate de comburant.

Figura 5 prezintă evoluția incendiului cu flăcări ascunse în fumul dens ca pericol pe care un transformator îl prezintă în caz de incendiu pentru ocupanților clădirilor din apropiere. Așa cum este vizibil în imaginea anterioară, orice fereastră deschisă ar duce la un pericol grav de intoxicare. Setarea inițială a simulării prezintă un vânt de 20 km/h de la transformator spre clădire stației, care împinge către aceasta fumul, flăcările și duce la creșterea temperaturii și risc de incendiu sporit ceea, ce face ca situația să devină mai periculoasă dar și mai realistă.

Înălțimea flăcărilor poate fi văzută în figura 6 și arată că acestea pot ajunge la o înălțime echivalentă a două etaje (~ 6m), prezentând un pericol ridicat de propagare a incendiului către vecinătăți.

Temperatura transformatorului incendiat și a zonei înconjurătoare este prezentată în figura 7 și poate ajunge la 720℃, reprezentată de zonele roșii și destul de ridicată, considerând că temperatura de aprindere a lemnului se situează în jurul a 250 ℃).

Un flux de aer amestecat cu gaze de combustie este prezentat în figura 8 în timp ce temperatura unui termocuplu de la etajul 1-fațadă este prezentată în figura 9.

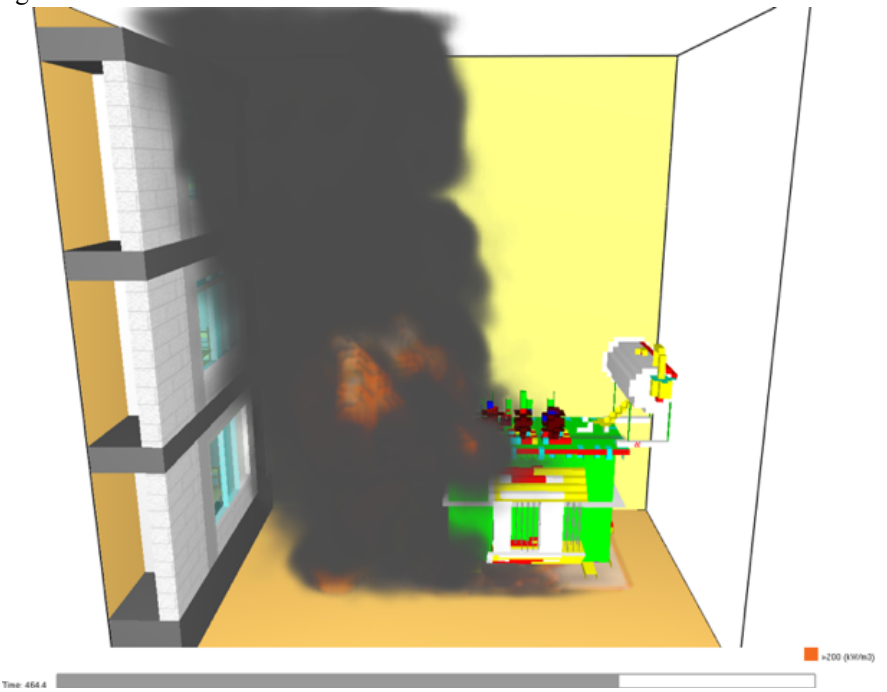

Fig. 5. Dezvoltarea incendiului cu flăcări și fum (calitativ)

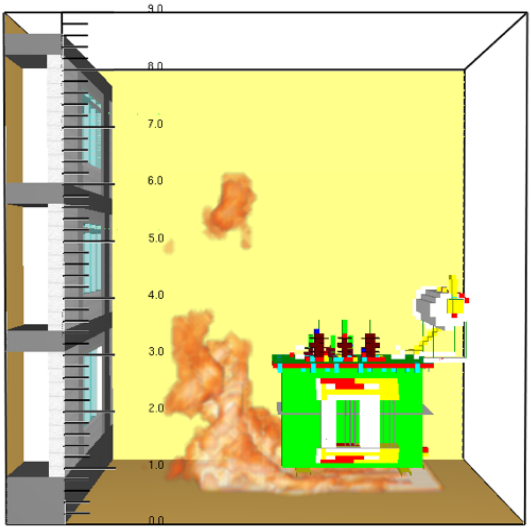

Fig. 6. Înălțimea atinsă de flăcări în cazul simulării calitative

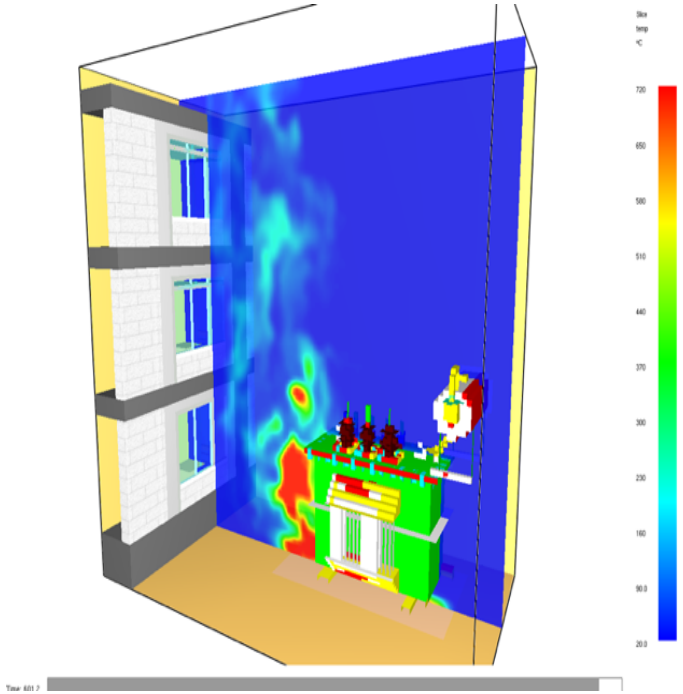

Fig. 7. Temperaturile asociate incendiului cu parametri calitativi

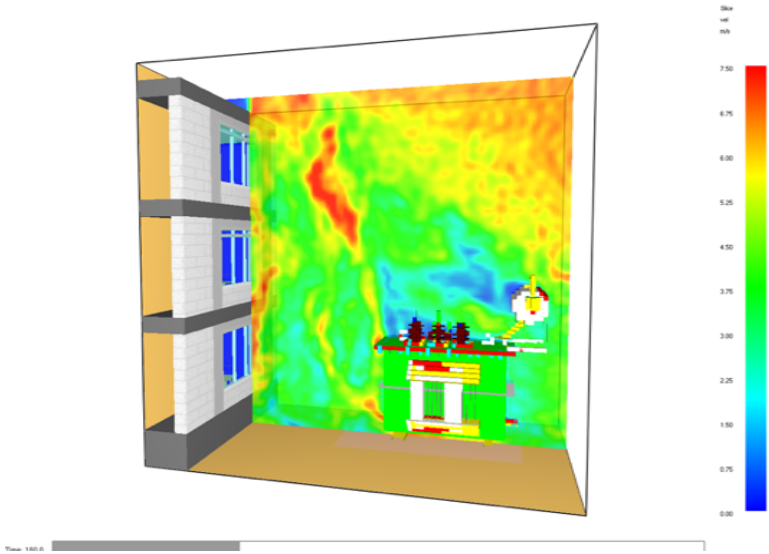

Fig. 8. Modelarea calitativă a incendiului: dinamica aerului și a gazelor de ardere

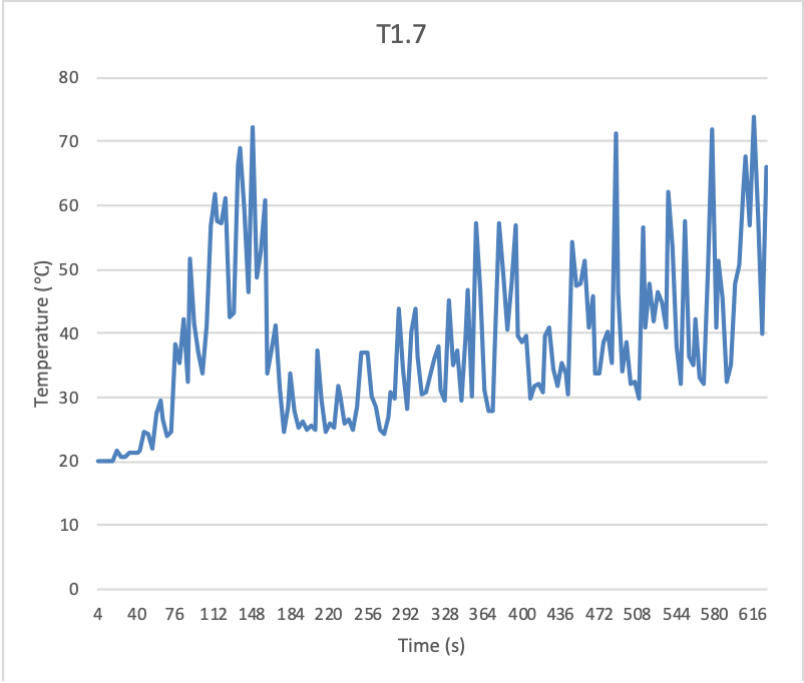

Fig. 9. Modelarea calitativă a temperaturii pe fațadă – etajul 1

Atacul cibernetic ce a cauzat situația modelată a produs pagube în mod direct până când atacatorii au fost identificați în sistem, le-a fost revocat dreptul de acces și modificările operate de aceștia au fost îndreptate coroborat cu acțiunea pompierilor de stingere a transformatorului incendiat în timp ce pagubele indirecte sunt cauzate de întreruperea alimentării cu energie electrică a consumatorilor din zonă.

Un răspuns prompt și eficient al autorităților competente și al specialiștilor companiei electrice ar însemna pentru o stație MT/JT reluarea furnizării energiei în câteva ore și un cost generat de înlocuirea transformatorului afectat. Pentru o stație de înaltă tensiune însă (infrastructură critică), consecințele ar fi grave, deoarece transformatoarele de mare putere sunt scumpe, iar companiile electrice nu păstrează de obicei transformatoare de rezervă. Un atac combinat la câteva astfel de stații bine alese de o organizație/stat ostil ar conduce la un efect în cascadă și o pană în întreaga țară, fără posibilitatea de a fi rezolvată rapid.

Situația modelată anterior este susținută de numeroși factori din care am selectat exemple recente, precum:

- situația precară a unor astfel de mașini electrice, prezentată succint anterior;
- vulnerabilități cibernetice;
- mai multe situații soldate cu avarii la transformatoare ce au degenerat în incendii și implicit în distrugerea totală a acestora, după cum am prezentat anterior exemplul stației Smârdan iar în continuare în figura 10 (preluată din comunicatul ISU Vrancea) cel mai recent caz de incendiu la un transformator ce a afectat transportul feroviar în zonă și a sistat furnizarea energiei electrice în municipiul Adjud în 09.07.2019 [34];
- defecțiuni la 2 transformatoare de mare putere ale operatorului de transport britanic a condus la o pană de energie electrică la ora de vârf în 09.08.2019, ce s-a manifestat în sud-estul Angliei inclusiv Londra, afectând inclusiv traficul rutier și feroviar;
- Un incendiu la un transformator a sistat energia electrică în Manhattan (cartier din New York) în 13.07.2019 conform pompierilor newyorkezi;
- situația statistică a defectelor pentru anii 2017-2018 pusă la dispoziție pentru 7 din județele în care operatorul de distribuție este prezent.

Fig. 10. Incendiu recent la un transformator în Adjud, Vrancea

IV.3.1.4 Date rezultate din modelarea parametrilor electrici la transformatorul supus atacului în simularea precedentă

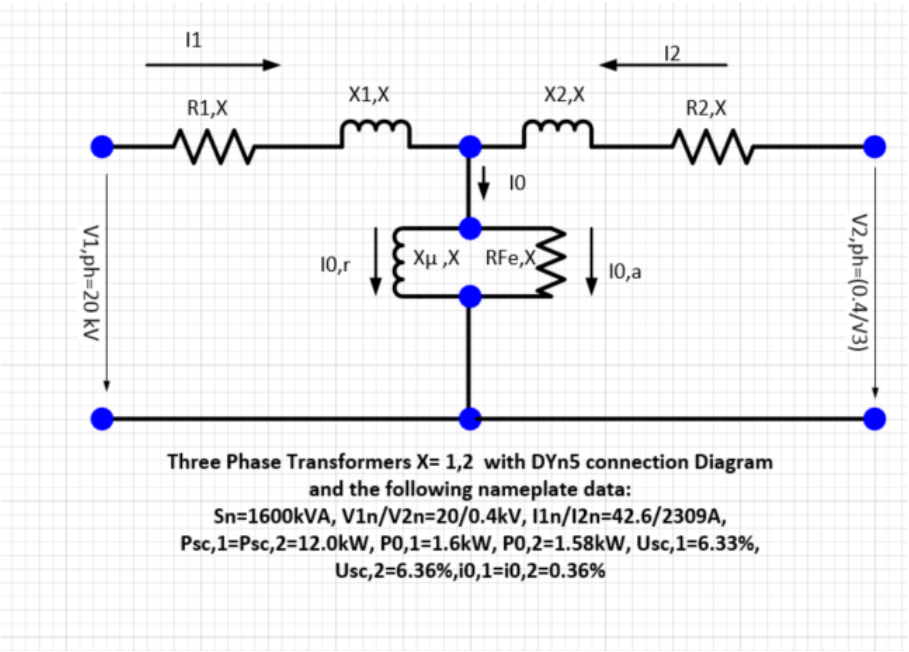

Fig. 11. Circuitul echivalent per fază al transformatorului trifazat din simulare

În figura 11 se prezintă schema și parametri transformatorului trifazat. Ținând cont că înfășurarea primară este conectată în triunghi atunci I1=I1,ph=I1n/√3 în timp ce V1,ph=V1n. X=1,2 sunt indecșii asociați cu transformatoarele 1 respectiv 2, notate în continuare T1 respectiv T2.

A. Determinarea parametrilor R1,X, R2,X, X1,X, X2,X din datele de scurtcircuit

Efectuarea testului de scurtcircuit necesită o tensiune redusă (dată), astfel încât curentul din înfășurarea transformatorului este ideal egală cu valoarea sa nominală. S-au notat:

- R1,X; X1,X – rezistența respectiv reactanța înfășurării primare;
- R2,X; X2,X – rezistența respectiv reactanța înfășurării secundare, raportată la cea primară;
- RkX- rezistența totală de scurtcircuit;
- RkX=R1,X + R2,X;
- XkX- reactanței totală de scurtcircuit;

- XkX=X1,X + X2,X.

Valorile absolute ale tensiunilor de scurtcircuit ale celor două transformatoare:

- Usc1[V]=usck1[%] x V1n/100 = 6.33 x 20000V/100=1266V;
- Usc2[V]=usc2[%] x V1n/100 = 6.36 x 20000V/100=1272V.

Rezistența de scurtcircuit pe fază ale transformatoarelor:

- Rk1=Psc,1/(3 x $I1^2$)=12000W/(3X(46.2/√3)^2)=5.622Ω=Rk2;
- R1,1=R2,1=Rk1/2=2.811Ω;
- R1,2=R2,2=Rk2/2=2.811Ω.

Impedanța de scurtcircuit pe fază ale transformatoarelor:

- Zk1=Usc1[V]/I1=1266/(46.2/√3)=47.46Ω;
- Zk2=Usc2[V]/I1=1272/(46.2/√3)=47.68Ω.

Reactanța totală pe fază:

- Xk1= ($Zk1^2$-$Rk1^2$)$^{1/2}$=47.126Ω;
- Xk2= ($Zk2^2$-$Rk1^2$)$^{1/2}$=47.347Ω.

Reactanțele pe fază ale transformatoarelor:

- X1,1=X2,1=Xk1/2=23.563Ω;
- X1,2=X2,2=Xk1/2=23.6735Ω.

B. Determinarea parametrilor RFe,X și Xμ,X din datele circuitului deschis pentru cele două transformatoare

Componenta activă a curentului din circuitul deschis:

- i0a,1=P0,1/(3 x V1,ph)=1600W/(3 x 20000V)=0.0267A;
- i0a,2=P0,2/(3 x V1,ph)=1580W/(3 x 20000V)=0.0263A.

Rezistențele echivalente corespunzătoare pierderilor din miez:

- RFe,1=V1,ph/I0a,1=749.065kΩ;
- RFe,2=V1,ph/I0a,2=760.456kΩ.

Componenta reactivă a curentului din circuitul deschis:

- i0r,1=(i0,1^2-i0a,1^2)$^{1/2}$=(0.36*(46.2/√3)/100)^2-0.0267^2)$^{1/2}$=0.0922A;
- i0r,2=(i0,2^2-i0a,1^2)$^{1/2}$=(0.36*(46.2/√3)/100)^2-0.0263^2)$^{1/2}$=0.0924A.

Reactanțele echivalente corespunzătoare magnetizării miezului:

- Xμ,1=V1,ph/I0r,1=216.920kΩ;
- Xμ,2=V1,ph/I0r,2=216.450kΩ.

Suplimentar pot fi determinate valorile intrinseci (fără a ne referi la înfășurarea primară) ale parametrilor înfășurării secundare folosind corelațiile de transformare:

- r2,1=R2,1 x (V2,ph/V1,ph)^2=2.811Ω x [(0.4/√3)/20]^2=0.0003748Ω;
- r2,2=R2,2 x (V2,ph/V1,ph)^2=2.811Ω x [(0.4/√3)/20]^2=0.0003748Ω;
- x2,1=X2,1 x (V2,ph/V1,ph)^2=23.563Ω x [(0.4/√3)/20]^2=0.003142Ω;
- x2,2=X2,2 x (V2,ph/V1,ph)^2=23.6735Ω x [(0.4/√3)/20]^2=0.003156Ω.

Rezultatele sunt rezumate conform tabelelor I și II, prezentate în continuare:

Tabel I. Calculul analitic al parametrilor pentru transformatorul nr.1

R1,1[Ω]	**X1,1[Ω]**	**R2,1[Ω]**	**X2,1[Ω]**	**Xμ,1[Ω]**	**RFe,1[Ω]**
2.811	23.563	2.811	23.563	216920	749065

Tabel II. Calculul analitic al parametrilor pentru transformatorul nr.2

R2,1[Ω]	**X2,1[Ω]**	**R2,2[Ω]**	**X2,2[Ω]**	**Xμ,2[Ω]**	**RFe,2[Ω]**
2.811	23.6735	2.811	23.6735	216450	749456

C. Modelare în software dedicat (ETAP) [35]

Transformatorul nr.1 (T1)

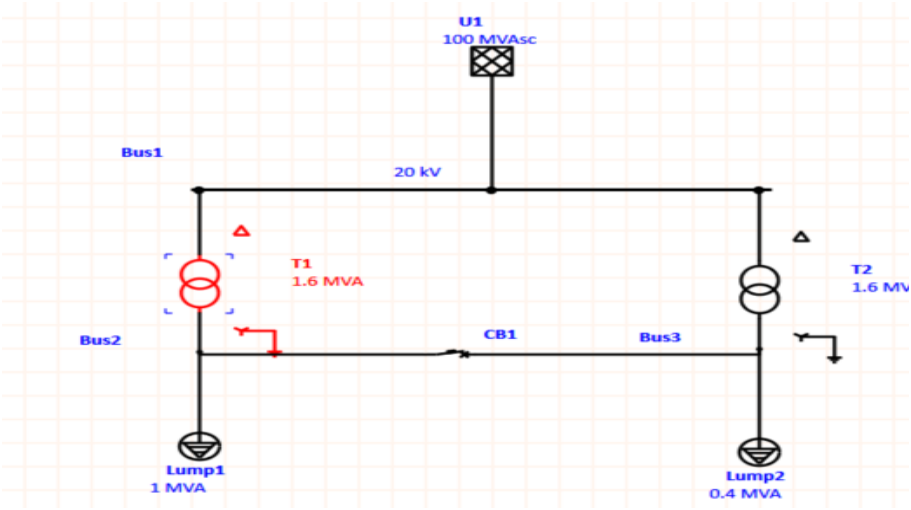

Fig. 12. Circuitul transformatorului T1 supus analizei

În figura 12 este prezentat circuitul transformatorului nr.1 iar în continuare sunt prezentați parametri electrici rezultați din rularea simulării ETAP pentru acesta.

Impedanța de bază: Zb=V1,ph/I1,ph=(20000V/(42.6/√3)A)=749.8Ω;

Impedanța de scurtcircuit: Zk1=(%Zx Zb)/100=(6.33 x 749.8Ω)/100=47.462Ω;

Rezistența de scurtcircuit: Rk1=(%R x Zb)/100=(1.041 x 749.8Ω)/100=7.805Ω;

Reactanța de scurtcircuit: Xk1=(%X x Zb)/100=(6.244 x 749.8Ω)/100=46.8175Ω;

Rezistențele înfășurării primare respectiv secunde raportată la cea primară: R1,1=R2,1=Rk1/2=3.9025Ω;

Reactanțele înfășurării primare respectiv secunde raportată la cea primară: X1,1=X2,1=Xk1/2=23.409 Ω.

Tabel III. Determinarea parametrilor pentru transformatorul nr.1 folosind ETAP

R1,1[Ω]	X1,1[Ω]	R2,1[Ω]	X2,1[Ω]	Xμ,1[Ω]	RFe,1[Ω]
3.9025	23.409	3.9025	23.409	N/A	N/A

Tabel IV. Determinarea parametrilor pentru transformatorul nr.2 folosind ETAP

R2,1[Ω]	X2,1[Ω]	R2,2[Ω]	X2,2[Ω]	Xμ,2[Ω]	RFe,2[Ω]
3.9215	23.5175	3.9215	23.5175	N/A	N/A

Din analiza ambelor seturi de valori prezentate în tabelele 3 și 4 se observă că valorile sunt apropiate.

Configurația circuitului și detaliile pentru defecțiunile diferitelor transformatoare sunt prezentate în Figurile 13-15. Fiecare scenariu se bazează pe simulări efectuate cu ajutorul softului ETAP.

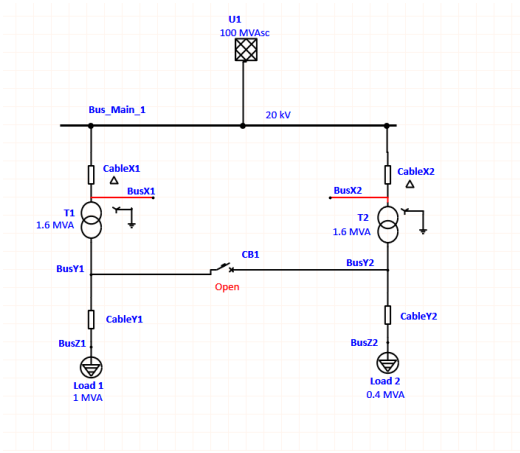

Fig. 13. Reprezentarea schematică a circuitului cu întrerupătorul deschis (swich)

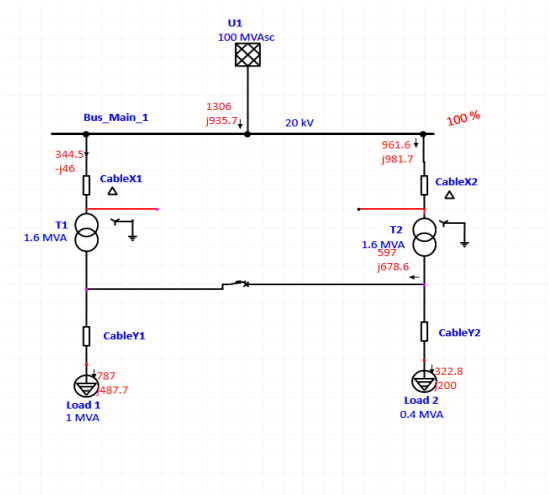

Fig. 14. Configurarea circuitului cu întrerupătorul închis

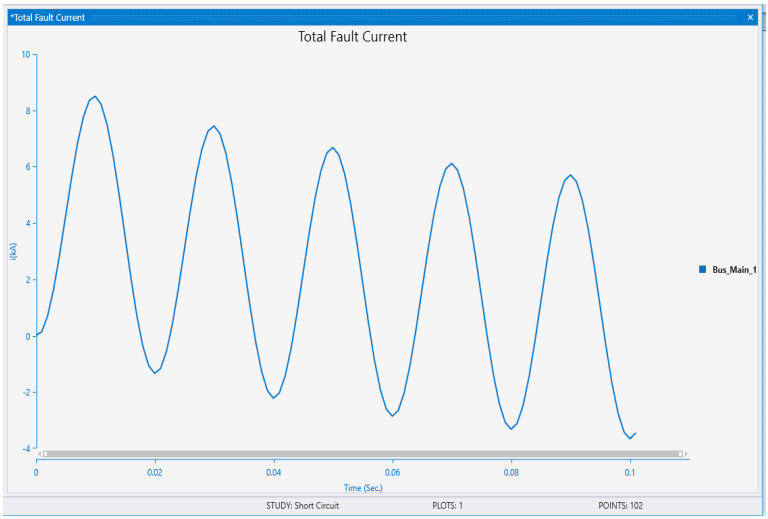

Fig. 15. Curent de avarie la Linia principală1

Rezultatele **finale** referitoare la valorile parametrilor sunt rezumate conform tabelului V, prezentat în continuare:

Tabel V. Valorile parametrilor electrici pentru transformatorul nr.1

Metodă	**R1,1[Ω]**	**X1,1[Ω]**	**R2,1[Ω]**	**X2,1[Ω]**	**Xμ,1[Ω]**	**RFe,1[Ω]**
Analitic	2.811	23.563	2.811	23.563	216920	749065
ETAP	3.9025	23.409	3.9025	23.409	N/A	N/A

IV.3.1.5 Exemplu de criptare a unor parametri electrici vehiculați prin intermediul SCADA

Am ales două transformatoare de producție autohtonă pentru care am propus, pentru a proteja sau cel puțin a îngreuna pentru un potențial atacator ce a reușit să intre în rețea pentru a produce daune, două modalități diferite de criptarea a parametrilor electrici.

În general, soluțiile software sunt globale fiind realizate în limba engleză, motiv pentru care am prezentat în continuarea parametrii aferenți fiecărui transformator astfel, însă același metode de criptare se aplică identic pentru parametri în limba română, oferind bineînțeles un text cifrat diferit.

A. Criptarea parametrilor electrici prin transpoziții

B. Criptarea parametrilor electrici prin substituții polialfabetice

Se alege un alt transformator trifazat 20/0.4kV cu următorii parametri:

Transformer power $\mathbf{S_n}$: 1600 kVA
Terminal Primary voltage $\mathbf{U_{1n}}$: 20kV
Terminal Secondary voltage $\mathbf{U_{2n}}$: 400V
Primary nominal current $\mathbf{I_{1n}}$: 46.2A
Secondary nominal current $\mathbf{I_{2n}}$: 2309A
Type of connection: **Dyn05**
No load losses $\mathbf{P_0}$: 1580W
Copper losses $\mathbf{P_k}$: 12000W
No load current $\mathbf{i_0}$: 0.36%
Short-circuit voltage $\mathbf{u_k}$: 6.36%

Construim un tablou Vigenere cu următorul alfabet: "*.%-:0123456789ABCDEFGHIJKLMNOPQRSTUVWXYZ*" și cheia "*3l3ctrica1transf0rm3r*", ce va returna textul cifrat "*Wcdzl663wfk gyj66 Se: N93L n73 Kw3wjg1v Cjxm1d1 y9o537w 6Bo: VRuI Ltrd4qd6 Vq5f5pksr my8lpg5 G5q: P3CO G9uwbkp xbexn17 fxcuqgk 0Dx: 5Z.TK F6roezduj q0f95mv dni11f8 IT9: 56LCM Mp7q yg 5fxa6rt9aq: GjqCY E6 xyb6 cyfkts GM: 48T38 5f71os ef2f67 Pb: N53L38 Gf 30ke 5l1e62t 9M: 3.6R% Vthib-oss5lsg n3lkwjh fn: I.WX%*".

V Concluzii și contribuții originale

În conținutul lucrării am prezentat amenințări variate, naturale sau antropice, asupra sistemului electroenergetic precum și vulnerabilități ale acestuia, cunoscute (ex: fenomene meteo extreme) sau emergente (ex: atacuri cibernetice) și am subliniat importanța conceptului de reziliență, astfel:

Valorile care stau la baza securității și rezilienței infrastructurilor critice sunt:

- Securitatea și reziliența trebuie luate în considerare din fazele de proiectare;
- Identificarea și managementul riscurilor trebuie executate într-o manieră coordonată și cuprinzătoare pentru

totalitatea infrastructurilor critice, în scopul alocării eficiente a resurselor;

- Înțelegerea și abordarea riscurilor din perspectiva dependințelor între infrastructurile critice sunt esențiale din punct de vedere al securității și rezilienței;
- Măsurile de protecție împotriva propagării vulnerabilităților datorită interdependențelor infrastructurilor critice se realizează prin comunicare, punând informațiile relevante la dispoziția tuturor celor implicați;
- Parteneriatul public-privat se bazează pe încredere, flexibilitate, adaptabilitate, scopuri clare și modalități obiective de măsurare a progresului. Expertiza participanților din domenii variate îmbunătățește siguranța și reziliența, în ansamblu;
- Anumite infrastructuri critice nu se limitează la granițele țării (ENTSO-E – European network of transmission system operators for electricity, în domeniul electric; Nabucco, în domeniul gazelor natural, etc.), securitatea și reziliența acestora reprezentând un factor de interes la nivel inter-statal sau continental.

Lucrarea propune integrarea pe harta României în rețeaua CIWIN, după modelul implementat de Universitatea Politehnică din Torino cu sprijinul Comisiei Europene coroborat cu, dar fără a se limita la modelele prezentate în Abordarea multirisc cu privire la reziliență, ce corelează riscul de incendiu cu managementul vegetației a unui model georeferențial care să cuprindă infrastructurile critice naționale, interconexiunile dintre ele și legăturile cu infrastructurile critice ale statelor cu care România se învecinează precum și informații relevante despre riscurile cu probabilitate de apariție în România.

Informații relevante precum creșterea vegetației ce amenință integritatea liniilor electrice aeriene și crește riscul de incendiu în condiții secetoase, starea infrastructurii, cotele topografice și particularitățile reliefului în funcție de condițiile meteorologice sunt importante pentru a lua deciziile corecte privind intervenția în caz de necesitate la o infrastructură critică izolată sau greu accesibilă în anumite perioade ale anului sau în condiții meteorologice defavorabile.

Particularitățile fiecărei zone seismice, zonele inundabile, zonele afectate în eventualitatea cedării unui baraj de acumulare, pericolele cauzate de fenomenele meteorologice extreme (temperaturi ridicate cu posibilitatea degenerării în incendiu, furtună însoțită de vânt puternic sau descărcări electrice, ceață, căderi masive de zăpadă, avalanșe etc.) integrate pe această hartă ar avertiza din timp operatorul infrastructurii critice afectate, infrastructurile critice naționale sau europene interdependente precum și autoritățile statului, astfel pericolul ar putea fi eliminat din timp sau efectele sale ar fi mult diminuate, cu un impact mult mai mic asupra victimelor, pagubelor și mediului.

Din simulările efectuate cu ajutorul datelor integrate în acest sistem, bazându-ne pe evenimentele negative din trecut și costurile generate de acestea pentru revenirea la funcționarea normală, amplasarea centralelor electrice, a stațiilor de transformare și a rețelei de distribuție aflate în stadiul de proiectare ar urma să se execute ținând cont de particularitățile enumerate anterior, evitând expunerea acestora la anumite riscuri naturale.

Pentru rețeaua electroenergetică aflată în uz, se pot lua măsuri pentru a evita consecințe grave, după cum am prezentat în exemplele anterioare.

Implementarea propusă în lucrare ar conduce la evoluția CIWIN dintr-o platformă de comunicare într-una operațională ce ar integra elemente GIS (Geographic Information System) și SCADA, cu potențialul de a reduce riscurile majore până la un nivel acceptabil deoarece toate structurile implicate vor beneficia de eficiență și timpi de răspuns îmbunătățiți în vederea eliminării sau reducerii efectelor negative datorită scenariilor simulate anterior și a informațiilor complexe și complete puse la dispoziție de aplicație, folosind ca bază platforma RO-RISK (Evaluarea riscurilor de dezastre la nivel național).

De asemenea, în funcție de particularitățile fiecărei zone seismice (normativ P 100-1/013), pentru construcțiile în stadiu de planificare sau proiectare se pot implementa soluții de izolare a bazei în timp ce pentru obiectivele în uz se pot implementa sisteme de izolare seismică a echipamentelor sensibile/critice, pe modelul implementat cu succes la Muzeul Național de Istorie Naturală Grigore Antipa.

Înmulțirea și diversificarea atacurilor cibernetice precum și tranziția către tehnologiile 5G și IoT reprezintă provocări la securitatea infrastructurilor critice din sectorul electroenergetic atât din perspectiva prezentului în care acestea se reglementează, proiectează și implementează treptat cât și din perspectiva unui viitor apropiat caracterizat de interconectare extinsă.

Lucrarea prezintă o viziune a riscurilor apărute ca urmare a digitalizării sistemului electroenergetic național prin exploatarea vulnerabilităților unor componente ce conduc la preluarea controlului în vederea modificării parametrilor și producerii de pagube sau sistării serviciului, motiv pentru care evoluția normală de la rețeaua convențională către cea inteligentă (Smart Grid) implică neapărat implementarea de măsuri corespunzătoare de securitate cibernetică. În funcție de ținta vizată de atacatori, un atac reușit implică modificarea parametrilor electrici conducând către incendiu sau explozie și pagube colaterale, după cum am prezentat în studiul de caz.

Tehnologiile avansate care oferă o mai bună gestionare a sistemului electroenergetic național precum și a conducerea acestuia la distanță au potențialul de a aduce beneficii importante, dar în procesul de integrare a unei astfel de tehnologii trebuie acordată importanța cuvenită adoptării contramăsurilor necesare pentru a preveni evenimentele nedorite și încălcările de securitate inerente acestei evoluții. Măsurile de securitate pentru un astfel de sistem trebuie susținute și dezvoltate pe măsură ce se implementează noi protocoale și apar noi strategii de

atac, ceea ce implică personal specializat ce beneficiază de sprijin și școlarizare frecvent deoarece tehnologia informației și telecomunicațiile au printre cele mai rapide avansuri tehnologice.

În ansamblu, tehnologiile noi prezintă avantaje clare dar, de asemenea, aduc posibile dezavantaje dacă implementarea se realizează incomplet sau defectuos, în special din perspectiva amenințărilor cibernetice, iar efortul de modernizare fără conștientizarea și pregătirea față de aceste tipuri de amenințări pot crea mari prejudicii, sens în care Fiancial Times propune integrarea sectorului privat în exercițiile militare, pentru a fi pregătite în fața agresiunilor emergente, care prin impactul asupra mediului privat lovesc simultan în economia, securitatea și secretele tehnologice ale statelor.

Securitatea cibernetică și securitatea energetică sunt componente ale Strategiei Naționale de Apărare a Țării pentru perioada 2015-2019 în timp ce numeroase state și organizații de profil consideră securitatea cibernetică ca prioritate a securității naționale deoarece cine deține informația deține puterea [36].

Multiplicarea și diversificarea atacurilor cibernetice care se desfășoară în prezent și urmează să evolueze în era 5G și IoT reprezintă provocări tot mai mari pentru securitatea infrastructurilor critice electroenergetice, atât în prezent în stadiul de reglementare, proiectare și implementare, precum și în viitorul apropiat, digitalizat și puternic interconectat.

Lucrarea oferă o perspectivă asupra modului în care digitalizarea rețelei electrice poate fi utilizată pentru a exploata vulnerabilitățile anumitor componente în scopul atacării infrastructurilor critice. Tranziția rețelei electrice clasice către cea inteligentă și toate beneficiile acestei evoluții implică în opinia noastră și responsabilitatea punerii în aplicare de măsuri adecvate pentru contracararea posibilelor atacuri cibernetice.

În funcție de echipamentul atacat în rețea, consecințele unui atac reușit variază și pot duce la vătămări grave și daune materiale în cazul unei explozii sau unui incendiu la un transformator electric, ca efect urmărit sau colateral în cazul unei stații de transformare electrică care furnizează putere la o zonă urbană cu funcție mixtă, așa cum se arată în studiul de caz din lucrare.

Tehnologiile avansate care oferă o gestionare îmbunătățită a rețelei electroenergetice și conducerea de la distanță a acesteia aduc beneficii importante, dar în procesul de adoptare a unei astfel de tehnologii noi, necesare, trebuie acordată importanța cuvenită atât implementării tehnologiei în sine cât și măsurilor de securitate suficiente pentru a preveni eventuale evenimente nedorite sau breșe de securitate.

Acțiunile de securizare pentru un astfel de sistem trebuie dezvoltate și actualizate pe măsură ce se implementează noi protocoale și apar noi strategii de atac, ceea ce înseamnă că personal specializat cu studii/competențe actualizate privitor la noile tipuri de amenințări trebuie să se ocupe de mentenanța, supervizarea și dezvoltarea unui astfel de sistem.

În ansamblu, noutățile tehnologice vin cu numeroase avantaje dar implică simultan și posibile dezavantaje legate de implementare, mentenanță sau actualizare. Efortul ce implică investițiile în modernizare și implementare a noilor tehnologii din domeniul electronică-automatizări, tehnologia informației și telecomunicații reprezintă o direcție de urmat pentru orice companie competitivă, iar conștientizarea și pregătirea față de amenințările, în special cibernetice, care însoțesc acest efort fac diferența dintre o companie rentabilă ce furnizează un serviciu vital în condiții de siguranță și o companie care poate pierde oricând controlul, vulnerabilă în fața competiție, criminalității cibernetice sau organizațiilor statale de profil, cu interese ostile.

Am ales să închei zona de concluzii cu unele dintre cele mai grave vulnerabilități cibernetice interconectate, respectiv vulnerabilități hardware în procesoarele Intel (cel mai mare producător de microprocesoare) cunoscute sub numele de Meltdown, Spectre și SWAPGS [37].

Acestea au fost rezolvate parțial prin update-uri (cu excepția SWAPGS ce a fost descoperit recent de specialiștii Bitdefender), însă o rezolvare completă este posibilă doar prin schimbarea arhitecturii hardware la nivelul noilor generații de microprocesoare, iar efectul acestor vulnerabilități nu este cunoscut deoarece un atac nu poate fi detectat sau stopat de soluțiile antivirus din cauză că nu poate fi deosebit de codul normal (non-malware), prin urmare atacurile speculând aceste vulnerabilități nu au lăsat urme și ca atare prezintă o vulnerabilitate majoră pentru infrastructurile critice din sectorul electroenergetic, unde un atac ar sustrage date clasificate și ar permite o acțiune ulterioară de sabotaj.

V.1 Contribuții originale

În urma cercetării efectuate pe durata studiilor doctorale au rezultat următoarele contribuții proprii:

- am realizat o prezentare a structurii și funcționării sistemelor electroenergetice la nivel mondial, prin parcurgerea unui volum important de referințe bibliografice;
- am elaborat o sinteză a vulnerabilităților și a diverselor tipuri de amenințări la adresa sistemelor electroenergetice pe plan mondial;
- am prezentat într-o manieră nouă sistemul SCADA cu referire directă la modalitatea transferului de date și a riscurilor asociate transmiterii parametrilor electrici;
- am prezentat principalele sisteme de criptare și alegerea celui mai potrivit sistem pentru securizarea informațiilor referitoare la parametri de natură electrică, transmise prin SCADA;
- am realizat un model de analiză de management pentru o companie ce activează în sectorul energetic;

- am implementat o aplicație în mediul de programare PyroSim prin care se ilustrează efectele unui atac cibernetic efectuat asupra unui transformator electric;
- am modelat în mediul de programare ETAP o aplicație prin care se simulează ieșirea din parametri nominali ai unui transformator electric din cauza unui atac cibernetic;
- am dezvoltat două exemple de cifrare a informațiilor pentru parametrii electrici ai unei stații de transformare.

V.2 Perspective de dezvoltare ulterioară

- Continuarea cercetărilor legate de identificarea celor mai eficiente metode de securizare a informațiilor referitoare la parametri electrici din sistemele electroenergetice;
- Implementarea unui sistem GIS și a dronelor pentru supravegherea vegetației din vecinătatea liniilor electrice aeriene și a riscurilor de inundații asupra sistemului electroenergetic la nivel național, conform modelelor menționate anterior și citate.

V.3 Lucrări dezvoltate pe parcursul cercetării doctorale

Pe parcursul cercetării doctorale am făcut parte din colectivul de autori care au redactat lucrările menționate în continuare.

I. Indexate Institute for Scientific Information Web of Science (ISI WoS):

1. H. Andrei, P.C. Andrei, M. Gaiceanu, M. Stanculescu, I. Arama, **I. Marinescu**, *Power Systems Recovery and Restoration Encouter with Natural Disaster and Deliberate Attacks,* pp.247-267, chapter 10 of the book *Power Systems Resilience*, *Modeling, Analysis and Practice,* editors M. Tabatabaei, S.V. Ravadanegh, N. Bizon, Springer, 2019, 353 pages.

2. H. Andrei, M. Gaiceanu, M. Stanculescu, **I. Marinescu,** P.C. Andrei, *Microgrid protection,* pp.606-630 chapter 25 of the book *Microgrid Architectures, Control and Protection Methods*, editors M. Tabatabaei, E. Kabalci, N. Bizon, Springer, 2019, 775 pages , ISBN 978-3-030-23722-6.

3. H. Andrei, M. Gaiceanu, M. Stanculescu, **I. Marinescu**, P. C. Andrei, *Security evaluation of sensor networks*, chapter 11 of the book *Recent Developments on Industrial Control Systems Resilience,* editors M. Tabatabaei, E. Pricop, Springer, 2020.

4. M. Stanculescu, C.A. Badea, **I. Marinescu**, P. Andrei, O. Drosu, H. Andrei, *Vulnerability of SCADA and Security Solutions for a Waste Water Treatment Plant,* IEEE XIth Int. Symposium on Advanced Topics in Electrical Engineering-ATEE, March 28-30, 2019, Bucharest, Romania, Paper 87, 978-1-7281-0101-9/19/$31.00 ©2019 IEEE.

5. **I. Marinescu**, B. Botea, H. Andrei**,** *Critical Infrastructure Risk Assessment of Romanian Power Systems*, IEEE-5th Int Symposium on Electrical and Electronics Engineering-ISEEE, 20-22 oct. 2017, Galati Romania, paper 69, IEEE Catalog Number CFP1793K-USB, ISBN 978-1-5386-2058-8, indexat ISI Web of Science.

6. **I. Marinescu**, H. Andrei, I. Iordache, *Protection methods and actions to increase the safety of operation in power systems assimilated to critical infrastructures,* IEEE-11th International Conference - Electronics, Computers and Artificial Intelligence (ECAI 2019), 27-29 june 2019, Pitesti Romania, paper 43, IEEE Catalog Number CFP1927U-USB, ISBN 978-1-7281-1623-5, indexat ISI Web of Science.

7. D. Burlacu, A. M. Georgescu, A. A. Vartires, **I. Marinescu**, *An experimental evaluation of visibility in simulated smoke, the* 9th International Conference on ENERGY and ENVIRONMENT CIEM 2019, 17-18 october 2019, Timisoara Romania, acceptat pentru prezentare în cadrul conferinței indexată ISI Web of Science.

8. ***I. Marinescu****, S. Deleanu, M. Stănculescu, L. Bobaru, P. Andrei, H. Andrei, Electrical equipment safety analysis and simulation. Case study: transformer's malfunctions,* IEEE-6th Int Symposium on Electrical and Electronics Engineering-ISEEE, 18-20 oct. 2019, Galati Romania, paper 14, acceptat pentru prezentare în cadrul conferinței indexată ISI Web of Science.

II. Indexate în Baze de Date Internaționale:

1. B. Botea, **I. Marinescu**, C. Dragoi, H. Andrei**,** *Modeling, Simulation and Analysis of Disturbance in Low Voltage Instalations,* The Scientific Bulletin of Electrical Engineering Faculty, 2019, year v19, 1(40), Published: May 2019, pp. 49–57, DOI: 10.1515/SBEEF-2019-0010

2. B. Botea, **I. Marinescu**, *New Approaches in the Consumer - Supplier Relationship Regarding Malfunctions in the Electroenergetic Systems and from the Perspective of the IoT Development,* The Scientific Bulletin of Electrical Engineering Faculty, 2017, year 17, 2(37), Published: October 2017, pp. 48–53, DOI: 10.1515/SBEEF-2017-0011

Bibliografie selectivă (din totalul de 260 de lucrări):

[1] A. Badea, Echipamente și instalații termice
[2] http://www.nuclearelectrica.ro/
[3] W. Wang, et al – Simultaneous production of fresh water and electricity via multistage solar photovoltaic membrane distillation
[4] http://www.termo.utcluj.ro/regenerabile/6_3.pdf
[5] The President's National Infrastructure Advisory Council (NIAC), SUA
[6] NIST Framework and Roadmap for Smart Grid Interoperability Standards, Release 1.0
[7] V. Boutin, M. Feasel, K. Cunic, J. wild, How Microgrids Contribute to the Energy Transition

[8] North American Electric Reliability Council, Technical Analysis of the August 14, 2003, Blackout: What Happened, Why, and What Did We Learn?
[9] https://thehackernews.com/2017/12/triton-ics-scada-malware.html
[10] R. Smith, Assault on California Power Station Raises Alarm on Potential for Terrorism, The Wall Street Journal
[11] WorldRiskReport-2018, https://weltrisikobericht.de/english-2/
[12] D. Oyedokun, P. Cilliers, Geomagnetically Induced Currents: A Threat to Modern Power Systems, Classical and Recent Aspects of Power System Optimization, 2018
[13] Clasificarea internațională a evenimentelor nucleare și radiologice (INES)
[14] Codul Tehnic al Rețelei Electrice de Transport, Compania Națională de Transport al Energiei Electrice S.A.
[15] H. Albert, S. Gheorghe, N. Golovanov, L. Elefterescu, R. Porumb, Calitatea energiei electrice. Contribuții. Rezultate. Perspective, Editura AGIR, București 2013
[16] Politica CNTEE Transelectrica în domeniul Smart Grid perioada 2018-2027
[17] C. Teba, Building Technologies: Who's Who? https://www.dexma.com/building-technologies-whos/
[18] SCADA architecture example https://www.electricaltechnology.org/2015/09/scada-systems-for-electrical-distribution.html
[19] Software specializat accesabil la adresa https://nmap.org/
[20] ISO/IEC 27000:2018 https://www.iso.org/standard/73906.html
[21] United States Naval Academy, The Cyber Battlefield https://www.usna.edu/Users/cs/wcbrown/courses/si110AY13S/lec/l21 /lec.html
[22] A. Andrei, M. Stănculescu, Criptografie vs. Criptanaliză, Printech 2014
[23] https://inmcm.wordpress.com/2010/03/14/basic-aes-128-encryption-in-vhdl-complete/
[24] Elliptic Curve Cryptography, https://www.ssl2buy.com/wiki/ecc-algorithm-to-enhance-security-with-better-key-strength
[25] Merkle–Damgård hash function, https://en.wikipedia.org/wiki/Merkle%E2%80%93Damg%C3%A5rd_construction
[26] https, https://ro.wikipedia.org/wiki/HTTPS
[27] VPN, https://en.wikipedia.org/wiki/Virtual_private_network
[28] International Association for Trusted Blockchain Applications, https://inatba.org/
[29] R. Ivorschi, Analiza SWOT - instrument managerial pentru eficientizarea activității
[30] M. Rouse, T. Culverhouse, TechTarget, automatic transfer swich (ATS)
[31] Universitatea "Dunărea de Jos" din Galați, Facultatea de Automatică, Calculatoare, Inginerie Electrică și Electronică, note de curs "Transformatorul electric"
[32] Releu_Buchholz, https://ro.wikipedia.org/wiki/Releu_Buchholz
[33] Sisteme de stingere a incendiilor la transformatoare electrice, http://www.sergi-tp.com/how-transformer-protector-works/
[34] https://monitoruldevrancea.ro/2019/07/09/video-si-foto-incendiu-pe-calea-ferata-circulatia-feroviara-este-intrerupta/
[35] ETAP (Electrical Power System Analysis & Operation Software), https://etap.com/
[36] V. Vevera, Spațiul cibernetic – noul câmp de luptă, Revista Română de Informatică și Automatică, vol. 26, nr. 1
[37] https://labs.bitdefender.com

Curriculum Vitae

INFORMAŢII PERSONALE

MARINESCU Ioan

Șos. Colentina nr. 16, Sector 2, 021177, București

0723 188 057

ioan.marinescu@yahoo.com

Sexul M | Data naşterii 22/11/1988 | Naţionalitatea român

EXPERIENŢA PROFESIONALĂ

07.2017 – prezent

Ofițer

Serviciul de Telecomunicații Speciale

Tipul sau sectorul de activitate: Telecomunicații și tehnologia informațiilor

06.2016 – 06.2017

Comandant companie (Instructor militar I)

Academia de Poliție „Al. I. Cuza”

Tipul sau sectorul de activitate: Învățământ - Ordine și siguranță publică

12.2012 – 05.2016

Comandant pluton (Instructor militar IV)

Academia de Poliție „Al. I. Cuza”

Tipul sau sectorul de activitate: Învățământ - Ordine și siguranță publică

EDUCAŢIE ŞI FORMARE

09.2016 - prezent

Studii universitare de doctorat specializarea “Inginerie electrică”

Universitatea “Valahia”

10. 2015

Curs „Manager de proiect”

Institutul de Studii pentru Ordine Publică

2013 - 2015

Master “Managementul activităților de ordine publică și siguranță națională”

Academia de Poliție „Al. I. Cuza” – Facultatea de Poliție

03. 2014

Curs „Formator”

Institutul de Studii pentru Ordine Publică

06.2013 – 12. 2013

Curs „Instructor în poligonul de tragere”

Institutul de Studii pentru Ordine Publică

2008 - 2012

Studii universitare de licență - Ingineria instalațiilor / Ofițer

Academia de Poliție „Al. I. Cuza” – Facultatea de Pompieri

2003 - 2007

Studii liceale, profil real, specializarea matematică-informatică

Grup Școlar Industrial “I. L. Caragiale” – Moreni

COMPETENȚE PERSONALE

Limba maternă: Română

Alte limbi străine cunoscute

	ÎNȚELEGERE		VORBIRE		SCRIERE
	Ascultare	Citire	Participare la conversaţie	Discurs oral	
Engleză	C2	C2	C2	C1	C2

Competenţe și abilități sociale

- Competenţe bune de comunicare și relaționare cu alte persoane;
- Capacitatea de a lucra în echipă, atât ca parte a grupului cât și în postura de lider;
- Comportament și conduită etică, în timpul și în afara serviciului;
- Capacitatea de integrare în colectiv, inclusiv în cadrul unor echipe multinaționale și de a dezvolta relații armonioase cu subordonații, colegii și comandanții;
- Capacitatea de asimilare a noilor informații și abilități;
- Capacitatea de a comunica în condiții de stres cu toate categoriile sociale (experiență în cadrul proceselor electorale).

Competenţe organizaţionale/manageriale

- Leadership;
- Capacitatea de a structura și a susține un discurs;
- Realizarea unui climat de muncă optim prin motivarea subordonaților, conducere prin exemplu și prin asumarea responsabilității pentru efectele acțiunilor proprii și ale structurii coordonate (experiență în cadrul conducerii unor subunități militare);
- Atenție distributivă și capacitatea de a anticipa evoluția situațiilor, acordând atenție detaliilor;
- Capacitatea de a lua decizii sub stres, cu adaptare la situații noi și complexe.

Competenţe informatice

-Cunoașterea sistemelor de operare Android, macOs și Windows;
-Atestat de competențe profesionale – informatică (obținut în 2007 în cadrul Grupului Școlar Industrial "I. L. Caragiale" – Moreni);
- Cunoaştere aprofundată a instrumentelor Microsoft Office (Word, Excel, PowerPoint);
- Cunoaștere de nivel mediu a mediului de simulare PyroSim;
- Cunoaştere aprofundată a programului;
- Cunoaştere aprofundată a programului Adobe;
- Cunoaştințe de nivel mediu a programului Adobe Photoshop.

Hobby-uri

Fotografia, călătoriile, tenisul, înotul.

Permis de conducere

Categoria B din 2008

INFORMAȚII SUPLIMENTARE

Misiuni cu participare internațională

Ofițer, responsabil al delegației Academiei de Poliție "Al. I. Cuza" la XI International Rescue Workshop "Fenix 2014", iunie 2014, Pionki, Polonia.

Ofițer, membru al delegației Academiei de Poliție "Al. I. Cuza" la exercițiul cu tema "Biological Threat Response Table-Top Exercise" susținut de Defense Threat Reduction Agency prin Ambasada SUA, septembrie 2013, București.

Student, membru al delegației Academiei de Poliție "Al. I. Cuza" la IX International Rescue Workshop "Fenix 2012", mai 2012, Pionki, Polonia.

Referințe

Referințele pot fi furnizate la cerere

Lista publicațiilor rezultate în urma cercetării științifice din programul de studii doctorale, publicate sau acceptate spre publicare

I. Indexate Institute for Scientific Information Web of Science (ISI WoS):

1. H. Andrei, P.C. Andrei, M. Gaiceanu, M. Stanculescu, I. Arama, **I. Marinescu**, *Power Systems Recovery and Restoration Encouter with Natural Disaster and Deliberate Attacks,* pp.247-267, chapter 10 of the book *Power Systems Resilience*, *Modeling, Analysis and Practice,* editors M. Tabatabaei, S.V. Ravadanegh, N. Bizon, Springer, 2019, 353 pages.

2. H. Andrei, M. Gaiceanu, M. Stanculescu, **I. Marinescu,** P.C. Andrei, *Microgrid protection,* pp.606-630 chapter 25 of the book *Microgrid Architectures, Control and Protection Methods*, editors M. Tabatabaei, E. Kabalci, N. Bizon, Springer, 2019, 775 pages , ISBN 978-3-030-23722-6.

3. H. Andrei, M. Gaiceanu, M. Stanculescu, **I. Marinescu**, P. C. Andrei, *Security evaluation of sensor networks*, chapter 11 of the book *Recent Developments on Industrial Control Systems Resilience,* editors M. Tabatabaei, E. Pricop, Springer, 2020.

4. M. Stanculescu, C.A. Badea, **I. Marinescu**, P. Andrei, O. Drosu, H. Andrei, *Vulnerability of SCADA and Security Solutions for a Waste Water Treatment Plant,* IEEE XIth Int. Symposium on Advanced Topics in Electrical Engineering-ATEE, March 28-30, 2019, Bucharest, Romania, Paper 87, 978-1-7281-0101-9/19/$31.00 ©2019 IEEE.

5. **I. Marinescu**, B. Botea, H. Andrei**,** *Critical Infrastructure Risk Assessment of Romanian Power Systems*, IEEE-5th Int Symposium on Electrical and Electronics Engineering-ISEEE, 20-22 oct. 2017, Galati Romania, paper 69, IEEE Catalog Number CFP1793K-USB, ISBN 978-1-5386-2058-8, indexat ISI Web of Science.

6. **I. Marinescu**, H. Andrei, I. Iordache, *Protection methods and actions to increase the safety of operation in power systems assimilated to critical infrastructures,* IEEE-11th International Conference - Electronics, Computers and Artificial Intelligence (ECAI 2019), 27-29 june 2019, Pitesti Romania, paper 43, IEEE Catalog Number CFP1927U-USB, ISBN 978-1-7281-1623-5, indexat ISI Web of Science.

7. D. Burlacu, A. M. Georgescu, A. A. Vartires, **I. Marinescu**, *An experimental evaluation of visibility in simulated smoke, the* 9th International Conference on ENERGY and ENVIRONMENT CIEM 2019, 17-18 october 2019, Timisoara Romania, acceptat pentru prezentare în cadrul conferinței indexată ISI Web of Science.

8. ***I. Marinescu****, S. Deleanu, M. Stănculescu, L. Bobaru, P. Andrei, H. Andrei, Electrical equipment safety analysis and simulation. Case study: transformer's malfunctions,* IEEE-6th Int Symposium on Electrical and Electronics Engineering-ISEEE, 18-20 oct. 2019, Galati Romania, paper 14, acceptat pentru prezentare în cadrul conferinței indexată ISI Web of Science.

II. Indexate în Baze de Date Internaționale:

1. B. Botea, **I. Marinescu**, C. Dragoi, H. Andrei**,** *Modeling, Simulation and Analysis of Disturbance in Low Voltage Instalations,* The Scientific Bulletin of Electrical Engineering Faculty, 2019, year v19, 1(40), Published: May 2019, pp. 49–57, DOI: 10.1515/SBEEF-2019-0010

2. B. Botea, **I. Marinescu**, *New Approaches in the Consumer - Supplier Relationship Regarding Malfunctions in the Electroenergetic Systems and from the Perspective of the IoT Development,* The Scientific Bulletin of Electrical Engineering Faculty, 2017, year 17, 2(37), Published: October 2017, pp. 48–53, DOI: 10.1515/SBEEF-2017-0011

PhD Summary

Analysis of the operational safety of the national power grid and the implementation of protective measures against risk factors

PhD supervisor,
Professor Horia Leonard Andrei

PhD student,
Ioan Marinescu

TÂRGOVIȘTE
2019

Content

I ELECTRICAL ENERGY SYSTEMS. GENERATOR – DISTRIBUTOR -CONSUMER CONNECTION.....

I.1 ELECTRICAL ENERGY SYSTEMS IN ROMANIA 4
I.1.1 Context of the research topic 4
I.1.1.1 Topicality of theme 4
I.1.1.2 General structure 4
I.1.2 Highlights of electricity generation, transmission, distribution and supplying in Romania 5
I.1.3 The main ways to generate electric energy in Romania 5
I.1.3.1 Thermal/thermoelectric power station 5
I.1.3.2 Nuclear power plants.....5
I.1.3.3 Hydropower plant.....6
I.1.3.4 Solar energy.....6
I.1.3.5 Wind power 6
I.2 GENERATOR – DISTRIBUTOR – CONSUMER CONNECTION.....7
I.2.1 Distribution and supplying electrical power in Romania 7
I.2.2 Romania as an actor on European energy system.....7
I.2.3 Energetic strategy expectation.....8
I.2.4 Analysis and forecasts of the Romanian Energy Regulatory Authority 8

II IDENTIFICATION OF CRITICAL INFRASTRUCTURES PARAMETERS OF THE POWER SYSTEMS AND RISK MANAGEMENT .....

II.1 CRITICAL INFRASTRUCTURES ASSOCIATED TO POWER SYSTEMS AND THE IDENTIFICATION OF THEIR PARAMETERS.....9
II.2 MODELLING CRITICAL INFRASTRUCTURES ASSOCIATED TO POWER SYSTEMS 11
II.2.1 Smart Grid.....11
II.2.2 Microgrid.....11
II.2.3 Power grid crisis.....12
II.3 RISK MANAGEMENT IN CRITICAL INFRASTRUCTURES. WAYS TO MITIGATE RISK. 14
II.3.1 Natural risks.....18
II.3.1.1 Earthquake.....18
II.3.1.2 Extreme weather phenomena 18
II.3.1.3 Solar phenomena with interference in the Earth's magnetosphere .20
II.3.2 Human related risks.....20
II.3.2.1 Nuclear energy 20

III METHODS AND PROTECTIVE MEASURES FOR INCREASING THE SAFETY IN OPERATION OF THE POWER SYSTEMS.....

III.1 THE INFLUENCE OF RISK FACTORS ON THE POWER GRID.....21
III.1.1 Romania in the European electricity transmission system.....21
III.1.1.1 National Electricity Transport Company Transelectrica and the National Energy Dispatcher.....21

III.1.1.2 Transport, distribution and supply voltages 21
III.1.1.3 System service, frequency adjustment systems 21
III.1.1.4 National energy efficiency policy 22
III.1.1.5 Electricity delivered in quality parameters 22
III.1.1.6 Electromagnetic compatibility 23
III.1.2 Risk factors and their influence on the national power grid 23
III.1.2.1 The national power grid reliability and safety in operation 23
III.1.2.2 Risks and vulnerabilities of the national power grid from the perspective of supervisory control and data acquisition systems 24
III.2 METHODS AND MEASURES TO PROTECT THE POWER GRID 26
III.2.1 Cyber security as a national security threat in Romania and within strategic partners..... 26
III.2.2 Cryptographic systems for secure communications 27
III.2.2.1 Substitution ciphering 27
III.2.2.2 Transposition cipher 28
III.2.2.3 Current cryptographic methods 28
III.2.2.4 Encrypted systems currently used for telecommunications (text, voice, images, video, documents) over the Internet 29

IV SIMULATION AND MODELING THE INFLUENCE OF RISK FACTORS 29

IV.1 MANAGEMENT ANALYSIS 29
IV.2 COMPONENTS OF THE NATIONAL POWER GRID AS PRESUMPTIVE TARGETS FOR A HOSTILE ENTITY 30
IV.2.1 Automatic transfer switch (ATS)..... 30
IV.2.2 Electrical transformer..... 31
IV.3 CASE STUDY 31
IV.3.1.1 Hypothesis 31
IV.3.1.2 The location of the electric substation 32
IV.3.1.3 Data resulting from fire modeling at a substation transformer 32
IV.3.1.4 Electrical parameters modeling for the transformer subjected to the attack in the previous simulation 40
IV.3.1.5 Example of electrical parameters encryption for secure SCADA communication 45

V ORIGINAL CONCLUSIONS AND CONTRIBUTIONS.....

V.1 ORIGINAL CONTRIBUTIONS 49
V.2 FURTHER DEVELOPMENT PERSPECTIVES 50
V.3 RESEARCH DEVELOPED DURING THE DOCTORAL STUDIES 50

SELECTIVE BIBLIOGRAPHY (OUT OF A TOTAL OF 260 ENTRIES): .....

Keywords: *risk, threat, vulnerability, resilience, critical infrastructures, Smart Grid, supervisory control and data acquisition, data encryption.*

I Electrical energy systems. Generator – distributor - consumer connection.

I.1 Electrical energy systems in Romania

I.1.1 Context of the research topic

Energy represents the engine of contemporary society without it our existence would return to a point similar to the medieval period. At the same time, its production is one of the main sources of pollution and the main cause of global warming. Access to energy is a priority for the individual and its uninterrupted availability and quality assurance is currently a priority for any state, being nominated as a fundamental strategic objective of our country.

Romania develops an energy policy based on its strategic interests, but at the same time, as a full-fledged member of the European Union, it applies the principle of solidarity and contributes to the creation and development of trans-European networks of interest for the subject of the thesis, respectively energy and telecommunications, included in the Treaty on European Union.

I.1.1.1 Topicality of theme

The near future involves the implementation of the fifth-generation telecommunications standard known as International Mobile Telecommunications Standard 2020 (IMT-2020 or 5G), in which the Romanian Authority for Communications Management and Regulation (ANCOM) announced that intends to grant the licenses by the end of 2019, with the possibility of use by operators starting from 2020.

The European Commission recommends a common approach of EU countries on the security of these new networks, regarding the Internet of Things (IoT) perspective and the interconnection of equipment from sectors considered critical infrastructure (such as energy). The United States of America is cautiously approaching the new evolution of telecommunications networks from the perspective of intelligence gathering and sabotage vulnerabilities.

I.1.1.2 General structure

The thesis was structured on 5 chapters, as follows:

Chapter I presents an introduction to the emergence and development of the national power grid, an overview of the main ways of electricity production, its transmission and related regional interconnections as well as the perspectives of the energy strategy.

Chapter II presents the projected evolution of the electricity systems its related risks are identified, classified and analyzed from a national and global perspective.

Chapter III presents the national power grid's interconnection with the European ones, its operating and quality parameters, driving examples through

supervisory control and data acquisition systems (SCADA), the perspective of the new cyber threats that appeared simultaneously with its evolution towards the Smart Grid, 5G, Internet of Things (IoT) and an overview of information encryption methods in order to secure the digital power grid by encrypting the parameters of electricity.

Chapter IV presents a management analysis model for an electro-energetic critical infrastructure component, a software modeling of the consequences of a successful attack on such a component of the national power system and another one regarding the electrical parameters fluctuation in case of an attack, and two ways of electrical parameters encryption.

Chapter V presents the conclusions, the original contributions, perspectives for further development and the scientific research results during the doctoral studies.

I.1.2 Highlights of electricity generation, transmission, distribution and supplying in Romania

The power plant generates the electricity, the transmission system operator operates the high voltage network and balances the demand with the supply, the distributor manages the medium and low voltage electricity network until the final consumer and the supplier represents the consumer in the contractual relationship with the distributor, collects the related invoices and pays the services to the producer, transporter and distributor.

I.1.3 The main ways to generate electric energy in Romania

I.1.3.1 Thermal/thermoelectric power station

The thermoelectric or thermal power station refers to the capacities of electricity production, based on the conversion of the thermal energy obtained by burning fuels such as: coal, natural gas, fuel, waste or biomass. These can be further classified as district heating plants (main purpose is heat and hot water production for an area, while the electricity generation is a byproduct) or thermoelectric power station (main purpose is electricity generation, while the production of heat is a technological byproduct).

Modern power plants are built using a combined steam-gas cycle, and cogeneration(tri-generation) by using the residual heat from the 1st technological process (1st generator is driven by the burned gases energy while the 2nd generator is driven by the steam pressure from the energy recovered and used to boil water). His process improves the efficiency to about 85% [1].

I.1.3.2 Nuclear power plants

The nuclear power plant represents a set of constructions and installations working together for the purpose of producing electricity and thermal energy, based on the controlled nuclear fission reaction.

The amount of energy in nuclear fuel (the term fuel being used by analogy because it does not burn but undergoes a fission process in the case of

energy production or fusion in the case of the most powerful nuclear weapons), is much higher than the energy contained in a similar mass of conventional fuel, this making nuclear fission a appealing source of energy [2].

I.1.3.3 Hydropower plant

A hydropower plant transforms the hydraulic energy produced by the movement of water into electricity, using a turbine.

The turbines represent the main component of such a power plant; these are connected by an axis to a generator, the electricity produced in this way being transmitted to a high voltage transformer, then through high voltage electrical lines to distributors and then consumers, through the National Energy System.

I.1.3.4 Solar energy

Solar energy represents the radiation of the Sun that reaches Earth, but only part of it reaches the ground while the rest is lost in the upper layers of the atmosphere (absorbed by it or reflected by clouds). This radiation can be converted to electrical energy by means of photovoltaic panels used in various implementations or in a concentrated solar power plant feasible in sunny areas.

Global warming is mainly caused by pollution, so more emphasis is directed for eco-friendly energy sources. Such an example con be Tesla which developed solar tiles to reduce the cost of construction; this design combines the role of weather protection of the roof with the generation of electricity, while offering a pleasing visual appearance because they cannot be distinguished from the classic tiles.

Economically speaking, photovoltaic panels return on investment (ROI) is reduced from the perspective of high cost and low power, which is backed-up by government through green certificates [3].

I.1.3.5 Wind power

The movement of air is caused by uneven heating (the equatorial zone receives more energy from the Sun than the polar zone), the warm air is less dense, rises and begins to move to the colder areas, thus this process is called wind.

Wind is a form of clean energy, used since ancient times by mankind for transportation (power-driven boats) and agriculture (for grinding cereals or irrigation).

The conversion of wind into mechanical energy and then into electrical energy is done by wind turbines. Thus, the wind drives the blades, fixed on the turbine shaft; this rotation motion (mechanical energy) is converted into electricity by an electric generator.

Romania has the highest wind power potential of all of continental Europe countries, (estimated at 14 GW); the region with the highest efficiency is Dobrogea, where most of the wind turbines in our country are installed [4].

I.2 Generator – distributor – consumer connection

I.2.1 Distribution and supplying electrical power in Romania

Electricity production must at all times be similar to the consumption of that period, in order not to destabilize the grid. This is why Transelectrica, the transmission and system operator of the electro energetic system in Romania, plays the role of administrator and operator of the electric transmission system, which also ensures the exchange of electricity between the countries of Central and Eastern Europe, as a member of ENTSO-E (European Network of Transmission System Operators for Electricity).

Transelectrica is the only operator that provides the electricity transmission service, the operational and technical management of the national power grid and the administration of the electricity market.

The electricity transmission grid represents a critical infrastructure of national and strategic interest and operates at a nominal line voltage greater than 110 kV (high voltage). According to the data published by the company, the operated infrastructure is:

- 81 electrical stations, as follows: one station at a voltage of 750 kV, 38 stations at a voltage of 400 kV, 42 stations at a voltage of 220 kV;
- 8834.4 km overhead power lines (of which interconnection lines - 486.2 km), as follows: 3.1 km at 750 kV, 4,915.2 km at 400 kV, 3,875.6 km at 220 kV, 40.4 km at 110 kV;
- 216 main transformer units, totaling 38058 MVA, as follows: 2 of 1250 MVA, 2 of 500 MVA, 22 of 400 MVA, 31 of 250 MVA, 81 of 200 MVA, 1 of 100 MVA, 2 of 63 MVA, 9 of 40 MVA, 24 of 25 MVA, 1 of 20 MVA, 32 of 16 MVA and 9 of 10 MVA.

Maintenance actions are planned considering the investment programs (refurbishment, modernization, development, replacement) and are correlated with them both at the stations and at the power lines. In the Electric Transport Network are performed maintenance services of preventive or corrective nature.

I.2.2 Romania as an actor on European energy system

Six regional groups were created within ENTSO-E, which develops the European power grid development. Transelectrica is part of the regional groups Continental Central-East and Continental South-East as an important player in the regional electricity markets.

The establishment of ENTSO-E as a cooperation group of the European Transmission System Operators aims to promote the completion and functioning of the internal market for electricity as well as cross-border energy trade. This aims to ensure optimal management, a coordinated exploitation and a positive technical evolution of the European electricity transmission network, established under the name „Ten Year Network Development Plan" - TYNDP.

I.2.3 Energetic strategy expectation

Analyzing the "Energy Strategy of Romania 2016 - 2030 with the perspective of the year 2050", comes the concept of Smart Grid that allows real-time control, bidirectional exchange of information and energy, with the instantaneous optimization of the production and consumption of energy.

It is expected that the interaction between the power grid, Internet and telecommunications networks will increase, enabling better energy efficiency and flexibility. New technologies will be adopted gradually, at a viable cost, with the protection of personal data and with a high degree of security in the face of cyber-attacks – an already increasing problem, with serious consequences, proportional to the faster and more profound adoption of information technology aspects into daily life.

Smart grid evolution will facilitate the consumer's transition to the role of **prosumer**, who generates a part of its electricity consumption and injects into the grid when he has an excess, while the national grid system operator balances demand and supply.

In the long term, this will have an impact on the network framework, especially when the prosumer also has a capacity of electricity storage, to limit the interaction with the network. The number of households without access to energy networks will also decrease, including through the adoption of micro-networks and autonomous solutions that will become more economically accessible, exempting the distributor of unprofitable investments, executed exclusively from the perspective of access to electricity for all consumers as a strategic objective of energy policy.

I.2.4 Analysis and forecasts of the Romanian Energy Regulatory Authority

National Energy Regulatory Authority (ANRE) represents the autonomous administrative authority, with legal personality, under parliamentary control, financed entirely from own revenues, independent decision-making, organizational and functional, having as activity object the elaboration, approval and monitoring of the application of the mandatory regulations at national level and necessary for the functioning of the electricity thermal and natural gas sectors and markets, under efficiency, competition, transparency and consumer protection.

According to ANRE, electrical energy distributors are:

- Electrica Furnizare;
- ENEL Energie;
- CEZ Vânzare rebranded in Distribuție Oltenia din 01.2017;
- E.ON Energie România, rebranded in Delgaz Grid.

II Identification of critical infrastructures parameters of the power systems and risk management

II.1 Critical infrastructures associated to power systems and the identification of their parameters

Electricity is the engine of contemporary society, but as demand is constantly growing, electricity production and distribution systems are running close to their peak, becoming more and more complex, being vulnerable to various risks, which can generate a cascading defects or black-outs, affecting the final consumer, related systems or even energy security of states.

There is a strong connection between the power grid, the environment, various risks and their management. Energy crisis and the effects of electro-energetic systems on the environment have led to the identification and analysis of risk factors, which has been and will continue to be a topic that many researchers around the world approach in their work.

Regarding risk management, we are talking about the systematic application of management policies, procedures and practices to **communication, consulting, context-setting activities, as well as identifying, analyzing, evaluating, treating, monitoring and reviewing risk**.

Approaching the risk as a function of probability and severity, in conjunction with the increasing dependence of the population, industry and especially most of critical infrastructures on the continuous access to electricity (supplied in quality parameters), the risk of a collapse of the electricity system has a high probability to engage chain malfunctions in the other critical infrastructures, an unacceptable situation in terms of consequences.

Physical security means the security of the power grid against physical attacks by individuals or organizations, with the intention of destroying its key points, interrupting its operation or stealing valuable parts (eg. copper conductors).

Cyber-security refers to the protection of the power system against threats regarding theft / destruction / manipulation of company data or customer information databases or the manipulation of sensors and equipment for the purpose of interrupting activity.

Although the two above mentioned are different, are also interconnected, as the risks are complex and an attack aimed at an electro-energetic critical infrastructure will be carried out on both planes simultaneously (for example the attacks in Ukraine developed further in the thesis).

Regarding technological developments in terms of the power network, it improves reliability but simultaneously opens new vulnerabilities in cases where (new) ways of remote access are added, or where redundancy is reduced.

Among the advantages of the technological evolution we find the possibility to simulate the operation of the equipment and implicitly the location and bug/flaw removal from the design phase as well as the improved automation that reduces the possibility of human errors occurrence.

The approach to the protection of critical infrastructures within NATO is different from that of the European Union, being viewed from the perspective of emergency services (civil protection), which is why common rules and norms are not established in this field.

National critical infrastructure is defined in EU Council Directive 114/2008/EC as "an asset, system or part thereof located in Member States which is essential for the maintenance of vital societal functions, health, safety, security, economic or social well-being of people, and the disruption or destruction of which would have a significant impact in a Member State as a result of the failure to maintain those functions".

Order 1178/2011 of the Minister of Economy, Trade and Business Environment for establishing sectoral criteria and critical thresholds related to the national / European critical infrastructure – Energetic sector identifies the critical infrastructures of power grids.

EU Council Directive above mentioned regulates activities in this sector with an approach that identifies and covers all risks, but gives priority to terrorist threats. According to it, human and natural disasters, as well as technological threats should be considered in the process of protecting critical infrastructures, but the fight against terrorism is the priority.

The concept of **resilience** has evolved considerably from Holling's fundamental definition (Holling, 1973) as a measure of a system's capacity to continue to function coping with changes in state, absorb disturbance and reorganize while maintaining the base identity, function and structure .

The key characteristics of the critical infrastructure resilience, originally designed by Stephen Flynn and defined later (2010) by the NIAC, are the following:

- **Adaptability** – how to absorb new lessons that can be drawn from an unwanted event. Revising plans, changing procedures and introduction of new tools and technologies needed to improve robustness, responsiveness and the rapid recovery before the next crisis;
- **Rapid recovery** – the ability to return to and / or restore normal operations as quickly and efficiently as possible after a break. This includes carefully prepared emergency plans, appropriate emergency operations, as well as how to have the necessary resources at the right place;
- **Resourcefulness (responsiveness)** – ability to properly prepare, respond and manage activities in the event of a crisis or disturbance: involves identifying how the crisis or disruption evolves, planning business continuity, training, supply chain management, prioritizing actions to control and mitigate damage and efficient communication;
- **Robustness** – the ability to maintain critical operations and functions in the face of crisis, reflected in physical building and infrastructure design (office buildings, power generation and distribution

structures) or in system redundancy and substitution (transportation, power grid, communications networks) [5].

Electricity is a type of energy crucial not only for the proper functioning, but even for the existence of the contemporary society; the power grid is subjected to various risks (predominantly natural causes, accidents or intentional malicious actions) whose occurrence can lead to serious disturbance of the operation of the system and propagating faults.

II.2 Modelling critical infrastructures associated to power systems

II.2.1 Smart Grid

National Institute of Standards and Technology (NIST) developed a model of upgraded, **Smart Grid**(artificial intelligence algorithms, IoT, extended communication), adapted to IT & telecom evolution, distributed into system and grid components. The constant evolution and changes of threats, globally and towards the electro-energetic critical infrastructures simultaneous to the evolution of its components demonstrate the importance of implementing the measures of reliability, safety in operation and interoperability from the design stage [6].

II.2.2 Microgrid

Contemporary power systems have heavily and just partially implemented new evolutions and technologies in electronics, automation, information technology and telecommunications. The evolution of electricity systems over time is presented, together with the trend of contemporary evolution towards the Smart Grid, based on decentralization and bidirectional exchange of energy and information.

The evolution from the traditional power grid based on a relatively small number of high-powerplants, towards decentralization and Smart Grid solutions improves resilience and eliminates the need for a category of generation (the one which functions only during the day to support peak consumption) by decentralizing part of the generation to the upgraded final consumers upgraded to prosumer status, microgrids, etc. (solar and wind solutions coupled with storage).

The basic feature of a microgrid is the possibility to operate in isolated mode when a malfunction occurs in the national power grid but also to protect it in the unlikely event that a malfunction occurred inside the microgrid, without allowing it to propagates into the national power grid and affects other users in a cascading sequence.

In addition to the protection against faults that can cause power outages, a microgrid relieves the national power grid of the peaks of consumption during the day by their own generation and storage solutions (photovoltaic panels, battery storage). Through bidirectional systems of telecommunications and energy management (EMS), users pay for their consumption and can take the best decisions according to the price dictated by the system load [7].

II.2.3 Power grid crisis

Global warming and pollution cause increasing illness while the extreme weather phenomena are increasing in severity and rate of occurrence, so the considerations related to environmental protection are increasingly present in our everyday life (awareness) and also in governmental regulations.

Automotive industry finally exceeded the area of electric concepts, manufacturers have understood that the near future of mobility is electric and the majority now have in their portfolio PHEV cars (hybrid that combines thermal and electric motorization, energy storage and regenerative breaking and of course the possibility to charge the battery an electrical outlet) while fully electric (EV) cars are in production or in final development by the majority of manufactures.

At the same time, authorities are increasingly taxing cars with internal combustion (from the perspective of pollution) while offering subsidies for purchasing "green" ones (the operation of electric cars does not involve emissions).

Modeling the nationally and EU interdependencies of critical infrastructures is needed, as well as awareness and classification of vulnerabilities, risks and threats in order to prevent crisis situations, such as:

- shortly after the 1977 earthquake affecting Romania, a power outage due to a human error propagated into the national power system, having important economic consequences;
- in 2005, extreme weather phenomena lead to a 5 days energy black-out in western Europe;
- in 2006 a fault in Germany propagated to another eleven European countries, leading to a cascading, affecting 15,000,000 people for 3 days;
- 2010 earthquake and 2016 hurricane in Haiti strongly affected the country, including the national power grid;
- in June 2019, a power outage affected ~ 48,000,000 people in South America (Argentina, Uruguay and partially Paraguay) due to extreme weather events;
- the most significant power outage in North America happened August 14, 2003, affecting 50,000,000 [8].

Sabotage, terrorism, or other criminal activities targeting power grids may produce results of a severity at least similar to North American black-out, unless appropriate safeguards are implemented.

We continue to present other cyber threats, which although at first glance seem less serious, are not visible or usually dealt with in the media, have the ability to be at least as dangerous as a terrorist attack or other physical attack.

Further on, we have extracted some cyber threats, which although at first glance seem less serious, are not visible or usually dealt with in the media, but have the ability to be extremely elusive and dangerous.

Malware gathers under 1 term all types of cyber threats, being an abbreviation from malicious software (software designed to infiltrate a computer system to damage the system, steal or encrypt data);

From sabotage perspective, in 2015 and 2016 Ukraine was subjected to advanced persistent threats – complex cyber-attacks, usually done by hostile country cyber-intelligence agencies where the aim is to infiltrate undetected in targeted systems, gain control, create back-doors to came back if detected and blocked, data theft, access grids framework and vulnerabilities in order to launch a successful attack at any given time.

Ukrainian power grid was subjected twice to such sabotage scenarios while Venezuela is facing a crisis, including frequent power outages in 2019.

Stuxnet is the first known type of malware classified as a cyber weapon. It was discovered in 2010 by Kaspersky specialists and it is believed to have been developed by USA & Israel cyberintelligence divisions targeting Iranian nuclear enrichment facilities by altering the spinners parameters in order to cause their physical destruction. It can be used against any type of industrial control systems or SCADA, such an advanced persistent threat being a risk for any digitalized critical infrastructures, including those in Romania.

One of the latest serious attacks on energetic critical infrastructure occurred at the end of 2017 by the means of the malware entitled **Triton** - developed specifically for attacking industrial control systems. It targets vulnerabilities on autonomous control systems manufactured by Schneider Electric (which independently monitors the status of critical systems) and automatically acts if it detects a dangerous situation [9].

NotPetya is the malware with the fastest infection rate and highest damage (~ $ 10,000,000,000), associated with Russian state agencies.

Lately, cybercriminals have approached a strategy to obtain funds by accessing and encrypting information, commonly called **ransomware** (malicious code that encrypts user data and requests an amount, usually in cryptocurrency to avoid anti money laundering policies, in exchange for the decryption code). Such an example for the year 2017 being titled **WannaCry** and for 2018 **GandCrab** in several versions, for all being developed free solutions by Bitdefender.

Many industrial control systems in use are designed in the ‘60s-‘90s, when no one considered these a cyberwarfare or cyber criminality target. Because these do not have security protocols implemented (authentication, encryption, etc.) are considered insecure.

A power grid is impossible to protect against all physical threats, given its size and the fact that certain targets are located in isolated or difficult to reach areas, at least at certain times of the year. Thus, as in the case of combating other forms of crime, the most effective method of protection is the **proactive collection of information** by the relevant structures, in conjunction with the action of law enforcement forces on the **prevention, deterrence and annihilation** of hostile

actions targeting energetical critical infrastructures before their plans can be effectively implemented.

Speaking about physical threats, a most eloquent case is the violent sabotage attempt that has already taken place in the United States of America on April 16, 2013; the attack, generically referred to as the "Metcalf sniper attack" hasn't reached its goal while the subject has been hardly treated mass-media, this is one of a severe gravity. The attackers previously cut fiber optics to make telecommunications impossible between the "Pacific" gas and electricity company Metcalf substation (Coyote, California) and authorities. Further, they opened fire on the 17 electrical transformers substation, which led to physical damage and leaking of electrotechnical cooling oil, overheating and going out of service [10].

This event indicates the ease in destabilizing a vital area of modern society - critical infrastructure (electricity).

The attackers would not have achieved such efficiency without inside information, so the Metcalf sniper attack cannot be considered a mere physical attack, but a hybrid one where the attackers exploited the vulnerabilities of the American power grid, with help from within (industrial espionage) or illegally accessing the cyber system of the electricity company (cyber-attack).

Our country faced a high-power transformer failure as I was able to identify in former national electricity company (RENEL) because of a technical malfunction which led to a fire and the loss of equipment. Nowadays, such a scenario can be deployed by a hostile state or organization, if appropriate cyberprotection measures aren't implemented and constantly updated.

In the documents extracted from the RENEL archive regarding the event produced in the station 400/110/20 kV Smârdan from Galați county on July 17, 1997, the explosion followed by fire is analyzed at transformer no. 2 (250 mVA, 400/110 kV).

Regarding the location and nature of the defect, the protections worked correctly and quickly isolated the defect and the fire protection system worked properly. The investigation of the event identifies the cause as a fault of the insulation of phase R (110 kV) above the transformer. The electric arc between the phase and the basin (the support phase of the phase R) created gases and an overpressure in the tank which had the effect of dislocating the 400 kV electrically insulating crossings, the R and S phases, with all the support panes, shearing the clamping screws and starting the fire.

II.3 Risk management in critical infrastructures. Ways to mitigate risk.

We can sort risks concerning Romanian power grid as:

a) natural:

- earthquake;
- landslide;

- extreme weather phenomena (extreme temperatures, floods, fire and draught, storms - wind and lightnings, gale to hurricane winds, supercell to tornado, heavy snow, avalanche);
- interference in the Earth's magnetic field (geomagnetic induced currents or de coronal mass ejection);

b) human related:

- work-related injury or human error;
- technologic wear;
- warfare (nuclear explosion or electromagnetic pulse weapon);
- malicious actions (terrorist attack, sabotage).

Romanian Government Decision no. 718/2011 regarding the approval of the National Strategy for the protection of critical infrastructures, defines 7 categories of vulnerabilities while the decision of the Prime Minister of Romania no. 166/2013 regarding Norms for the realization, equivalence or revision of the security plans of the owners / operators / administrators of national / European critical infrastructure identifies 7 categories of threats which are not fixed but adapt to the specific of the critical infrastructure, by analyzing its relevant elements, the technical details of the equipment, authorized users to operate directly or remotely, in order to identify the critical areas of the system.

Simultaneously with the development of electricity generation systems based on renewable sources, identical systems replicated on the order of thousands - hundreds of thousands, operated by intelligent communication devices, can be affected by a single threat. Security updates are an important component of cyber security, but they apply with delay and difficulty in the power system due to the diversity of the equipment.

The development of electricity generation systems based on renewable sources involved identical systems replicated up to hundreds of thousands, operated by intelligent communication devices, that can be affected by a single threat. Security updates are an important component of cyber security, but they apply with delay and difficulty in the power system due to the diversity of the equipment.

Regarding vulnerabilities caused by the remote operation of the assets through intelligent communications devices, the 2015 cyber-attack on the Ukrainian power grid focused on identifying the dispatchers and phishing for credential access SCADA platform, followed by malware installation to take over the remote-control operations and leaving back-doors to extend the return to normal operating status.

Weaknesses found following this attack are:

- Awareness of the phishing phenomenon and staff training in order to detect it, scan and filter emails, protected authenticating credentials to workstations;
- Properly configured and controlled network (connections);

- All communications are executed using encryption;
- Implementation of a back-up communications solution (also encrypted);
- Call-center filtering by source, in order to avoid DDoS (Designated Denial of Service);
- The physical possibility to stop remote asset management as well as for installing remote updates should be considered;
- Implementation of technical solutions to avoid the interruption of the electricity supply.

The risk and vulnerability assessment mentioned above is performed using a risk matrix.

The security and resilience of electrical critical infrastructure is a priority for the owners and operators as well as for the authorities, regarding the country's energy security.

In order to help organizations working with industrial control systems to identify potential vulnerabilities, experts from antivirus products "Kaspersky Lab" conducted an analysis based on information from public sources and Open Source Intelligence, for 2015.

In order to reduce the vulnerabilities of a cyber-attack, industrial control systems must operate in an isolated environment. In the industrial analysis mentioned above, 13,698 servers were identified through which industrial control systems are connected to the Internet. They belong to large organizations in various fields (energy, aerospace, transport, oil and natural gas, chemical, auto, food and beverage, etc.), critical infrastructure operators, government, financial and medical institutions and in 91.1 % of these cases were identified vulnerabilities that can be exploited remotely. **The most vulnerabilities in industrial control were man-machine interfaces, electrical devices and SCADA systems**.

In 2013 two United States researchers identified and documented cyber vulnerabilities in 20 critical infrastructure operators, which, if exploited, would have allowed a power grid black-out by changing the electrical parameters or switching off equipment that ensures the distribution of electricity.

USA Today presents 362 attacks on the power grid between 2011 - 2014, most of which being classified by unknown author. The Federal Energy Regulatory Commission (FERC) study of March 2014 draws attention to the fact that a successful attack on maximum 10 out of 55,000 in USA would cause a large black-out.

According to few extracted previous events or studies, the critical infrastructures are a target and there were already numerous cases of successful attacks. The explosion at a steelwork in Germany due to a cyber-attack was successful because it tricked the employees to open emails infected with malware which allowed the attackers to steal the authenticating credentials, changed the parameters of the technological processes, causing the blast of a furnace.

(Unencrypted) communications through Internet for industrial control systems presents advantages but raises many security problems, offering interested parties (cybercriminals, state or terrorist organizations, etc.) the possibility to remotely control vital components, which represents an unacceptable risk due to the high probability of occurrence and the serious consequences for the entire critical infrastructure.

The use of deep and dark web, encrypted communication apps available usually for free for everyone and payment methods in cryptocurrencies easily bring these cybercrime organizations within the reach of interested persons or organizations while make very difficult to identify and bring it to the court. Such organizations include global members who do not know each other in real life and live in different countries, a major cooperation effort for law enforcement institutions.

Kaspersky cybersecurity specialists predict, regarding the industrial domain (including Romanian power grid), the following trends:

- **A rise in targeted or accidental malware infection:** cybercriminals haven't yet discovered simple and reliable schemes to generate money from attacks on industrial control systems, the trend being to attack corporate networks while industrial IT systems are infected in most cases unintentionally, as a consequence of a weak cyber security culture instead of targeted malware;
- **High risk in targeted ransomware:** WannaCry/GandCrab shown that operational technologies are more vulnerable to attacks than computer systems and are often exposed to Internet access;
- **Targeted industrial espionage:** data theft regarding industrial control systems for the purpose of preparing and implementing attacks (ransomware to block the company's activity until it obtains money, or malware to gather industrial secrets and/or disrupt its activity);
- **A new type of crime arises, focused on the development of attack services and hacking tools:** there is an increase in demand on the black market for exploiting the vulnerabilities of industrial information systems, so the future trend is towards targeted attack campaigns;
- **New malware and advanced persistent threats:** Following Stuxnet model, new, complex forms of malware are developed with features such as the ability to remain inactive in the target computer network to avoid detection and will be used to target industrial networks and goods;
- **Cybercriminals will take advantage of the analyzes on the vulnerabilities of the industrial IT systems of control published by the security providers:** the cyber security specialists have identified and published data on various attacks on the industrial infrastructures regarding their operation and the exploited vulnerabilities. This approach allows for a better understanding and awareness of the phenomenon by those who may be targeted (including critical infrastructure operators in the field of electricity) but as a disadvantage

cybercriminal have better access to and understand industrial vulnerabilities and can develop specific, difficult or impossible to detect by present security solutions;

- **Cybersecurity regulation:** a first step to increasing protection and awareness of threats, vulnerabilities and how to protect against them;
- **Industrial insurance:** insurance policies against cyber risks becomes an integral part of risk management for industrial enterprises. Previously, the risk of a cyber security incident was excluded from insurance contracts, as was the risk of a terrorist attack. However, in order to be compensated, industrial operators have to meet certain requirements, which raises awareness among them and the measures taken will surely increase safety and resilience.

A complex, varied system is more difficult to globally destabilize while a modular system has the advantage of flexibility and in case of problems in key points (for example high power transformers) the affected parts can be quickly replaced, at lower costs, because the company allows to maintain a spare stock, with no high logistical costs due to the diversity of parts and manufacturers.

II.3.1 Natural risks

II.3.1.1 Earthquake

An earthquake is natural destructive phenomenon which at medium magnitudes interrupts the public utilities and at the large ones it causes extensive damage in the area, also to the power grid.

Romanian Government Decision 372/2004 for the approval of the National Program for Seismic Risk Management is the law while the seismological research falls within the attributions of the National Research-Development Institute for Earth Physics.

The institution defines earthquakes as natural phenomena caused by the release of energy inside the Earth, following the fracture of the rocks subjected to the stresses accumulated by them and the surface along which the rupture occurs and the displacement starts is called the fault plane.

II.3.1.2 Extreme weather phenomena

This section analyzes natural threats from a global, European and national perspective.

Romania is placed on the risk map in the middle field, at position 102 of 172 states, indicating a risk coefficient of 5.4618 [11].

According to the articles regarding the Italian power grid and the meteorological data (AccuWeather), floods represent the natural risk with the highest probability of occurrence, which produces maximum damages related to the gross domestic product in Romania.

The latest report of the World Meteorological Organization draws attention to the increasing socio-economic impact of global warming, which is constantly increasing due to greenhouse gases.

Regarding the security of the power grid, the climate changes caused by global warming have led to the manifestation of extreme weather phenomena with an accelerated rate of occurrence and gravity, which have produced even worse effects on each continent. Thus, in 2018 alone, approximately 62,000,000 people were affected by threats associated with extreme weather events or as a result of climate change.

Even though a dam collapsed recently (Laos), the most catastrophic event I could identify happened in 1975 in China. In response to severe flooding and to ensure electricity generation in the '50s, China built the Banqiao Dam (completed in 1952) in the Huai River basin in Henan Province, which collapsed because of design flaws at a catastrophic flooding and led to the breakdown of another 62 downstream dams.

Over 10,000,000 people throughout the region were badly injured, 26,000 people died from flooding and another 145,000 died from epidemics or famine, about 6,000,000 buildings collapsed and flooding affected over 1,000,000 hectares, but the conservative regime has covered up the tragedy, making it difficult to obtain data consistent with reality.

Currently in Romania, according to the Romanian Register of Great Dams, 246 such structures are registered, with heights of 5 - 168 m and with a volume of the lake from 100,000 m^3 to 2,400,000,000 m^3.

Analyzing the extreme weather events of the current year, a storm hit Halkidiki Greek peninsula July 11, 2019 and caused extensive damage to buildings, boats and infrastructure, more people lost their lives, including 2 Romanian citizens trapped under a building destroyed by the strong gale.

In the context of the extreme weather phenomena on the continent, Romania was also subjected to storms; thus, from the press releases of the National Meteorological Administration and the General Inspectorate for Emergency Situations, in the current year the high intensity wind associated with the storms (gale, hail, lightning) caused damage (roofs, cars, etc.) and among them we find electrical black-outs caused by breaking the overhead power lines.

The classifications of the destructive meteorological phenomena caused by wind are determined empirically by the Beaufort scale of the wind speed developed in 1805 from the perspective of its effects on the sea and subsequently adapted to the effects produced on the ground, according to the Royal Meteorological Society data. It has 12 positions, of which the most dangerous are classified:

- 9 – severe gale;
- 10 – storm (whole gale);
- 11 – violent storm;
- 12 – hurricane.

The Polytechnic University of Turin, with the support of the European Commission and the electricity distribution company "Terna" in Italy, has

developed a geo-referential model based on natural risks on the electricity distribution network.

The quoted models have the potential to be used cumulatively to improve resilience through risk analysis, planning, management, monitoring and consolidation of electricity distribution systems. Spatial analysis is useful for formulating scenarios, generation optimization, environmental impact and asset management.

II.3.1.3 Solar phenomena with interference in the Earth's magnetosphere

Induced geomagnetic currents are the representation at the ground level of the consequences of changes in the magnetosphere and ionosphere of the Earth due to solar explosions or nuclear fusion bombs detonated in the upper layers of the atmosphere [12].

The induced geomagnetic current flowing through the windings of a transformer produces an additional magnetization which, during the half-cycle when the magnetization of the alternating current is in the same direction can lead to the saturation of the ferromagnetic core of the transformer and cause the heating of their windings, with destructive potential.

This phenomenon leads to a sinusoidal form with harmonics, leads to losses through inefficient transmission and increased likelihood of erroneous triggering of automatic protection systems such as the situation in Canada - 1989 when a cascade interruption caused by a coronal mass ejection stopped the electricity supply for 6,000,000 people.

II.3.2 Human related risks

II.3.2.1 Nuclear energy

Fortunately, nuclear faults were rare events, but those strongly marked Earth and humanity. The International Nuclear and Radiological Event Scale was introduced in 1990 by the International Atomic Energy Agency in order to promptly communicate relevant safety information in the event of nuclear accidents [13].

Following the return to public attention of the Chernobyl nuclear disaster, Nuclearelectrica management announced that reactors 1 and 2 of the Cernavodă nuclear power plant have been built and are operating in accordance with principles of indepth protection, have a containment structure and the emergency shutdown of a reactor is maximum 2 seconds through 4 protection systems, of which 2 are independent of the central system; this security measures led to a good rating following an external audit.

Given that the Cernavodă nuclear power plant reactors 1 and 2 produces between 15-20% of the country's consumption and reactors 3 and 4 are partially built, I appreciate the opportunity to continue the completion of these reactors from the perspective of the country's energy security as well as Romanian status of mainly energy exporter (unfortunately, due to the legislative unpredictability, the

consequences of the Emergency Ordinance 114/2018 led, according to the data of the National Institute of Statistics, to increase the imports of electricity by 78.5% in the first quarter of 2019 compared to for the similar period of 2018); as for the choice of partners, the competent institutions of the state are to judge the opportunity not only from a financial perspective but also from a geopolitical and strategic perspective.

III Methods and protective measures for increasing the safety in operation of the power systems

III.1 The influence of risk factors on the power grid

III.1.1 Romania in the European electricity transmission system

III.1.1.1 National Electricity Transport Company Transelectrica and the National Energy Dispatcher

The National Energy Regulatory Authority (ANRE) was created in 1998 and is an autonomous administrative authority whose activity object is the elaboration, approval and monitoring of the application of mandatory regulations at national level, necessary for the functioning of the electricity sector and market under conditions of efficiency, competition, transparency and consumer protection.

Transelectrica manages and operates the electric electricity transmission system and also ensures the exchanges of electricity between the countries of Central and Eastern Europe, as ENTSO-E member.

III.1.1.2 Transport, distribution and supply voltages

Voltages have been standardized and the following are currently being used:

- **750 kV** – long-distance interconnection and transport **high-voltage**;
- **400 kV** – interconnection and transport **high-voltage**;
- **220 kV** – transport **high-voltage**;
- **110 kV** –distribution **high-voltage**;
- **20 kV** – local distribution **medium voltage**;
- **400/230V** – small business/receptors and household **low voltage**.

As a transmission operator, Transelectrica manages and operates the high voltage network (up to and including 110 kV - national critical infrastructure) and as a system operator it manages the operation of the national power grid, performing the system service through the National Energy Dispatcher [14].

III.1.1.3 System service, frequency adjustment systems

The system service is the one provided to maintain the safety in operation of the national power grid as well as the quality of electricity parameters according to the norms in effect. The functional system services are provided by Transelectrica and represent the current activity of the transmission system

operator, while the technological system services are provided by the users of the electrical transmission network (usually by the manufacturers) at the request of Transelectrica with the following resources as follows:

a) the primary frequency control systems;
b) the secondary frequency-power control systems;
c) power reserves;
d) local voltage adjusting systems;
e) automatic isolation systems on their own services and on self-starting the groups in order to restore the power to the national power grid after a zonal or global black-out;
f) dispatchable consumers that reduce their consumption or can be disconnected, at Transelectrica request.

III.1.1.4 National energy efficiency policy

Energy efficiency is regulated in Romania by Law 121/2014, which creates the legal framework for the elaboration and application of the national policy in the field of energy efficiency in order to reach the national objective of increasing energy efficiency, with a national target indicative of reducing energy consumption by 19% until 2020.

III.1.1.5 Electricity delivered in quality parameters

The quality of electricity can be analyzed from the perspective of supply voltage, supply service or commercial and requires the examination of the entire power chain: generation, transport, distribution, supply and use. The current norms that regulate the quality of the electricity are established according to the average damages in case of deviations from the quality indicators.

The quality of the electricity supply service is determined by the following factors:

- operational safety;
- the quality of electricity at the delimitation point between the consumer and the supplier;
- electromagnetic compatibility of the installations with their operating environment, in the common point of connection.

Depending on the responsibility of the decision, the quality indicators are classified as such:

A. Primary indicators (under the responsibility of the distribution operator):

a) *Product quality:*
- voltage - frequency (P – f adjustment);
- voltage amplitude (Q – U adjustment);
- voltage void (relay protection);
- power surge (appropriate protection systems).

b) *Service quality:* short(<3 minutes) or long interruptions.

The typical accepted interruptions are established by an agreement between the supplier and the final user.

B. Secondary indicators (refers to the disturbances caused by the end user and these are under its responsibility).

A. Primary adjustment reserve represents the power reserve that in case of frequency deviation (±200 mHz) from the reference value (50 Hz) will be mobilized automatically and completely in maximum 30 seconds, having the capacity to remain in operation for at least 15 minutes. Every company generating electrical energy are obliged to provide this service.

B. Secondary adjustment reserve will be fully and automatically mobilized in maximum 15 minutes, having to restore the primary one;

C. Tertiary adjustment reserve

- **fast** (maximum 15 minutes);
- **slow** (no more than 7 hours) [15].

III.1.1.6 Electromagnetic compatibility

Electromagnetic compatibility is the ability of systems or equipment to operate in the environment without suffering or causing unacceptable degradation of operation due to electromagnetic influences. In the International Electrotechnical Commission's acceptance electromagnetic compatibility represents their ability to function in their electromagnetic environment without inducing unacceptable disturbances in any other equipment or system existing in that environment.

III.1.2 Risk factors and their influence on the national power grid

III.1.2.1 The national power grid reliability and safety in operation

Automation and energy management systems involve major risks from attackers because all equipment is interconnected, covers a large area (including difficult or inaccessible under adverse weather conditions) and integrates data flows on monitoring, decision-making and executing actions necessary to maintain the frequency of the national power grid stable (50 Hz) and its integrity in any conditions, along the path of the electrical energy from source to final user.

Through this thesis we unequivocally acknowledge the great progress made possible by the implementation of new technological systems (IT, telecom, SCADA, EMS, etc.) and we want to draw attention to the vulnerabilities arising with the implementation of new technologies (5G, encrypted communications) so that the benefits (much improved response speed, instantaneous location of any error) / interruptions, automatic protection systems, flexibility, etc.) don't introduce new vulnerabilities with serious consequences.

Connectivity between all the structures that make up the national power grid integrates advanced digital functions in the field of telecommunications and information technology that aim at its evolution towards the Smart Grid in order to

gain sustainability, flexibility and resilience facing new threats, especially those regarding cybersecurity.

An efficient example of the decentralization of the Power Grid is Denmark, while the forecasted evolution of Romanian Power Grid towards the transition to Smart Grid is presented by Transelectrica. This transition, from a traditional (one-way energy flow from generator to final user) power grid to the Smart one is based on bidirectional energy and telecommunications flows [16].

III.1.2.2 Risks and vulnerabilities of the national power grid from the perspective of supervisory control and data acquisition systems

A. SCADA in regulatory perspective

Regarding industrial automation, I have approached DCS, SCADA and EMS as being representative for the technological processes of any electricity critical infrastructure.

Distributed control systems (**DCS**) are commonly used in a process, equipment or plant, usually with a large number of control loops, in which stand-alone controllers are distributed throughout the system, but there is central control over the system (a human dispatcher). These increase the reliability and reduce the installation costs by locating the control functions near the technological process, installation, plant, etc. with centralized on-site monitoring and surveillance and are preferred in areas where safety and reliability are a priority.

Energy management systems (**EMS**) monitor, control and optimize energy use using physical components (hardware) to collect energy consumption data and software applications to read and analyze this data in order to provide an image of a building's energy consumption and highlights areas for efficiency improvement. With increasingly intelligent systems, EMS are moving towards greater control and optimization of energy in civil and industrial applications.

Supervisory control and data acquisition (**SCADA**) are commonly used for large environments, which can be dispersed over a given geographical area. These include a command center that monitors and controls an entire technological process, a distribution system, a plant, etc. and most of the operations are performed automatically by the Remote Terminal Units (RTU) or by Programmable Logic Controllers (PLC) while in the command center, management decisions are based on the human-machine (graphic) interface of SCADA [17].

Transelectrica admits the need to implement a new EMS/SCADA solution in the near future, using the telecommunications and information technology capabilities of the present. The strategic modernization option includes:

- setting up a dedicated structure for preventing, analyzing, identifying and responding to cyber security incidents;
- adapting the new EMS/SCADA according to the security requirements in the field of critical infrastructures (NERC CIP) and the latest specific security standards (IEC 62351, ISO/IEC 27001);
- implementation of secure communication;

- upgrade to Smart Grid approach.

Industrial automation evolved from a few locally built implementations, to nowadays complex systems, with standardized hardware and software (in the way of construction based on components built in assembly line regime and marketed as a mainstream product/service not unique, adapted to each companies' specification). This approach is more economically feasible and appropriate for a high demand product bat also makes the system's component open to anyone to easily find details, making digitalized, interconnected critical infrastructures vulnerable to cyber threats that are increasingly present and effective today.

SCADA was not designed using encryption methods (as it was considered to be a closed loop), so once an attacker managed to establish an entry point to the system and hack the authentication process (if any), it can steal information and cause damage, for example by overwriting the security limits or by sending a false data (for example, it can alter the voltage or frequency parameters in an electrical equipment, following the automatic control systems or the service operators to decouple the targeted areas of the attacker from the power supply, or even cause the destruction of the equipment).

From a legal point of view, in Romania the security of the information systems of EMS/SCADA is treated in the Energy Security Strategy and requires the adaptation of the frameworks of these systems according to the security requirements of the field of critical infrastructures (NERC CIP) and the latest security standards specific to the EMS / SCADA process systems (IEC 62351, ISO/IEC 27001).

The document specifies the need to set up a dedicated organizational structure for the prevention, analysis, identification and response to cyber security incidents of computer systems from the aforementioned systems and from other systems associated with critical infrastructures. This structure is to implement the objectives and directions of action provided in the national legal basis, respectively Romanian Government Decision no. 271/2013 for approving the Cyber Security Strategy of Romania and the National Action Plan on the implementation of the National Cyber Security System.

B. Regulations and practice examples of supervisory control and data acquisition systems

Modern SCADA/EMS replace the manual labor force to perform manual processes in distribution systems through automated equipment. The implementation of such systems increases the efficiency of the energy distribution system by providing functions such as real-time visualization of operations, system dynamics, data recording, maintaining the desired voltages, currents, power factor and frequency as well as generating warnings in situations that exceed the normal pre-determined parameters.

SCADA/EMS perform automatic monitoring, protection and control of various equipment in distribution systems using remote-controlled intelligent

electronic devices (RTUs). Their purpose is to restore the electricity supply service during a fault, but above all, as we have detailed above, it is aimed at locating a potential fault and taking the necessary measures to prevent it before it occurs, in order to maintain normal operating conditions [18].

C. SCADA cyber security framework

The cyber security framework of modern SCADA is classified by Jacob Brodsky and Robert Radvanovsky in the Handbook of SCADA/Control Systems Security, according to the following categories, while the architecture of a cyber security system is described in the US regulations:

1. Knowledge/expertise of the security structure;
2. Capabilities of potential opponents;
3. Proper access/authenticate;
4. Vulnerabilities;
5. Possible damages;
6. Detection;
7. Recovery.

D. Cyber threats

An attacker will try all possible ways to get into the system, searching for devices that have integrated antennas and wireless network processors to hack an access point through those devices that have already been identified with security breaches and haven't yet updated to the necessary security patches [19].

III.2 Methods and measures to protect the power grid

III.2.1 Cyber security as a national security threat in Romania and within strategic partners

- Romanian Cyber Defense Command Structure (CApC- Defence Staff);
- National Cyber Security Incident Response Center (CERT-RO);
- National Centre for Coordination of Critical Infrastructure Protection (CCPIC);
- National Cyberintelligence Center (SRI);
- The Operational Response Centre for Security Incidents (CORIS-STS);
- North Atlantic Treaty Organization (NATO) Cooperative Cyber Defence Centre of Excellence (CCDCOE);
- NATO Communications and Information Agency's (NCI Agency);
- United States Federal Bureau of Investigation (FBI) Cyber Division;
- Cybersecurity Directorate, Central Security Service within United States National Security Agency (NSA);

- United States Department of Homeland Security, Cybersecurity and Infrastructure Security Agency (CISA);
- The European Union Agency for Cybersecurity (ENISA).

III.2.2 Cryptographic systems for secure communications

Previously, we have identified a vulnerability in the industrial automation that could be easily exploited by an attacker and we propose to solve it by securing the communications between the components of EMS/SCADA; Here are some solutions simple or more complex, depending on the desired level of protection.

Regarding cybersecurity, we are approaching encryption through 3 basic characteristics:

- **Availability** (data accessible at any given time);
- **Integrity** (unaltered data from source to receiver);
- **Confidentiality** (data intelligible only to desired receiver) [20];

and also, on the following subsequent features but no less important:

- **Authentication** (a method of verifying the user's identity and subsequent establishing if he has access to that information);
- **Responsibility** (any type of action on the information can be associated with the responsible person);
- **Authenticity or identity assurance** (original data, not something different made to resemble the original);
- **Non-repudiation** (the sender receives the proof of delivery and the receiver receives the proof of the identity of the sender; thus, no one can claim that not processing the information);
- **Reliability** (desired behavior and results) [21].

Cryptography derives its name from ancient Greece, where *kryptos* means hidden and *graph*e refers to writing and is the branch of mathematical science that deals with the development of ciphered (numerical) systems by which the initial information is intended to be incomprehensible to anyone other than sender and receiver.

Decryption is the reverse process of encryption, provided that you know the system and the encryption key, while **deciphering** is the process of analyzing ciphertext in those situations where the system and encryption keys are unknown, in order to transform the information in their original, intelligible form. The science that deals with the decryption is called **cryptanalysis** and together with **cryptography** it forms the **cryptology** [22].

III.2.2.1 Substitution ciphering

- **Caesar code** (Caesar cipher, Caesar displacement or cipher);
- **Vigenere Cipher** is an evolution of Caesar cipher being now easy to decipher evolved to
- **Polyalphabetic substitution cipher.**

III.2.2.2 Transposition cipher

In cryptography, transpositions refer to the encryption methods where positions held by text units are moved according to a predefined system, so that the encrypted text is a permutation of the plain text, in particular the characters of the visual text are rearranged to generate the encrypted text.

III.2.2.3 Current cryptographic methods

A. Symmetric key encryption

Symmetric encryption uses the same key for both encryption and decryption, called *PSK* – Pre-Shared Key:

- ***DES*** (***Data Encryption Standard*** 56 bit key) and ***3DES***;
- ***Blowfish***;
- ***AES*** **(*Advanced Encryption Standard*)** [23].

B. Asymmetric encryption

Asymmetric encryption offers much greater complexity, offers superior security but also needs greater computing resources as the significant difference from symmetric encryption is the use of an additional (private) key as follows:

In order to maintain **data confidentiality**, it is encrypted by the public key and decrypted by the private key;

In order to **authenticate**, it is encrypted by the private key and decrypted by the public key, the result being the digital signature;

Of the asymmetric encryption algorithms, the most used are:

- ***RSA***;
- ***DSA*** (*Digital Signature Algori*thm);
- ***DH*** *(Diffie-Hellman key exchange)*;
- ***ECC*** **(***Elliptic Curve Cryptography)* [24].

C. Hash, the integrity function

Data confidentiality has been previously presented in various ways following the known (encryption was and is a basic military advantage used in every country diplomatic and military area, being classified top secret) course of this discipline throughout history, but we need the encrypted data to arrive without modifications (partial loss of data or changes of content) from sender to receiver. For this purpose (ensuring **data integrity**) were developed algorithms named **hash** functions. When the sender transmits data to the receiver, the hash generates (mathematically) a unique, one-way identification code that is also sent to the receiver. Once the data has reached the receiver, it recalculates the unique identification code and if the two are identical, the data has reached the destination without affecting their integrity [25].

D. Internet Cryptographic protocols

Hyper Text Transfer Protocol is used to access information from the World Wide Web; to secure this transmission of information one can use:

- **Secure Hyper Text Transfer Protocol** (S-HTTP);

- **Hyper Text Transfer Protocol Secure** (HTPPS) [26].

III.2.2.4 Encrypted systems currently used for telecommunications (text, voice, images, video, documents) over the Internet

Privacy in the digital world has led to the encryption of mobile communications, via the Internet and the most popular solutions in this field, encrypted along the way or designed initially with high privacy privileges are:

A. ***WhatsApp***
B. ***Telegram***
C. ***Threema***
D. ***Signal***
E. **Virtual Private Network (VPN)** [27]
F. **Blockchain** solutions [28]

IV Simulation and modeling the influence of risk factors

IV.1 Management analysis

SWOT analysis, acronyms for **strengths(S), weaknesses(W), opportunities(O)** and **threats(T)** for an electricity critical infrastructure [29]:

	Positive	**Dangerous**
The internal circumstance of the organization	**S** **STRENGTHS**	**W** **WEAKNESSES**
	What are we best at	What are we needing most as improvement
	Available financial resources	Financial needs
	Staff professional level	Training needed for employees
	Strategy to attract and maintain quality human resources	How do employees report to the company in terms of satisfaction
	Technologies available and in use	Past errors
		Measures to avoid similar errors
		Any lacking new, needed and trusted technologies
External circumstance	**O** **OPPORTUNITIES**	**T** **THREATS**
	Environmental changes to be exploited	Knowledge of competition
	Knowledge of the user's consumption habits constantly adapting to market dynamics	Extensive, trusted testing of new technologies before implementation
	Known weaknesses of competitors	Anticipation of competition approaches in our detriment
	Healthy work environment and	Parting of skilled workers

	appropriate payment	
	Business continuity plan, service delivery and operations	Vulnerable areas to physical attacks
	Recovery plan following a disaster	Vulnerabilities to natural disasters and extreme weather phenomena
	Response plan following a security incident	Systems, networks and components vulnerable to cyber-attack
	Strong IT department with dedicated cybersecurity specialists	Lack of updating security policies for known fixes and vulnerabilities
		Personnel non-compliance with cyber security guidelines
		Delayed security updating to recent solutions regarding identified vulnerabilities
		Unsecured remote access devices in supervisory control and data acquisition
	Collaboration with specialized state agencies, academic researchers and cybersecurity companies	Wide availability and easy access of technical information about SCADA
	Opportunities for implementation new physical or cyber technologies	Tested the integrity and security policies of partners, suppliers, and those providing outsourced services in order to identify threats and vulnerabilities
	How, where and in what way can we be one step ahead of attackers and competition by implementing *Blockchain* technologies	

IV.2 Components of the national power grid as presumptive targets for a hostile entity

IV.2.1 Automatic transfer switch (ATS)

An automatic transfer switch known (ATS) is a device part of electrical installations and serves to transfer electricity automatically from the primary source to a backup source if it detects a fault at the primary source or another interruption/modification of the energy parameters at the primary source [30].

IV.2.2 Electrical transformer

The transformer is a static electromagnetic device that transforms the parameters of the electrical energy (usually the voltage) from the primary circuit into the secondary circuit, based on the law of electromagnetic induction. The alternating current in the primary circuit crosses the primary winding and produces a magnetic field in the ferrous core, which in turn produces alternating electrical voltage in the secondary winding [31].

IV.3 Case study

IV.3.1.1 Hypothesis

In the content of the latest version at the time of writing the thesis (Transmission Electricity Network Development Plan 2018-2027) Transelectrica offers a list of 80 high-power transformers (table 8.8), the type of construction, the factory and the year of manufacture, the substation location and the technical situation. The document concludes the urgent need for refurbishment or replacement in case of some equipment (like the transformer 110kV-20kV produced in 1976, in technical poor condition - 32%).

In conjunction with the details of EMS/SCADA system and telecommunications infrastructure available on-line, without hardly any effort an interested attacker (individual or hostile organization) obtains easy, fast, open-source useful information that is helpful in choosing a target and planning a successful attack be it physical, cyber or combined as hybrid warfare evolved nowadays.

As a risk scenario, we have chosen to implement such an attack, aiming to change the electrical parameters of a substation and to model the effects of this attack. Fire protection systems in the case of a power transformer, oil-cooled (also known as electrotechnical oil or transformer oil) can be with a gas relay (Buchholz) or a modern inert gas extinguishing system [32].

For the case study we have chosen a 20kV-400V medium to low voltage substation where through a successful cyber-attack, one of the transformers is overloaded. Because of this, the insulation fails and creates an electric arc, with a temperature between 4000 -20000℃. From the technical data sheet available on the manufacturer's website, we have chosen as an example a mineral oil that has a flash point at 170 ^{O}C, the self-ignition temperature at 280℃ and the specific heat (the amount of heat required for a body for which 1 kg of its mass changes to with a degree) of 1860J/kg* ^{O}K.

Due to the temperature of the electric arc, the oil vaporizes and creates a pressure wave that propagates with ~1200m/s into the transformer tank and can cause it to break. The gas relay (Buchholz) is inefficient at a sudden increase in pressure, while the aforementioned inert gas detection, signaling, warning and extinguishing system has been designed to minimize the impact of this phenomenon, by integration of an expansion vessel for the oil transformed into

gaseous state and an extinguishing system with inert gases, to suppress the fire resulted from the combustion of the oil in the gaseous state and the heat of the electric arc [33].

The case study consists of 3 components, as follows:

- a hypothetical model for the location of the substation serving a neighborhood consisting of residential, technological and relaxation areas;
- the characteristics of a fire produced at one of the transformers of the substation described above;
- modeling of electrical parameters;
- the practical example of methods of encrypting electrical parameters.

IV.3.1.2 The location of the electric substation

We have developed a model of an Area Town Planning using the SketchUp online application and the open source 3D Warehouse resources that includes mixed functions such as housing, production spaces, traffic and transport services, public education, health institutions and emergency services, shopping and recreation areas, according to figure 1.

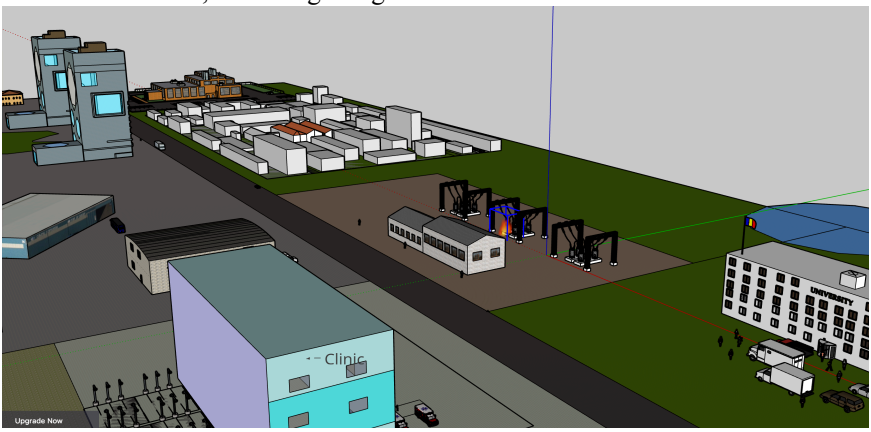

Fig. 1. Area Town Planning as case study centered on substation

IV.3.1.3 Data resulting from fire modeling at a substation transformer

We have created, using dedicated fire simulation software (PyroSim) and with the help of the open-source resources GrabCAD community, a model of an electric substation (ground level and 2 floors with 5 rooms at each level).

We have placed 3 (medium to low voltage) transformers at 4 meters from the facade of the building and 10 meters away one from each other. We have chosen transformer no. 2 (middle) (2.75*2*1.85 m) around which we have created a mesh of 500,000 cells (a mesh of small geometric objects around the transformer subjected to modeling in order to have a finite surface on which the software will

perform calculations and through which it will graphically display computational fluid dynamics- CFD). At each floor we have applied 8 thermocouples on the facade while at ground floor we have applied 4 thermocouples inside the room, according to figure 2.

For a real-life possible situation and in order to aggravate the consequences of this scenario, we have set the wind speed blowing from the transformer to the substation building at 6.4 m/s (25 Pascal).

Adapting the scenario to the possibilities of the software, we have considered the transformer tank broken as a result of the shock wave, the oil starting to leak towards the ground where it ignites on a surface equal to the transformer's footprint (burner).

In order to run this simulation, we have set the software to indicate the release of smoke and flames, from which we have extracted several screenshots (quantitative simulation) presented in figures 3 and 4 in order to visually present the effects of the fire on the transformer and its possible evolution towards the substation building (the building is considered fireproof, to reduce the render time and because a modelled fire at the building isn't a subject for the electrical reference of the thesis).

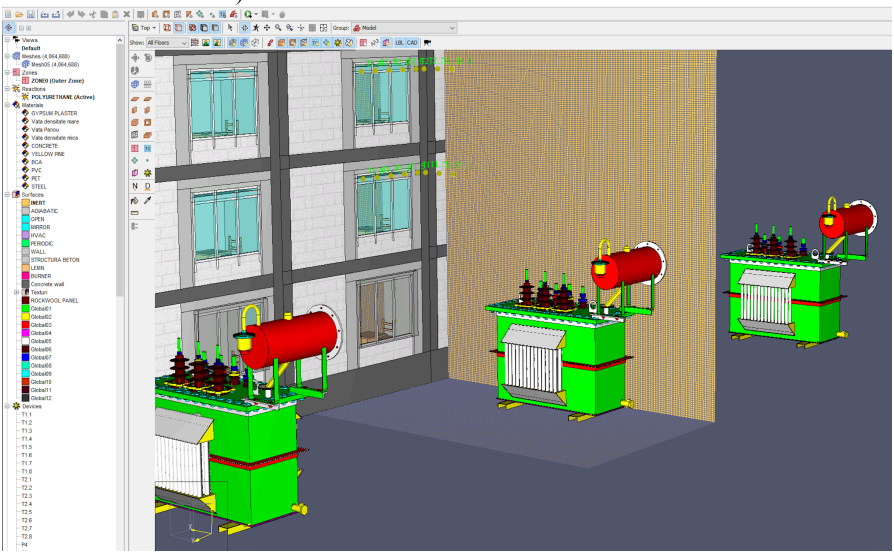

Fig. 2. Mesh and thermocouples for simulating fire at transformer no.2

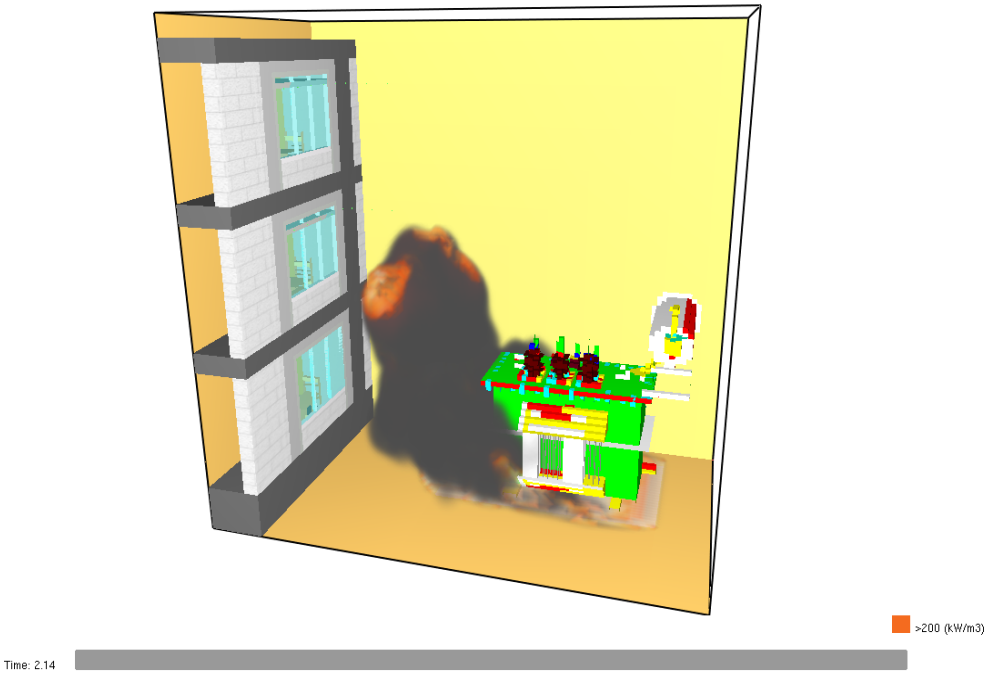

Fig. 3. Generalized fire (quantitative)

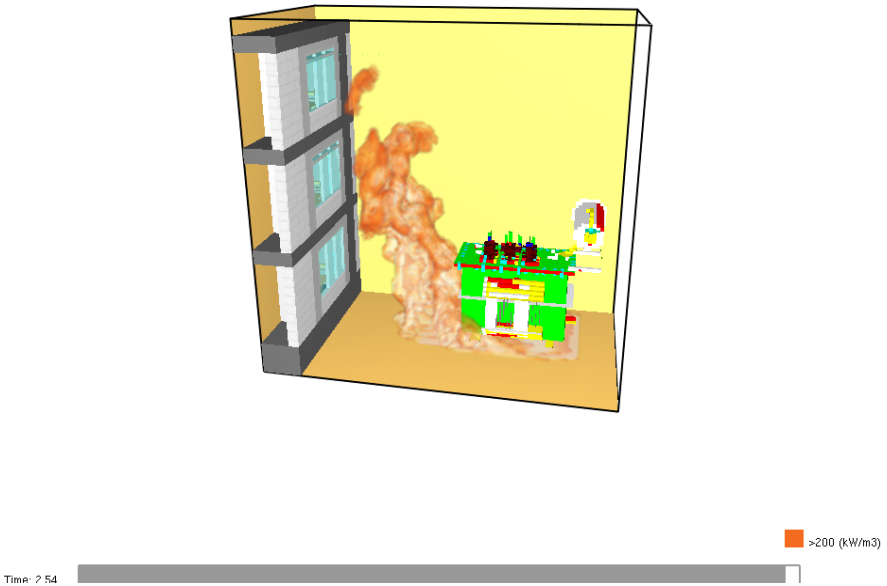

Fig. 4. Development of the fire towards the building with the presentation of the flames and with the smoke removed (quantitative)

For the purpose of a simulation that presents **qualitatively** the results of the scenario presented above, we have extracted and presented in Figures 5-9 the results of the first 627 seconds of a fire simulation that would have been extinguished by complete combustion in 10 hours (transformer only, also no fire development towards the building) without extinguishing measures been taken.

Unlike the previous quantitative approach that returned results in a few minutes, this realistic one took 2 weeks of computational fluids dynamics on a specialized computer. For the realistic simulation we have considered the following parameters: 1600kg of electrotechnical oil that after the tank breaks would spill on a surface of $2m^2$, it has a caloric capacity of 46,000kJ/kg, it releases a total energy of 73,600MJ and a heat release rate of 2045kW.

The substation building was considered inert (they do not react, do not transfer heat and do not catch fire due to the thermal transfer from the transformer). We have chosen this approach due to the unreasonable computation time as well as due to the topic of interest for the thesis, in particular the physical effects of a cyber-attack on a transformer as an exploitable vulnerability of an important component in the national power grid as critical infrastructure.

The oil leaks through a gap in the transformer housing and contacting the oxygen in atmosphere it ignites due to the high temperature.

Figure 5 presents the evolution of the fire with hidden flames in the dense smoke as a danger that a transformer presents in case of fire for the occupants of the nearby buildings. In this situation, any open window would lead to a serious danger of suffocation. The initial setting of the simulation presents a 20 km/h wind blowing from the transformer to the substation building, which pushes smoke and flames, increasing the temperature and also the risk of fire, which makes the situation more dangerous but also more realistic.

The height of the flames can be seen in figure 6 with a dangerous height of two floors (~ 6m), presenting a high risk of spreading the fire to the neighborhoods and a difficult fire to extinguish.

The temperature of the burned transformer and the surrounding area is shown in figure 7 and can reach 720°C, represented by red. It's a high temperature, considering that the ignition temperature of wood is around 250°C).

An air flow mixed with combustion gases is shown in Figure 8 while the temperature of a thermocouple from the 1st floor facade is presented in Figure 9.

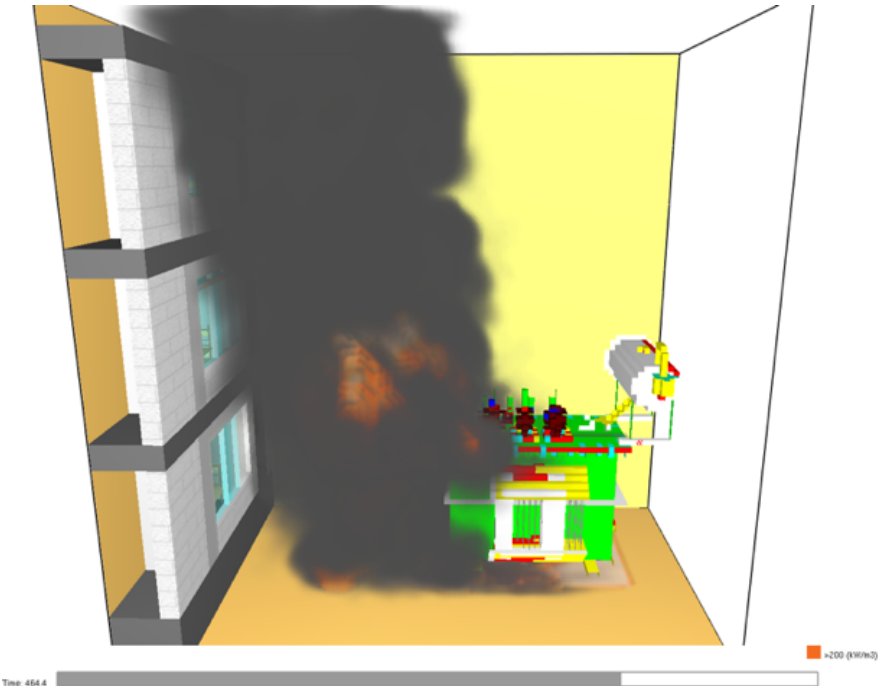

Fig. 5. Development of fire with flames and smoke (qualitative)

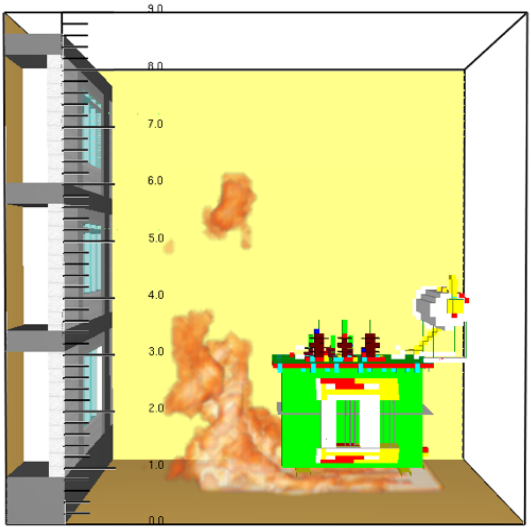

Fig. 6. The height reached by flames in the case of qualitative simulation

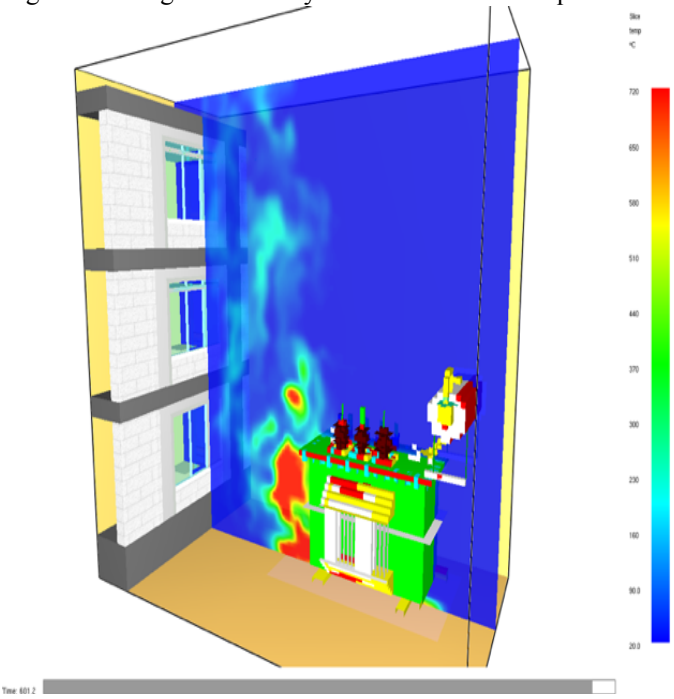

Fig. 7. The fire developed temperatures with qualitative simulation parameters

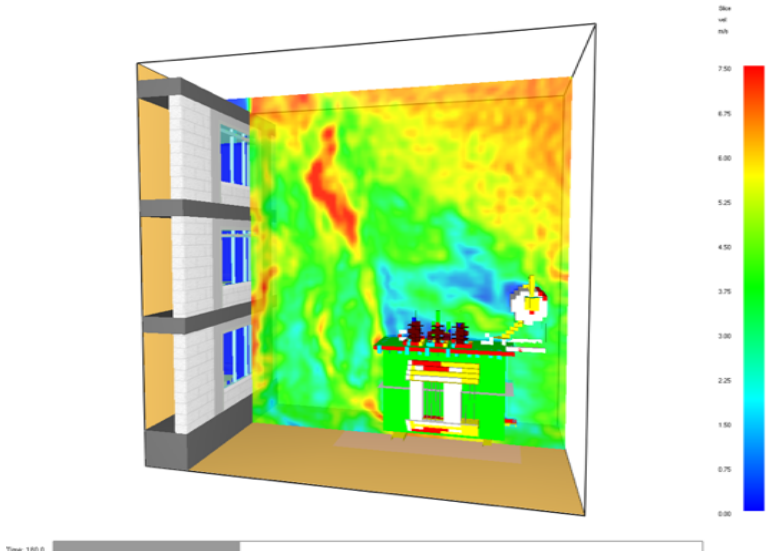

Fig. 8. Qualitative modeling of fire: air and combustion gases flow

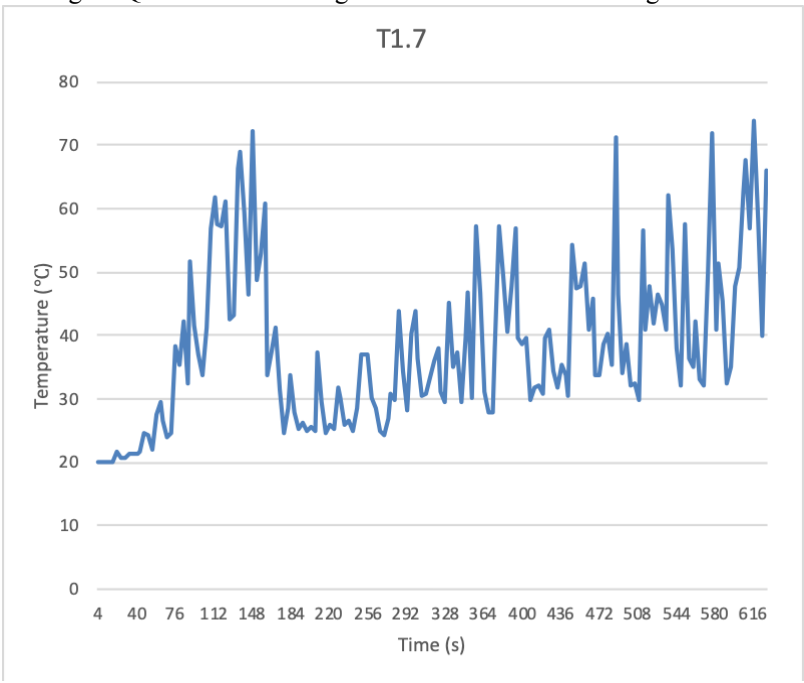

Fig. 9. Qualitative modeling of the temperature on the 1st floor facade

The cyber-attack that caused the modeled situation would have caused physical damage until the attackers were identified in the system, their access right was revoked and the modifications made were corrected, in conjunction with the firefighters extinguishing the fire; Indirect damages would have been caused by the black-out affecting consumers in the area, so a larger substation implies more serious consequences.

A prompt and efficient response of competent authorities and electrical company specialists would mean for a medium to low voltage substation that the power resumption within a few hours and a cost generated by the replacement of the affected transformer. For a high voltage substation (critical infrastructure), the consequences would be serious, as high-power transformers are expensive and electrical companies don't usually keep spare transformers. A combined attack on a few, well-chosen such substations could mean a cascading effect blackout for a country, unable to be quickly fixed. The situation modeled above is supported by many factors extracting a few such as:

- the precarious situation of such electric machines, briefly presented before;
- digitalization and cyber vulnerabilities;
- several transformers malfunctions that have developed into fires, leading to the destruction of the equipment, (Smârdan -1997, recently in figure 10 the most recent case of fire at a transformer in Romania leading to a city black-out and railway transport halting in Adjud on 09.07.2019) [34];
- malfunctions at 2 high-power transformers of the British transport operator led to a black-out at peak hours on 09.08.2019, in south-east England including London, affecting road and rail traffic;
- A fire at a transformer led to a black-out in Manhattan (New York City) on July 13, 2019;
- defects statistics for the 2017-2018 made available for 7 of the counties in which the undisclosed Romanian distribution is present.

Fig. 10. Recent fire at a transformer in Adjud, Vrancea, Romania

IV.3.1.4 Electrical parameters modeling for the transformer subjected to the attack in the previous simulation

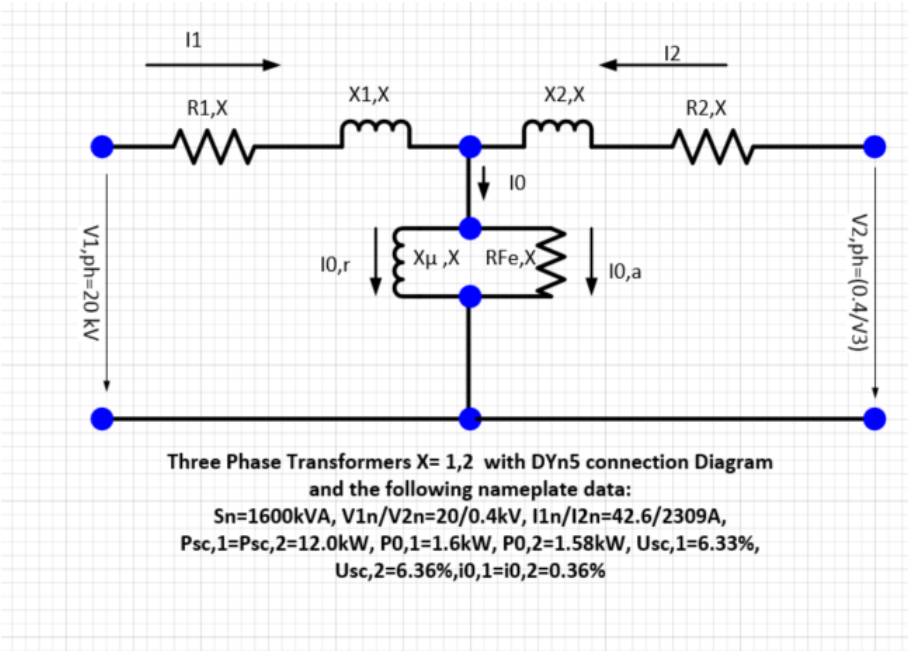

Fig. 11. The equivalent phase circuit of the three-phase transformer

A. Determining the **R1,X, R2,X, X1,X, X2,X** parameters from the short circuit data

Let's consider two three phase medium power transformers T1 and T2, with the equivalent circuit and nominal data provided in fig. 11 - showing the diagram and parameters of the three-phase transformer; Because the primary winding connection is D (DELTA), then $I_1=I_{1,ph}=I_{1n}/\sqrt{3}$ whereas $V_{1,ph}=V_{1n}$. X=1,2 are the indexes associated with transformers 1, respectively 2.

- R1,X; X1,X – the resistance respectively the reactance of the primary winding;
- R2,X; X2,X – the resistance respectively the reactance of the secondary winding regarding the primary winding;
- RkX- total short circuit resistance;
- RkX=R1,X + R2,X;
- XkX- total short circuit reactance;
- XkX=X1,X + X2,X.

The absolute values of the short-circuit voltages of the two transformers:

- Usc1[V]=usck1[%] x V1n/100 = 6.33 x 20000V/100=1266V;
- Usc2[V]=usc2[%] x V1n/100 = 6.36 x 20000V/100=1272V.

Short-circuit resistance/phase of the transformers:

- Rk1=Psc,1/(3 x $I1^2$)=12000W/(3X(46.2/√3)^2)=5.622Ω=Rk2;
- R1,1=R2,1=Rk1/2=2.811Ω;
- R1,2=R2,2=Rk2/2=2.811Ω.

Short-circuit impedance/phase of the transformers:

- Zk1=Usc1[V]/I1=1266/(46.2/√3)=47.46Ω;
- Zk2=Usc2[V]/I1=1272/(46.2/√3)=47.68Ω.

Total reactance/phase:

- Xk1= ($Zk1^2$-$Rk1^2$)$^{1/2}$=47.126Ω;
- Xk2= ($Zk2^2$-$Rk1^2$)$^{1/2}$=47.347Ω.

Phase reactance of transformers:

- X1,1=X2,1=Xk1/2=23.563Ω;
- X1,2=X2,2=Xk1/2=23.6735Ω.

B. Determining the **RFe,X** and **Xμ,X** parameters from the open circuit data for the two transformers

Active component of the open circuit current:

- i0a,1=P0,1/(3 x V1,ph)=1600W/(3 x 20000V)=0.0267A;
- i0a,2=P0,2/(3 x V1,ph)=1580W/(3 x 20000V)=0.0263A.

Equivalent resistances corresponding to core losses:

- RFe,1=V1,ph/I0a,1=749.065kΩ;
- RFe,2=V1,ph/I0a,2=760.456kΩ.

Reactive component of the open circuit current:

- i0r,1=($i0,1^2$-$i0a,1^2$)$^{1/2}$=(0.36*(46.2/√3)/100)^2-0.0267^2)$^{1/2}$=0.0922A;
- i0r,2=($i0,2^2$-$i0a,1^2$)$^{1/2}$=(0.36*(46.2/√3)/100)^2-0.0263^2)$^{1/2}$=0.0924A.

Equivalent reactances corresponding to core magnetization:

- Xμ,1=V1,ph/I0r,1=216.920kΩ;
- Xμ,2=V1,ph/I0r,2=216.450kΩ.

In addition, the intrinsic values (without referring to the primary winding) of the parameters of the secondary winding can be determined using the transformation correlations:

- r2,1=R2,1 x (V2,ph/V1,ph)^2=2.811Ω x [(0.4/√3)/20]^2=0.0003748Ω;

- r2,2=R2,2 x (V2,ph/V1,ph)^2=2.811Ω x [(0.4/√3)/20]^2=0.0003748Ω;
- x2,1=X2,1 x (V2,ph/V1,ph)^2=23.563Ω x [(0.4/√3)/20]^2=0.003142Ω;
- x2,2=X2,2 x (V2,ph/V1,ph)^2=23.6735Ω x [(0.4/√3)/20]^2=0.003156Ω.

The results are summarized according to tables VI and VII, presented below:

Table I. Analytical calculation of the parameters for transformer no.1

R1,1[Ω]	X1,1[Ω]	R2,1[Ω]	X2,1[Ω]	Xμ,1[Ω]	RFe,1[Ω]
2.811	23.563	2.811	23.563	216920	749065

Table II. Analytical calculation of the parameters for transformer no.2

R2,1[Ω]	X2,1[Ω]	R2,2[Ω]	X2,2[Ω]	Xμ,2[Ω]	RFe,2[Ω]
2.811	23.6735	2.811	23.6735	216450	749456

C. Electrical power system analysis software-modelling [35]

Transformer no.1 (T1)

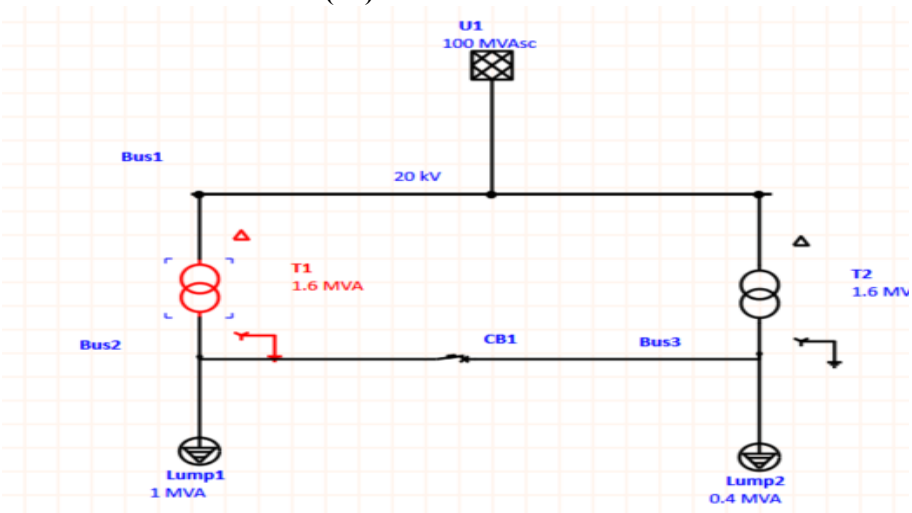

Fig. 12. T1 transformer circuit under analysis

Figure 12 shows the circuit of the transformer no.1 and below are presented the electrical parameters resulting from running ETAP simulation for it.

Base impedance: Zb=V1,ph/I1,ph=(20000V/(42.6/√3)A)=749.8Ω;

Short-circuit impedance: Zk1=(%Zx Zb)/100=(6.33 x 749.8Ω)/100=47.462Ω;

Short-circuit resistance: Rk1=(%R x Zb)/100=(1.041 x 749.8Ω)/100=7.805Ω;

Short-circuit reactance: Xk1=(%X x Zb)/100=(6.244 x 749.8Ω)/100=46.8175Ω;

The resistances of the primary winding respectively second to the primary winding: R1,1=R2,1=Rk1/2=3.9025Ω;

Reactance of the primary winding respectively second to the primary winding: X1,1=X2,1=Xk1/2=23.409 Ω.

Table III. Determination of parameters for transformer no.1 using ETAP

R1,1[Ω]	X1,1[Ω]	R2,1[Ω]	X2,1[Ω]	Xμ,1[Ω]	RFe,1[Ω]
3.9025	23.409	3.9025	23.409	N/A	N/A

Table IV. Determination of parameters for transformer no.2 using ETAP

R2,1[Ω]	X2,1[Ω]	R2,2[Ω]	X2,2[Ω]	Xμ,2[Ω]	RFe,2[Ω]
3.9215	23.5175	3.9215	23.5175	N/A	N/A

Analyzing both sets of values presented in tables 3 and 4 it can be observed that the values are close.

The circuit configuration and the failure details of different transformers are shown in Figures 13-15 (each scenario is based on simulations performed using the ETAP software).

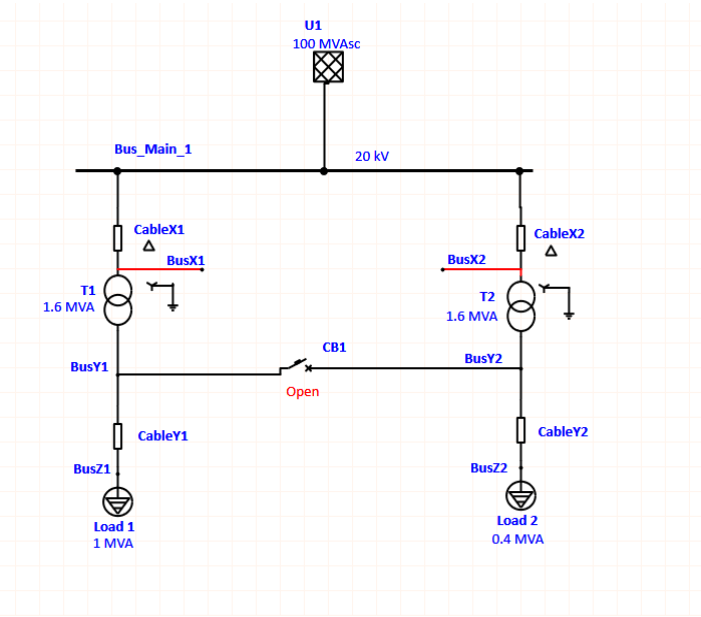

Fig. 13. Schematic representation of the circuit with open breaker

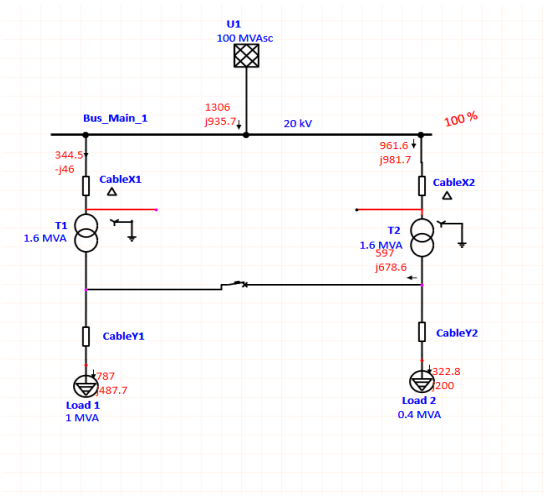

Fig. 14. Circuit configuration with closed breaker

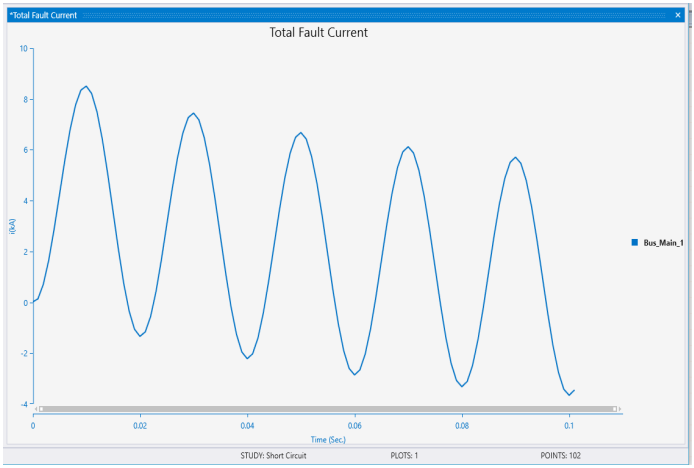

Fig. 15. Fault current at main bus

The **final** results regarding the parameter values are summarized according to table V, presented below:

Table V. Electrical parameters values for transformer no.1

Metodă	**R1,1[Ω]**	**X1,1[Ω]**	**R2,1[Ω]**	**X2,1[Ω]**	**Xμ,1[Ω]**	**RFe,1[Ω]**
Analitic	2.811	23.563	2.811	23.563	216920	749065
ETAP	3.9025	23.409	3.9025	23.409	N/A	N/A

IV.3.1.5 Example of electrical parameters encryption for secure SCADA communication

We have chosen two domestic production (Ro) transformers for which I proposed two different ways of encrypting the electrical parameters for enhanced protection, or at least make it more difficult for a potential attacker who managed to enter the network to produce damage.

Generally, the software solutions are global, being developed in English, which is why we have presented below the parameters related to each transformer like this, but the same encryption methods apply the same way for the parameters in Romanian, offering of course a different ciphered text.

A. Encryption of electrical parameters by transpositions

B. Encryption of electrical parameters by polyalphabetic substitutions

A three-phase transformer 20/0.4kV is chosen with the following parameters:

Transformer power $\mathbf{S_n}$: 1600 kVA
Terminal Primary voltage $\mathbf{U_{1n}}$: 20kV
Terminal Secondary voltage $\mathbf{U_{2n}}$: 400V
Primary nominal current $\mathbf{I_{1n}}$: 46.2A
Secondary nominal current $\mathbf{I_{2n}}$: 2309A
Type of connection: **Dyn05**
No load losses $\mathbf{P_0}$: 1580W
Copper losses $\mathbf{P_k}$: 12000W
No load current $\mathbf{i_0}$: 0.36%
Short-circuit voltage $\mathbf{u_k}$: 6.36%

We build a Vigenere matrix with the following alphabet: "*.%-:0123456789ABCDEFGHIJKLMNOPQRSTUVWXYZ*" şi cheia "*3l3ctrica1transf0rm3r*", returning the ciphered text "*Wcdzl663wfk gyj66 Se: N93L n73 Kw3wjg1v Cjxm1d1 y9o537w 6Bo: VRuI Ltrd4qd6 Vq5f5pksr my8lpg5 G5q: P3CO G9uwbkp xbexn17 fxcuqgk 0Dx: 5Z.TK F6roezduj q0f95mv dni11f8 IT9: 56LCM Mp7q yg 5fxa6rt9aq: GjqCY E6 xyb6 cyfkts GM: 48T38 5f71os ef2f67 Pb: N53L38 Gf 30ke 5l1e62t 9M: 3.6R% Vthib-oss5lsg n3lkwjh fn: I.WX%*".

V Original conclusions and contributions

In the content of the thesis we presented various threats on the electricity system, natural or anthropic, as well as its known (eg extreme weather phenomena) or emergent vulnerabilities (eg. cyber-attacks) and we have emphasized the importance of **resilience**, as follows:

The values underlying the security and resilience of critical infrastructures are:

- Security and resilience must be considered starting from the design phase;

- Risk identification and management must be carried out in a coordinated and comprehensive manner for all critical infrastructures, in order to efficiently allocate resources;
- Understanding and addressing risks from the perspective of critical infrastructure dependencies are essential in terms of security and resilience;
- Protective measures against vulnerabilities propagation due to the interdependencies of critical infrastructures are made through communication, making the relevant information available to all involved operators;
- The public-private partnership is based on trust, flexibility, adaptability, clear goals and objective ways of measuring progress. The expertise of participants in various fields improves safety and resilience as a whole;
- Some critical infrastructures are not limited to the borders of the country (ENTSO-E for electricity, Nabucco for natural gas, etc.), their security and resilience being a factor of inter-state or continental interest.

The thesis proposes the integration on the map of Romania in the CIWIN network, following the model implemented by the Polytechnic University of Turin with the support of the European Commission, corroborated with, but not limited to the models presented in the multi-risk approach on resilience, which correlates the fire hazard with vegetation management. A geo-referential model that includes the national critical infrastructures, the interconnections between them and the links with the ones of the neighboring countries, as well as relevant information about the risks with probability of occurrence in Romania.

Relevant information such as vegetation growth that threatens the integrity of overhead power lines and increases the risk of fire in drought conditions, infrastructure status, topographic elevations and the particularities of the relief depending on weather conditions are important to make the correct decisions regarding an intervention in case of a critical infrastructure in isolated, or hardly accessible at certain times of the year or in adverse weather conditions.

The details of each seismic zone, the floodable areas, the affected areas in the event of a dam failure, the dangers caused by the extreme weather phenomena (high temperatures with the possibility of fire degeneration, storm accompanied by strong wind and electrical discharges, fog, heavy snowfall, earthquake, etc.) integrated on this map would issue an early warning to the operator of the potentially affected critical infrastructure, the interdependent national or European critical infrastructures as well as the state authorities, so the danger could be eliminated in time or its effects would be greatly diminished, with a much smaller impact on victims, damages and the environment.

From simulations carried out using data integrated into this system, based on the past negative events statistics and the costs generated by those for

returning to normal operation, the location of power plants, transformer stations and distribution network at design stage would be executed considering the particularities listed above, avoiding their exposure to certain natural risks.

For the power grid in use, measures can be taken to avoid serious consequences, as we have shown in the previous examples.

The proposed implementation in the thesis would lead to the evolution of CIWIN from a communication platform into an operational one that would integrate GIS (Geographic Information System) and SCADA elements, with the potential to reduce major risks to an acceptable level because all the involved structures will benefit through efficiency and improved response times to eliminate or reduce adverse effects due to the previously simulated scenarios and the complex and complete information made available by the application, using the RO-RISK platform (National Disaster Risk Assessment) as a basis.

Also, depending on the particularities of each seismic zone (normative P 100-1/013 in Romania), for the constructions in the planning phase can be implemented solutions of seismic isolation of the foundation whereas for the objectives in use seismic isolation systems can be implemented for sensitive/critical equipment, following the model successfully implemented at the National Museum of Natural History "Grigore Antipa".

The proliferation and diversification of cyber-attacks as well as the transition to 5G and IoT technologies presents challenges to the security of critical infrastructures in the power sector both from the present regulatory perspective, design and gradual implementation as well as the perspective of a near future characterized by extended interconnection.

The thesis presents a vision of the risks arising as a result of extended digitalization of the national power grid by exploiting the vulnerabilities of some components that lead to taking over of the control in order to modify electrical parameters and produce damages or black-outs. This is the reason why the evolution from the conventional power grid to the smart one is due to involve the implementation of appropriate cyber security measures. Depending on the energetic system component targeted by the attackers, a successful cyber-attack involves changing the electrical parameters leading to fire or explosion and collateral damage, as presented in the case study, all being more elusive than an armed sabotage.

Advanced technologies that provide better management of the national power grid as well as its remote management have the potential to bring significant benefits, but in the process of integrating such technology, due consideration must be given to necessary countermeasures to prevent unwanted events and security breaches inherent in this development. Security measures for such a system need to be sustained and developed as new protocols are implemented and new attack strategies appear, which involves specialized personnel frequently receiving support and schooling as IT and telecommunications technology are among the fastest technological advances.

Overall, new technologies have clear advantages, but also bring potential disadvantages if implementation is incomplete or flawed, especially from the perspective of cyber threats, while the modernization effort without awareness and preparation for these types of threats can cause great harm. Financial Times proposes the integration of the private sector in military exercises to be prepared in the face of emerging aggressions, which by the impact on the private environment simultaneously affects the economy, security and technological secrets of the states.

Cyber security and energy security are components of the National Defense Strategy 2015-2019, while many states and organizations consider cybersecurity as a priority of national security because the one controlling the information has the power [36].

The multiplication and diversification of cyber-attacks that are currently underway are expected to evolve in the 5G and IoT era represent growing challenges for the security of critical energy infrastructure, both at the legislative, design and implementation stage, as well as in the digital and strongly interconnected near future.

The paper offers a perspective on how the digital evolution of the power grid can be used to exploit the vulnerabilities of certain components in order to attack critical infrastructures. The transition from the classic power grid to the intelligent one and all the benefits of this evolution imply, in our opinion, the responsibility of implementing appropriate measures to counter possible cyber-attacks.

Depending on the equipment being attacked in the network, the consequences of a successful hack vary and can result in serious injury and property damage in the event of an explosion or fire to an electrical transformer, as a result or collateral effect in the case of an electrical transformer providing power to an urban area with a mixed function, as shown in the case study, evolving to black-outs in case of high voltage stations.

Advanced technologies that provide improved power grid management and remote control bring significant benefits, but in the process of adopting such new, necessary technology, due consideration must be given to both the implementation of the technology itself and sufficient security measures to prevent unwanted events or security breaches.

Security actions for such a system must be developed and updated as new protocols are implemented and new attack strategies appear, which means that specialized personnel with up-to-date studies/skills regarding new types of threats must handle maintenance, supervision and development of such a system.

Overall, technological innovations bring many advantages, but also involve possible disadvantages related to implementation, maintenance or updating. The effort of investments in the modernization and implementation of new technologies in the field of electronics, automation, information technology and telecommunications represents a direction to be followed for any competitive

company, and the awareness and preparation for the threats (especially cybernetics) makes the difference between a profitable company that provides a vital service in safe conditions and a company that can lose control at any time, vulnerable to competition, cybercrime or state-owned organizations with hostile interests.

We have chosen to end the conclusion area with some of the worst interconnected cyber vulnerabilities, namely hardware vulnerabilities in Intel microprocessors (the largest microprocessor manufacturer) known as Meltdown, Spectre and SWAPGS [37].

These have been partially resolved by updates (with the exception of SWAPGS which was recently discovered by Bitdefender specialists), but a complete solution is only possible by changing the hardware architecture with the new generations of microprocessors, and the effect of these vulnerabilities is unknown because such an attack cannot be detected or stopped by any antivirus solutions because it cannot be distinguished from the normal code (non-malware), therefore the attacks speculating these vulnerabilities have left no traces so it presents a major vulnerability for critical infrastructures in every sector including electricity, where an attack would steal classified data and allow further sabotage attempts.

V.1 Original contributions

The research conducted during doctoral studies have returned the following personal contributions:

- we have presented a summary of structure and functioning of worldwide power grids, through a large volume of bibliographic references;
- we have elaborated a summary of threats and vulnerabilities regarding power grids;
- we presented in a new way SCADA with direct reference to the method of data transfer and the risks associated with plain text transmission of electrical parameters;
- we have presented a summary of encryption methods and possible choices regarding such a way for securing the information (electrical parameters) transmitted through SCADA;
- we have developed a management analysis model for a company operating an electrical critical infrastructure;
- we have implemented an application in PyroSim modelling software which illustrates the effects of a cyber-attack on an electric transformer;
- we have modeled in ETAP software an application that simulates the output of nominal parameters of an electrical transformer due to a cyber-attack;
- we have developed two examples of electrical parameters encryption for secure SCADA communications.

V.2 Further development perspectives

- Further research related to identifying the most efficient methods of securing information regarding electrical parameters in electricity systems;
- GIS implementation and drone usage for vegetation surveillance in the vicinity of overhead power lines and flood risks regarding the power grid infrastructures, according to models mentioned above and cited.

V.3 Research developed during the doctoral studies

During the doctoral research I was part of the group of authors developing the works mentioned below:

I. Indexed Institute for Scientific Information Web of Science (ISI WoS):

1. H. Andrei, P.C. Andrei, M. Gaiceanu, M. Stanculescu, I. Arama, **I. Marinescu**, *Power Systems Recovery and Restoration Encouter with Natural Disaster and Deliberate Attacks,* pp.247-267, chapter 10 of the book *Power Systems Resilience*, *Modeling, Analysis and Practice,* editors M. Tabatabaei, S.V. Ravadanegh, N. Bizon, Springer, 2019, 353 pages.
2. H. Andrei, M. Gaiceanu, M. Stanculescu, **I. Marinescu,** P.C. Andrei, *Microgrid protection,* pp.606-630 chapter 25 of the book *Microgrid Architectures, Control and Protection Methods*, editors M. Tabatabaei, E. Kabalci, N. Bizon, Springer, 2019, 775 pages , ISBN 978-3-030-23722-6.
3. H. Andrei, M. Gaiceanu, M. Stanculescu, **I. Marinescu**, P. C. Andrei, *Security evaluation of sensor networks*, chapter 11 of the book *Recent Developments on Industrial Control Systems Resilience,* editors M. Tabatabaei, E. Pricop, Springer, 2020.
4. M. Stanculescu, C.A. Badea, **I. Marinescu**, P. Andrei, O. Drosu, H. Andrei, *Vulnerability of SCADA and Security Solutions for a Waste Water Treatment Plant,* IEEE XIth Int. Symposium on Advanced Topics in Electrical Engineering-ATEE, March 28-30, 2019, Bucharest, Romania, Paper 87, 978-1-7281-0101-9/19/$31.00 ©2019 IEEE.
5. **I. Marinescu**, B. Botea, H. Andrei**,** *Critical Infrastructure Risk Assessment of Romanian Power Systems*, IEEE-5th Int Symposium on Electrical and Electronics Engineering-ISEEE, 20-22 oct. 2017, Galati Romania, paper 69, IEEE Catalog Number CFP1793K-USB, ISBN 978-1-5386-2058-8, indexat ISI Web of Science.
6. **I. Marinescu**, H. Andrei, I. Iordache, *Protection methods and actions to increase the safety of operation in power systems assimilated to critical infrastructures,* IEEE-11th International Conference - Electronics, Computers and Artificial Intelligence (ECAI 2019), 27-29 june 2019, Pitesti Romania, paper 43,

IEEE Catalog Number CFP1927U-USB, ISBN 978-1-7281-1623-5, indexat ISI Web of Science.

7. D. Burlacu, A. M. Georgescu, A. A. Vartires, **I. Marinescu**, *An experimental evaluation of visibility in simulated smoke, the* 9th International Conference on ENERGY and ENVIRONMENT CIEM 2019, 17-18 october 2019, Timisoara Romania, acceptat pentru prezentare în cadrul conferinței indexată ISI Web of Science.

8. ***I. Marinescu**, S. Deleanu, M. Stănculescu, L. Bobaru, P. Andrei, H. Andrei, Electrical equipment safety analysis and simulation. Case study: transformer's malfunctions,* IEEE-6th Int Symposium on Electrical and Electronics Engineering-ISEEE, 18-20 oct. 2019, Galati Romania, paper 14, acceptat pentru prezentare în cadrul conferinței indexată ISI Web of Science.

II. Indexed in International Databases:

1. B. Botea, **I. Marinescu**, C. Dragoi, H. Andrei**,** *Modeling, Simulation and Analysis of Disturbance in Low Voltage Instalations,* The Scientific Bulletin of Electrical Engineering Faculty, 2019, year v19, 1(40), Published: May 2019, pp. 49–57, DOI: 10.1515/SBEEF-2019-0010

2. B. Botea, **I. Marinescu**, *New Approaches in the Consumer - Supplier Relationship Regarding Malfunctions in the Electroenergetic Systems and from the Perspective of the IoT Development,* The Scientific Bulletin of Electrical Engineering Faculty, 2017, year 17, 2(37), Published: October 2017, pp. 48–53, DOI: 10.1515/SBEEF-2017-0011

Selective bibliography (out of a total of 260 entries):

[1] A. Badea, Thermal equipment and installations
[2] http://www.nuclearelectrica.ro/
[3] W. Wang, et al – Simultaneous production of fresh water and electricity via multistage solar photovoltaic membrane distillation
[4] http://www.termo.utcluj.ro/regenerabile/6_3.pdf
[5] The President's National Infrastructure Advisory Council (NIAC), SUA
[6] NIST Framework and Roadmap for Smart Grid Interoperability Standards, Release 1.0
[7] V. Boutin, M. Feasel, K. Cunic, J. wild, How Microgrids Contribute to the Energy Transition
[8] North American Electric Reliability Council, Technical Analysis of the August 14, 2003, Blackout: What Happened, Why, and What Did We Learn?
[9] https://thehackernews.com/2017/12/triton-ics-scada-malware.html
[10] R. Smith, Assault on California Power Station Raises Alarm on Potential for Terrorism, The Wall Street Journal
[11] WorldRiskReport-2018, https://weltrisikobericht.de/english-2/
[12] D. Oyedokun, P. Cilliers, Geomagnetically Induced Currents: A Threat to Modern Power Systems, Classical and Recent Aspects of Power System Optimization, 2018
[13] International Nuclear and Radiological Event Scale (INES)
[14] Technical Code of the Electric Transport Grid, National Electricity Transport Company Transelectrica S.A.

[15] H. Albert, S. Gheorghe, N. Golovanov, L. Elefterescu, R. Porumb, Quality of electricity. Contributions. Results. Perspectives, publishing house AGIR, Bucharest 2013
[16] Transelectrica policy in the field of Smart Grid, years 2018-2027
[17] C. Teba, Building Technologies: Who's Who? https://www.dexma.com/building-technologies-whos/
[18] SCADA architecture example https://www.electricaltechnology.org/2015/09/scada-systems-for-electrical-distribution.html
[19] Specialized software accessible at https://nmap.org/
[20] ISO/IEC 27000:2018 https://www.iso.org/standard/73906.html
[21] United States Naval Academy, The Cyber Battlefield https://www.usna.edu/Users/cs/wcbrown/courses/si110AY13S/lec/l21 /lec.html
[22] A. Andrei, M. Stănculescu, Cryptography vs. cryptanalysis, publishing house Printech 2014
[23] https://inmcm.wordpress.com/2010/03/14/basic-aes-128-encryption-in-vhdl-complete/
[24] Elliptic Curve Cryptography, https://www.ssl2buy.com/wiki/ecc-algorithm-to-enhance-security-with-better-key-strength
[25] Merkle–Damgård hash function, https://en.wikipedia.org/wiki/Merkle%E2%80%93Damg%C3%A5rd_construction
[26] https, https://ro.wikipedia.org/wiki/HTTPS
[27] VPN, https://en.wikipedia.org/wiki/Virtual_private_network
[28] International Association for Trusted Blockchain Applications, https://inatba.org/
[29] R. Ivorschi, SWOT analysis - managerial tool to improve efficiency
[30] M. Rouse, T. Culverhouse, TechTarget, automatic transfer swich (ATS)
[31] "Dunărea de Jos" University in Galați, Faculty of Automatic, Computers, Electrical and Electronic Engineering, course notes "Electric transformer"
[32] Buchholz relay, https://ro.wikipedia.org/wiki/Releu_Buchholz
[33] Fire extinguishing systems for electrical transformers, http://www.sergi- tp.com/how-transformer-protector-works/
[34] https://monitoruldevrancea.ro/2019/07/09/video-si-foto-incendiu-pe-calea-ferata-circulatia-feroviara-este-intrerupta/
[35] ETAP (Electrical Power System Analysis & Operation Software), https://etap.com/
[36] V. Vevera, Cyber space - the new battlefield, Romanian Journal of Computer Science and Automation, vol. 26, no. 1
[37] https://labs.bitdefender.com

PERSONAL INFORMATION

Ioan Marinescu

Șoseaua Colentina nr. 16, 021177, Bucharest, Romania

+40 723 188 057

ioan.marinescu@yahoo.com

Sex M | Date of birth 22/11/1988 | Nationality Romanian

WORK EXPERIENCE

07.2017 – present

Officer

Special Telecommunications Service, Bucharest, Romania

Business or sector Governmental institution – public order and safety

06.2016 – 06.2017

Company commander

Police Academy "Alexandru Ioan Cuza", Bucharest, Romania

Business or sector Education – public order and safety

12.2012 – 05.2016

Platoon commander

Police Academy "Alexandru Ioan Cuza", Bucharest, Romania

Business or sector Education – public order and safety

EDUCATION AND TRAINING

10.2016 - present

PhD "Electrical Engineering"

Valahia University of Targoviste, Dambovita County, Romania

10. 2015

Course „Project manager"

Institute for Studies in Public Order, Bucharest, Romania

2013 - 2015

Master "Management of public order and national security"

Police Academy „Alexandru Ioan Cuza" – Police Faculty, Bucharest, Romania

03. 2014

Course „Trainer"

Institute for Studies in Public Order, Bucharest, Romania

06.2013 – 12. 2013

Course „Shooting range instructor"

Institute for Studies in Public Order, Bucharest, Romania

2008 - 2012

Bachelor's degree in Installation engineering & Firefighter Officer certificate

Police Academy „Alexandru Ioan Cuza" – Fire Officers Faculty, Bucharest, Romania

2003 - 2007

Baccalaureate, specialization in mathematics-informatics

High school "I. L. Caragiale" – Moreni, Dambovita County

PERSONAL SKILLS

Mother tongue(s) Romanian

Other language(s)

	UNDERSTANDING		SPEAKING		WRITING
	Listening	Reading	Spoken interaction	Spoken production	
English	C1	C1	C1	C1	C1

Levels: A1/A2: Basic user - B1/B2: Independent user - C1/C2 Proficient user

Communication skills

- Good communication skills and networking with others;
- Ability to work in a team, both as part of the group and the position of leader;
- Ethics during and outside of work;
- Ability of social integration, including through multinational teams and to develop harmonious relations with subordinates, peers and commanders;
- Ability to assimilate new information and skill;
- The ability to communicate under stress conditions with all social categories (experience in electoral processes).

Organisational / managerial skills

- Leadership;
- Ability to structure and deliver a speech;
- Establish an optimal work environment by motivating subordinates, leading by example and by taking responsibility both for my own actions and effects and those of the coordinated structure;
- Efficient as a group leader or subordinate;
- Distributive attention and ability to forecast the evolution of dangerous situations, with attention to details;
- Ability to take good decisions under stress, with adaptation to new and complex situations.

Job-related skills

- Disciplined (military training);
- Decision maker (developing and applying fire safety regulations and controlling the way these are implemented throughout the organization);
- Diplomacy (was in charge of international relations for the Firefighters Faculty, now I'm developing an efficient communication between employer and fire safety structures in the other governmental structures).

Digital competence

- Knowledge of operating systems Android, macOS and Windows
- Certificate of professional skills - informatics (obtained in 2007 under High school "I. L. Caragiale" - Moreni)
- Moderate knowledge, PyroSim
- Good knowledge of Microsoft Office Suite (Word, Excel, PowerPoint)
- Good knowledge of AutoCAD;
- Good knowledge of Adobe Lightroom and Adobe Photoshop.

Hobbies

- Photography, travelling, swimming, tennis

Driving licence B since 2008

ADDITIONAL INFORMATION

International attendance missions

- Officer, head of „Alexandru Ioan Cuza" Police Academy team, representing Romania at XI International Rescue Workshop "Fenix 2014", June 2014, Pionki, Poland;
- Officer, part of „Alexandru Ioan Cuza" Police Academy staff at "Biological Threat Response Table-Top Exercise" held by Defense Threat Reduction Agency through USA Embassy, september 2013, Bucharest, Romania;
- Student, member of „Alexandru Ioan Cuza" Police Academy team representing Romania at IX International Rescue Workshop "Fenix 2012", May 2012, Pionki, Poland.

References

References can be provided upon request