Buletinul Universităţii Naţionale de Apărare „Carol I”
10.53477/2065-8281-22-73

REZILIENȚA INFRASTRUCTURILOR CRITICE DIN CADRUL SISTEMULUI ENERGETIC NAȚIONAL ÎN SCOPUL ASIGURĂRII SECURITĂȚII ENERGETICE ȘI NAȚIONALE

THE RESILIENCE OF CRITICAL INFRASTRUCTURES WITHIN THE NATIONAL ENERGY SYSTEM IN ORDER TO ENSURE ENERGY AND NATIONAL SECURITY

Șef lucr.dr.ing. Nicolae Daniel FÎȚĂ*
Prof.univ.dr.ing. Sorin Mihai RADU**
Conf.univ.dr.ing. Dragoș PĂSCULESCU***

Securitatea energetică și, implicit, arhitectura energetică regională, compusă din infrastructuri critice energetice (stații electrice și linii electrice aeriene, la tensiunea de 400 kV), pot suferi diferite mutații și transformări, determinate de eventuale sincope în extragerea, transportul și valorificarea resurselor energetice și a energiei, din cauza dinamismului energetic. Vulnerabilitatea acestor infrastructuri critice energetice generează o serie de riscuri și amenințări la adresa lor, periclitând astfel viața societală, creând disfuncționalități și generând daune extreme, aduse statului. Infrastructurile critice energetice devin astfel indispensabile societății, fără de care statul și mecanismele lui nu pot funcționa și asigura bunăstarea societală, iar protecția lor devine obiectiv major național și european, determinând reprezentanții statelor membre ale Uniunii Europene să ia măsuri în direcția identificării și gestionării oricărui risc sau amenințare. În fața vulnerabilităților, amenințărilor și riscurilor cu care se confruntă România în noul context geopolitic dinamic, turbulent și impredictibil, de securitate globală, regională și euroatlantică, pe fondul crizei militare și sanitare, amplificat de criza energetică mondială, manifestată prin creșterea nefondată și neașteptată a prețului energiei, statul român ar trebui să dețină o strategie de consolidare a rezilienței infrastructurilor critice energetice, bazată pe predictibilitate, flexibilitate, continuitate, adaptabilitate și reziliență.

Energy security and implicitly the regional energy architecture composed of critical energy infrastructures (power substations and overhead lines at 400 kV), can undergo various mutations and transformations caused by possible syncope in the extraction, transport and exploitation of energy resources and energy, due to energy dynamism. The vulnerability of these critical energy infrastructures generates a number of risks and threats to them, thus endangering societal life, creating malfunctions and generating extreme damage to the state. Critical energy infrastructures thus become indispensable to society, without which the state and it`s mechanisms cannot function and ensure societal well-being, and their protection becomes a major national and European objective, prompting representatives of the member states of the European Union to take action to identify and manage any risk or threat. In the face of the vulnerabilities, threats and risks Romania faces in the new dynamic, turbulent and unpredictable geopolitical context of global, regional and Euro-Atlantic security, amid the military and health crisis and amplified by the global energy crisis manifested by the unfounded and unexpected increase in energy price, the Romanian state should have a strategy for strengthening the resilience of critical energy infrastructures, based on predictability, flexibility, continuity, adaptability and resilience.

Cuvinte-cheie: reziliență; infrastructuri critice energetice; securitate națională; black-out.
Keywords*: resilience; critical energy infrastructure;national security; black-out.*

Universitatea din Petroșani
e-mail: *daniel.fita@yahoo.com*
****Universitatea din Petroșani***
e-mail: *sorin_mihai_radu@yahoo.com*
*****Universitatea din Petroșani***
e-mail: *pdragos_74@yahoo.com*

Definiție „black-out electroenergetic”: „pană generalizată de energie electrică, care se manifestă prin lipsa energiei electrice la consumatorii casnici, industriali și critici și poate provoca crize majore la nivel național cu efecte catastrofale și devastatoare, punând în pericol securitatea și bunăstarea națională.” *națională* (N. D. Fîță, S.

M. Radu și alții 2021, 37-58).

Deoarece infrastructurile electroenergetice (centrale electrice, stații electrice și linii electrice aeriene) asigură accesul populației și industriei naționale la electricitate, ele sunt critice prin faptul că toate sectoarele economiei naționale sunt dependente de energia electrică, iar statele Uniunii Europene sunt obligate să ia măsuri în direcția identificării, desemnării, analizei, evaluării, protecției și rezilienței acestora. Dar aceste infrastructuri critice electroenergetice, vitale vieții cotidiene și asigurării securității naționale, pot fi vulnerabile, punând în pericol bunăstarea societală, generând disfuncționalități mecanismelor statului și cetățenilor.

Un posibil „black-out” la nivel național este extrem de puțin probabil, deoarece Sistemul Energetic Național, care este compus din infrastructuri critice energetice (centrale electrice, stații electrice și linii electrice aeriene), este un sistem tehnic destul de sigur, iar angajații Companiei Naționale de Transport al Energiei Electrice Transelectrica SA, compania care gestionează buna funcționare a SEN în condiții optime, de siguranță și securitate, sunt foarte bine specializați și instruiți în acest domeniu.

Totuși, în contextul crizei energetice mondiale actuale, pe fondul impredictibilității sistemului politic și legislativ, al corupției și incompetenței din sistemul energetic și al lipsei investițiilor, un posibil black-out trebuie avut în vedere, iar unele calcule pot fi făcute, din acest motiv, prevenirea unui astfel de eveniment nedorit fiind absolut necesară și obligatorie.

În urma constatărilor concluzive asupra Sistemului Energetic Național, se admite că o abordare a celor mai adecvate căi pentru prevenirea, reducerea, combaterea și eliminarea potențialelor *breșe de securitate energetică*[1] implică o cunoaștere și înțelegere mai profundă și exactă a motivelor fundamentale care stau la baza breșelor de securitate energetică, ce pot fi înșelătoare, variate și, de foarte multe ori, combinate combinate (Fîță, Păsculescu, și alții 2022, 180-201).

Conceptul de reziliență

Conceptul de reziliență este adoptat relativ recent din studiul științelor sociale, în special din cercetarea comportamentelor populației în situații de criză, generate de anumite evenimente neprevăzute, ca: *dezastre naturale* (furtuni, tornade, inundații, secete, incendii, îngheț, avalanșe, alunecări de teren, cutremure, erupții vulcanice etc.), *războaie* (civile, militare, hibride etc.), *riscuri și amenințări teroriste* (cibernetice, chimice, biologice, ecologice, energetice etc.), *tulburări interne* (revolte, greve, revoluții etc.), *accidente de muncă* (individuale, colective etc.), *evenimente tehnologice* (incidente, avarii etc.), *traume psihologice* (deces, divorț, pierderi, constrângeri etc.) și *epidemii/pandemii* (naturale, artificiale etc.). Semnificațiile conceptuale ale rezilienței sunt foarte diverse, aceasta fiind întâlnită în domenii ca *sociologia, psihologia, psihiatria, managementul, economia, ecologia, ingineria, cibernetica* etc., toate aceste definiții fiind integrate în *știința durabilității* (Bănică și Muntele 2015), iar această disciplină se caracterizează printr-o abordare generală, cu o sferă de cuprindere largă a semnificațiilor conceptuale și aplicative ale durabilității, care integrează ideile și acțiunile provenite din științele naturii, sociale, inginerești, medicale etc., pentru îmbunătățirea cunoștințelor și a modului de acțiune, precum și a creării unei legături dinamice între componente, în scopul asigurării sustenabilității (dezvoltării durabile), mai ales a sistemelor sociale. Includerea rezilienței în această știință multidisciplinară complexă evidențiază rolul teoretic și practic al conceptului, pentru menținerea și dezvoltarea sistemelor sustenabile (durabile), iar caracteristica sa fundamentală este aceea de *a capacita resursele și componentele structurale ale unei entități societale (sociale) sau fizice, pentru a face față schimbărilor sau acțiunilor perturbatoare.* Departamentul pentru Securitate Internă al Statelor Unite ale Americii – DHS[2] consideră că reziliența înseamnă capacitatea și abilitatea unei entități de a se pregăti și adapta la schimbarea condițiilor, de a rezista și recupera rapid, în urma unor perturbări, atacuri deliberate, accidente, incidente sau amenințări.

[1] Breșe de securitate energetică – nerespectarea prescripțiilor de securitate, generate de infrastructurile critice și/sau de factorul uman, urmate de incidente tehnice (izolate/asociate), de avarii tehnice (ușoare/grave – black-out) și de accidente de muncă din cadrul Sistemului Energetic Național – SEN.

[2] Department of Homeland Security.

Dimensiuni ale rezilienței (MCEER 2008):

- *reziliența societală (socială):* capacitatea societății de a reduce impactul unei crize, de adaptare prin ajutorarea primelor persoane care intervin sau a celor care acționează în calitate de voluntari;
- *reziliența economică:* capacitatea unei entități de a face față costurilor suplimentare care apar într-o criză;
- *reziliența organizațională:* capacitatea managerilor care se ocupă de criză de a lua decizii și măsuri care să conducă la evitarea unei crize sau la reducerea impactului acesteia;
- *reziliența tehnică:* capacitatea sistemului fizic al organizației de a se comporta în mod corespunzător, în cazul unei crize.

Proprietăți ale rezilienței:

- *robustețea:* rezistența sau capacitatea elementelor, sistemelor și a altor unități analizate de a rezista la un anumit nivel de stres sau de solicitare, fără a suferi degradarea sau pierderea funcționalităților;
- *redundanța:* măsura în care elementele, sistemele sau alte unități analizate, capabile să satisfacă cerințele funcționale, în cazul unor evenimente de perturbare, degradare sau pierdere a funcționalității;
- *capacitatea de reacție:* capacitatea de a identifica probleme, de a stabili priorități și de a mobiliza resurse, atunci când există condiții care amenință să perturbe unele elemente, sisteme sau alte unități analizate;
- *capacitatea de recuperare rapidă:* capacitatea de a îndeplini prioritățile și de a atinge obiectivele, în timp util, pentru a limita pierderile și pentru a evita perturbările viitoare.

Reziliența și securitatea:

Reziliența a devenit un indicator al politicii de securitate al Uniunii Europene, iar în acest sens, Comisia Europeană a elaborat *Planul de Acțiune pentru Reziliență în Țările Predispuse la Criză – Action Plan for Resilience in Crisis Prone Countries 2013-2020*[3], astfel ajungându-se la o nouă abordare a dimensiunii societale a securității naționale și europene, care pune accent pe cetățean, comunitate și pe populația unui stat sau a unei regiuni. În Comunicarea din 2012 a Comisiei Europene (Comisia Europeană 2017) privind abordarea UE referitoare la reziliență, aceasta este definită ca fiind *capacitatea unei persoane fizice, a unei gospodării, a unei comunități, a unei regiuni sau a unei țări de a rezista, de a se adapta și de a-și reveni rapid din situații de stres și de șoc*. Strategia globală a UE extinde definiția acestui concept și reziliența este considerată ca fiind un concept mai larg, cuprinzând toate persoanele și întreaga societate, care se bazează pe democrație, încredere în instituții și dezvoltare durabilă, precum și pe capacitatea de a se reforma. Abordarea strategică a UE în materie de reziliență vizează îndeplinirea în mod durabil a ansamblului de obiective ambițioase pentru acțiunea externă a UE, consolidând:

- adaptabilitatea statelor, a societăților, a comunităților și a indivizilor la presiunile politice, economice, de mediu, demografice sau societale, pentru a continua progresele în realizarea obiectivelor naționale de dezvoltare;
- capacitatea unui stat, confruntat cu presiuni semnificative, de a construi, de a menține sau de a restabili funcțiile sale esențiale, precum și coeziunea socială și politică de bază, întrun mod care să asigure respectarea democrației, a statului de drept, a drepturilor omului și a drepturilor fundamentale și care să favorizeze securitatea și progresul tuturor pe termen lung;
- capacitatea societăților, a comunităților și a indivizilor de a gestiona oportunitățile și riscurile într-un mod pașnic și stabil și de a constitui, de a menține sau de a restabili mijloacele de subzistență, în fața unor presiuni majore.

Ciclul de viață al infrastructurilor critice energetice

Guvernul României a mandatat Ministerul Afacerilor Interne, prin Centrul Național pentru Coordonarea și Protecția Infrastructurilor Critice – CNCPIC, să coordoneze și să protejeze infrastructurile critice de pe teritoriul României. Protecția infrastructurilor critice naționale este o sarcină complexă, multi/inter/transdisciplinară, care implică toate sectoarele economiei naționale, de apărare, intelligence și de intervenție în caz de urgență și necesitate, fără de care securitatea națională și bunăstarea poporului român ar fi în mare pericol.

[3] *Action Plan for Resilience in Crisis Prone Countries 2013-2020* – European Commision.

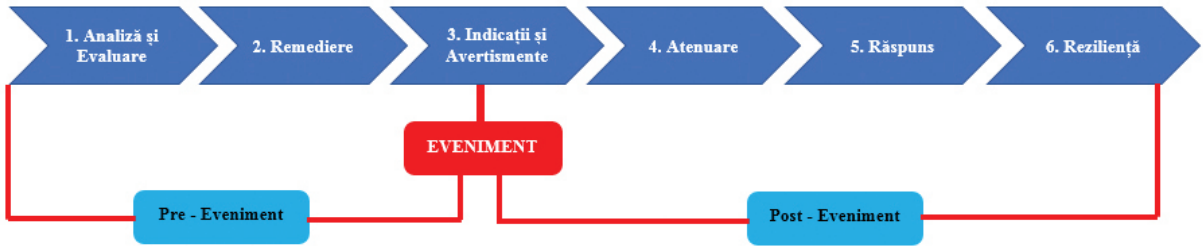

Figura 1 *Ciclul secvențial al infrastructurilor critice*

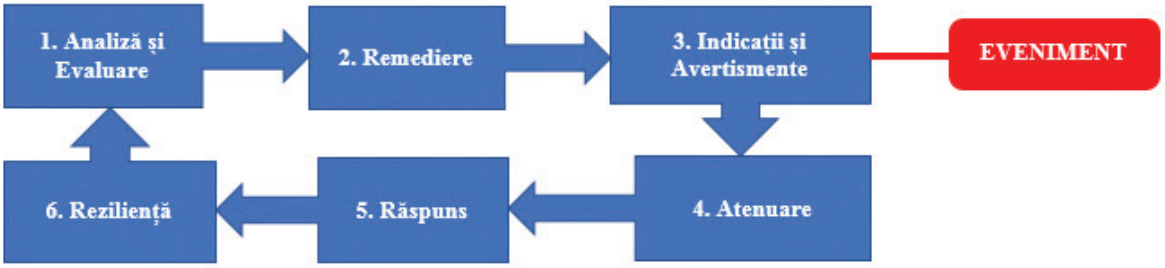

Figura 2 *Circuitul închis al infrastructurilor critice*

Se presupune și se consideră că este aproape imposibil să se protejeze sută la sută o infrastructură critică, indiferent de sectorul din care provine, de aceea trebuie acordată o importanță sporită în acest sens de către instituțiile statului și companiile private care sunt deținătoare, gestionare sau operatoare de infrastructuri critice, prin activitatea de prevenire și prevenție (analiză, evaluare și remediere a riscurilor și vulnerabilităților constatate), în scopul securizării acestora.

De asemenea, trebuie acordată o importanță deosebită și activității de atenuare a impactului și revenirii (reziliența tehnică/societală/umană) la normalitate a infrastructurilor critice, în urma unui eveniment negativ.

Ciclul secvențial și circuitul închis al infrastructurilor critice (N. D. Fîță 2020) sunt schematizate în figurile 1 și 2 (Fîță, Radu și Păsculescu 2021).

Cele șase faze ale ciclului de viață ale infrastructurilor critice creează o soluție globală în vederea protecției și securizării ei. Fazele ciclului de viață au loc înainte, în timpul și după eveniment și pot compromite, degrada sau distruge infrastructurile critice.

Sinteza celor șase faze sunt comentate în Tabelul nr. 1.

Descrierea, analiza și cuantificarea unui black-out electroenergetic național – 10 mai 1977

Descrierea evenimentului

La data de 10 mai 1977, în România a fost cea mai gravă pană de energie electrică din toate timpurile. Aceasta a durat între 4 și 5 ore și a constat într-o succesiune de incidente tehnice, amplificată de erorile personalului de dispecerizare și exploatare și, în tot acest timp, niciun consumator casnic sau industrial nu a fost alimentat cu energie electrică, generând daune imense.

Analiza evenimentului (derulare secvențială)

Derulare Secvențială
ECHIPAMENTE ȘI APARATE ENERGETICE VECHI (lipsă investiții și retehnologizare) + SUCCESIUNE DE INCIDENTE TEHNICE + ERORI PERSONAL DISPECERIZARE ȘI EXPLOATARE (lipsă personal specializat) → BLACK-OUT
STAȚIE ELECTRICĂ (110 kV) → DETERIORARE IZOLATOR → SCURTCIRCUIT → DECONECTARE AUTOMATICĂ DE PROTECȚIE CHE → DECONECTARE CTE → DEFICIT PUTERE ÎN SEN (MW) → REDUCERE TENSIUNE ÎN SEN (Rețea electrică 220 kV și 400 kV) → SUPRAÎNCĂRCARE (Rețea Electrică 220 kV) → SEPARARE SEN → FUNCȚIONARE ASINCRONĂ → DECLANȘARE LEA (220 kV și 400 kV) → DECONECTARE SEN ZONA NORD (nesincronism) / DECONECTARE SEN ZONA SUD (protecții) → IEȘIRE TOTALĂ DIN FUNCȚIUNE A SEN → INSECURITATE ENERGETICĂ → INSECURITATE ECONOMICĂ → INSECURITATE NAȚIONALĂ → DAUNE → STARE DE INSTABILITATE

Tabelul nr. 1
DESCRIEREA FAZELOR CICLULUI DE VIAȚĂ AFERENT INFRASTRUCTURILOR CRITICE

Număr fază	Nume fază	Când are loc	DESCRIERE
1	ANALIZA ȘI EVALUAREA	Înaintea unui eveniment	- această fază este fundamentală și reprezintă cea mai importantă etapă a ciclului de viață a unei infrastructuri critice; - în această fază, se determină vulnerabilitățile, dependențele și interdependențele acestora astfel încât factorii de decizie să aibă toate informațiile de care au nevoie pentru a face alegeri eficiente în gestionarea riscurilor; - în urma acestei faze, se face o evaluare a impactului operațional al compromiterii, degradării sau distrugerii infrastructurii critice; - în plus, se poate anticipa un atac cibernetic asupra acestor infrastructuri critice, deoarece ele pot fi telecomandate de la distanță de hackeri în scopuri distructive sau militare; - această fază este de prevenire, prevenție sau autoapărare; - infrastructurile critice sunt dispuse în toate sectoarele economiei naționale, iar fiecare sector este compus din sisteme, persoane, programe, echipamente sau facilități; - infrastructurile critice pot fi simple, cum ar fi o facilitate dintr-o locație geografică, sau complexă, care implică și noduri dispersate geografic; - analiza și evaluarea sunt alcătuite din 5 etape care includ activități care acoperă și cuprind toate sectoarele de activitate ale economiei naționale și infrastructurile critice ale acestora: 1) identificarea infrastructurilor critice și a elementelor critice; 2) caracterizarea infrastructurii critice (asocierea dintre funcții și relații); 3) analiza impactului operațional; 4) evaluarea vulnerabilității (probabilitatea dezastrelor naturale, evenimente criminale sau de securitate națională, eșecuri tehnologice); 5) analiza interdependenței.
2	PREVENIREA	Înaintea unui eveniment	- în această fază, sunt discutate slăbiciunile și vulnerabilitățile cunoscute, unde se adoptă măsuri de precauție și se întreprind acțiuni, înainte de producerea unui eveniment, prin remedierea vulnerabilităților, pericolelor și amenințărilor fizice sau cibernetice constatate, care ar putea provoca compromiterea, degradarea sau distrugerea infrastructurilor critice; - acțiunile de remediere sunt măsuri menite să remedieze vulnerabilități virtuale și fizice, cunoscute înainte de apariția unui eveniment, și ele pot fi: • educație și conștientizare despre securitate; • îmbunătățirea proceselor operaționale; • îmbunătățirea configurării sistemului; • modificări ale sistemului prin înlocuirea componentelor vechi, uzate moral și fizic, cu componente ultramoderne cu siguranță și fiabilitate ridicată. - scopul remedierii este de a îmbunătăți fiabilitatea și disponibilitatea infrastructurilor critice și se aplică oricărui tip de vulnerabilitate; - costul fiecărei acțiuni de remediere depinde de natura vulnerabilității.
3	INDICATORI DE AVERTIZARE	Înaintea unui eveniment și/sau în timpul unui eveniment	- această fază implică monitorizarea zilnică a sectorului de infrastructură critică, pentru a evalua capacitățile de asigurare și securizare și pentru a determina dacă există indicii de eveniment care trebuie raportat; - indicațiile se bazează pe informații la nivel tactic, operațional, teatral și strategic; - la nivel tactic, informația provine de la proprietarii de infrastructuri critice; - la nivel operațional, informația provine din sectoarele aferente infrastructurilor critice; - la nivel teatral, informația provine de la partenerii regionali (UE, NATO, guvernele aliate, forțele de coaliție, etc.); - la nivel strategic, informația provine de la serviciile de informații interne și/sau externe, de la autoritățile de aplicare a legii și din sectorul privat; - avertismentul este procesul de notificare a posesorilor de infrastructuri critice despre o posibilă amenințare sau pericol la adresa acestora; - indicațiile și avertismentele sunt acțiuni care semnalează un eveniment probabil, planificat sau în derulare; în cazul în care se detectează o indicație, se poate emite un avertisment care să anunțe toți proprietarii sau operatorii de infrastructuri critice, cu privire la un pericol sau la o amenințare.
4	ATENUAREA	Înaintea unui eveniment și/sau în timpul unui eveniment	- această fază cuprinde acțiunile de prevenire (imunizare), de consolidare pentru prevenirea impactului rezultat în urma producerii evenimentului negativ; - proprietarii sau operatorii de infrastructuri critice, indiferent de sectorul industrial din care acestea fac parte, iau măsuri pentru a minimiza impactul operațional al compromiterii, degradării sau distrugerii acestora; - scopul principal al fazei de atenuare este de a minimiza impactul operațional asupra altor infrastructuri critice, atunci când infrastructura critică este compromisă, degradată sau distrusă; - acțiunile de atenuare ajută la activitățile de urgență, de investigații și de gestionare a fazei 5, precum și la activitățile de reziliență din faza 6.
5	RĂSPUNSUL	După eveniment	- răspunsul la incidente sau accidente cuprinde planurile și activitățile întreprinse pentru a elimina efectele sau consecințele unui eveniment.
6	REZILIENȚA	După eveniment	- această fază implică acțiuni întreprinse pentru a reconstrui sau reabilita infrastructura critică, după de a fost compromisă, degradată sau distrusă; - acest proces este cel mai provocator și cel mai puțin dezvoltat și revine, implicit, proprietarilor de infrastructuri critice.

Eveniment 1:

În jurul orei 08:40, un scurtcircuit în rețeaua de 110 kV (stația electrică Tismana) a dus la deconectarea prin automatica de protecție a 3 grupuri din CHE Porțile de Fier (525 MW) și a LEA 400 kV Djerdap (325 MW import).

În regim stabilizat, după declanșările de mai sus, la CTE Rovinari personalul a deconectat, în curs de câteva minute, blocurile 3 și 4 (290 MW).

Ca urmare, în SEN s-a produs un important deficit de putere (1.100 MW), determinând reducerea substanțială a tensiunilor în rețeaua electrică de 220 kV și 400 kV.

Eveniment 2:

În jurul orei 08:45, prin declanșarea cuplei transversale 400 kV Sibiu, se întrerupe circulația de putere prin rețeaua de 400 kV spre zona de sud-est a SEN deficitară, redistribuindu-se în rețeaua de 220 kV și supraîncărcând arterele Luduș – Ungheni – Fântânele, respectiv Mintia – Pești – Hășdat – Paroșeni.

Eveniment 3:

În jurul orei 08:47, se deteriorează bobina de blocaj înaltă frecvență de pe linia de 220 kV Ungheni – Fântânele, care declanșează, ca urmare, arterele de legătură între nord și sud, momentan în funcțiune (Pești – Hășdat, Mintia – Timișoara, Arad – Szeged), declanșează la suprasarcină.

Acest eveniment conduce la separarea SEN în două zone:

- zona de sud, profund deficitară, în care acționează automatica de descărcare a sarcinii la

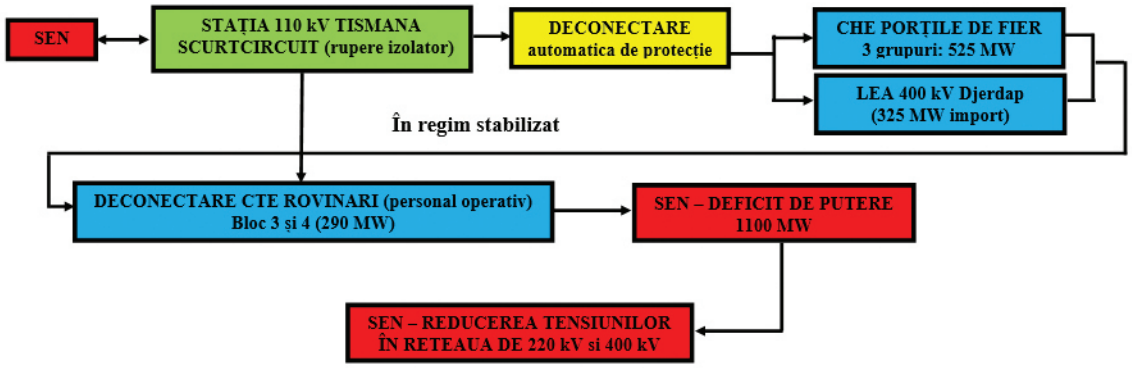

Figura 3 *Descriere tehnică – Eveniment 1*

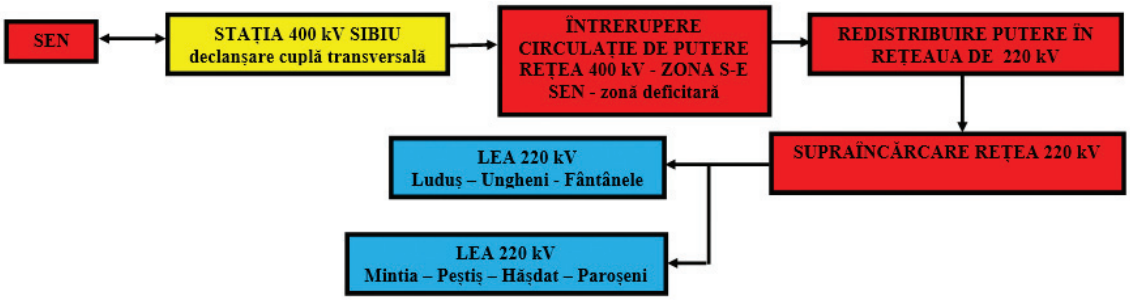

Figura 4 *Descriere tehnică – Eveniment 2*

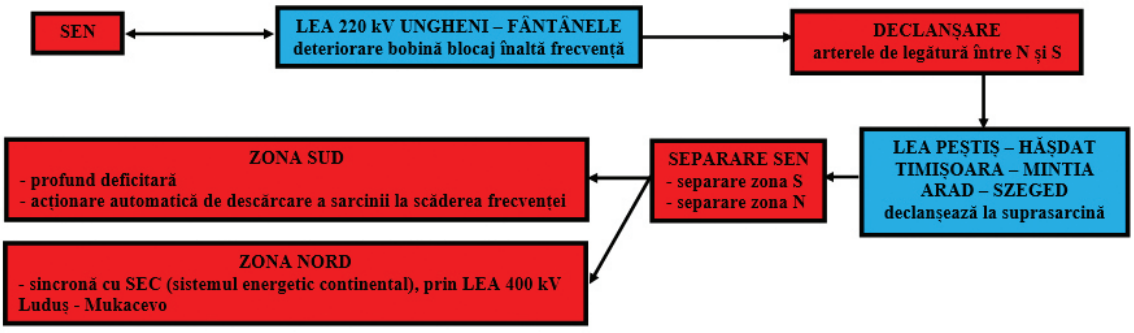

Figura 5 *Descriere tehnică – Eveniment 3*

scăderea frecvenței;

● zona de nord, sincronă cu SEC (sistemul electroenergetic continental) prin LEA de interconexiune (400 kV) Luduș – Mukacevo.

Eveniment 4:

În jurul orei 08:49, se conectează cupla de 400 kV, din stația 400 kV Sibiu, între subsistemele menționate ale SEN, funcționându-se asincron (Df=3Hz). Șocul produs de această conectare determină declanșarea liniilor 400 kV Luduș – Sibiu, Sibiu – Slatina, Sibiu – Brașov și a LEA 220 kV Pești – Cluj. Subsistemul de nord se împarte în două zone: zona CTE Mintia – Sibiu – Hunedoara și zona Cluj – Baia Mare, care funcționează în continuare cu LEA de interconexiune Luduș – Mukacevo. Subsistemul de sud, unde, în decurs de câteva minute, au declanșat (prin protecții tehnologice sau de suprasarcină) sau au fost deconectate manual (funcționând la parametri necorespunzători) toate grupurile generatoare, rămâne fără tensiune (cu excepția insulelor Galați, Palas și Chișcani). În sistemul de nord, încercarea de conectare a LEA 220 kV Hășdat, în stația Peștiș, și a LEA 400 kV Sibiu – Luduș a dus, din cauza nesincronismului, la declanșarea grupurilor CET Mintia.

Evenimente 1 + 2 + 3 + 4.

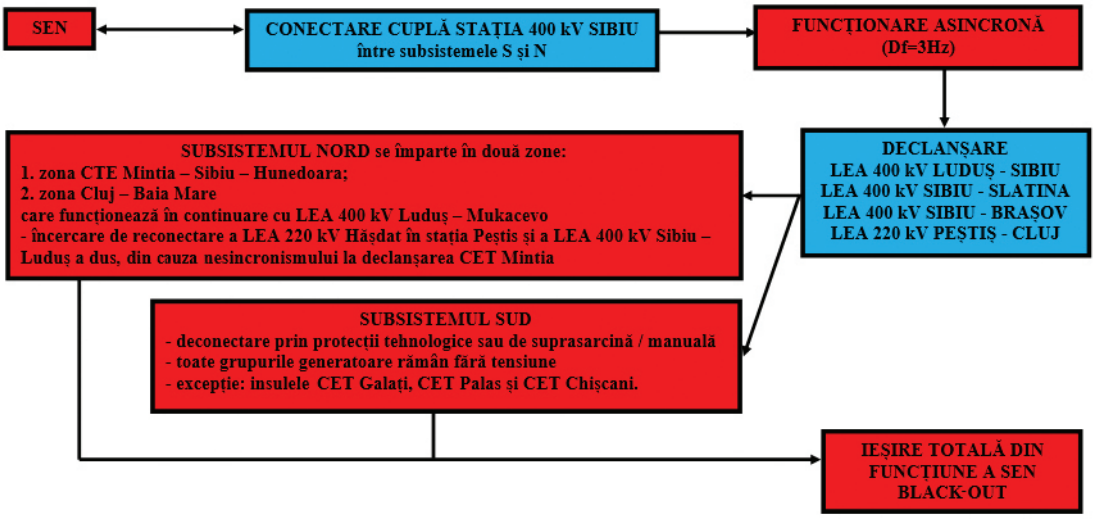

Figura 6 *Descriere tehnică – Eveniment 4*

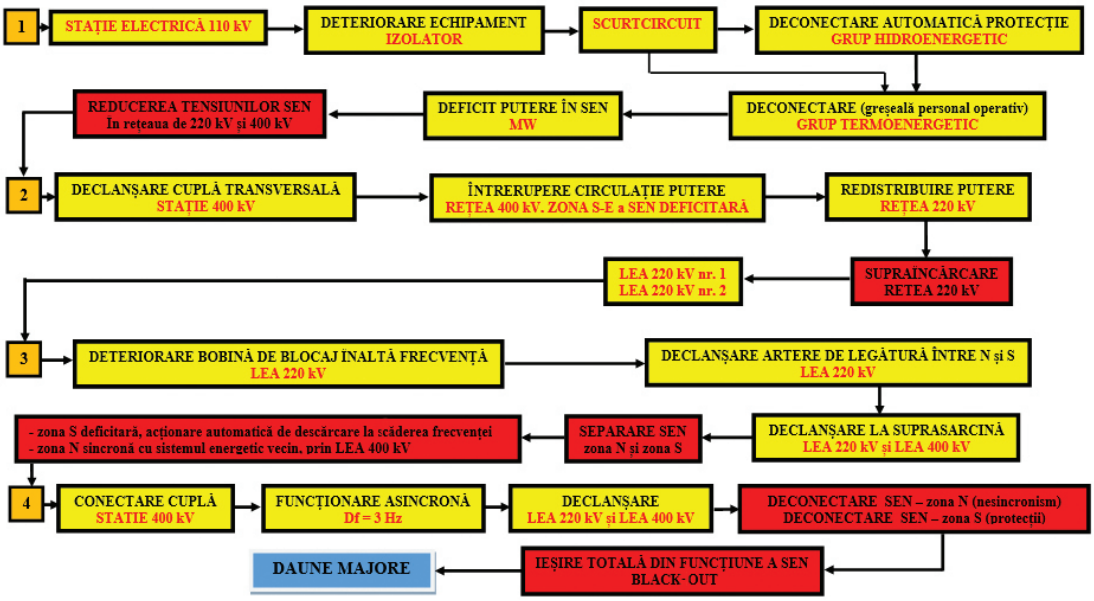

Figura 7 *Descriere tehnică – Evenimente 1 + 2 + 3 + 4*

Cuantificarea evenimentului

Banca Mondială a estimat o daună de circa 2 miliarde de dolari, iar analiza a fost făcută doar

estimativ, unde s-a folosit o cercetare (studiu) a Copenhagen Economics, pe baza datelor Eurostat și a prețurilor la energia electrică din 2016, publicată de Comisia Europeană. În această cercetare (studiu), se vorbește despre „value of lost – VoLL”, adică un cost al lipsei de energie, un indicator aproximativ care ține cont de foarte multe variabile (perioada din an sau zi în care are loc întreruperea, amploarea, cât de avansată este societatea, cum se consumă energia etc.) și în plus există diverse moduri de calcul al acestui indicator, de la țară, la țară. Studiul calculează pierderea în euro/kWh de energie neconsumată pentru consumatorii casnici și cei comerciali, iar la nivelul Uniunii Europene, rezultatele au o marjă extrem de mare, pentru consumatorii casnici variază de la 2 euro/kWh, în Bulgaria, la 32 euro/kWh, în Luxemburg, iar pentru consumatorii comerciali, de la 11 euro/kWh, în Bulgaria, la 67 euro/kWh, în Irlanda.

În România, în anul 2016, indicatorul era de 3 euro/kWh pentru consumatorul casnic și de 21 euro/kWh pentru consumatorul comercial (date pe baza prețurilor și a PIB din 2016), și cunoscând aceste date, s-a putut estima dauna acestui nefericit black-out, generalizat de 6 ore.

Puterea medie orară consumată în România a fost, la data de 23.01.2016, de 8.269 MW (consum mediu de 8.087 MWh), deci calculat la o medie de șase ore, consumul național a fost de 49.614 MWh, adică aproximativ 50 de milioane de kWh.

Dacă se consideră că estimarea de 28% din consum este reprezentată de consumatorii casnici, consumul total al acestora a fost de 14 milioane de kWh, iar restul de 36 de milioane de kWh se socotește comercial (aici, intră și consumul propriu tehnologic – CPT al Sistemului Energetic Național). Dacă valorile de studiu sunt medii, rezultă o VoLL de 42 de milioane de euro pentru populație și de 756 de milioane de euro pentru industrie, deci un black-out generalizat de energie electrică la nivel național, timp de șase ore, ar aduce daune economice (altele nu pot fi socotite) de cel puțin 800 de milioane de euro, din neutilizarea energiei electrice necesare activității economice și casnice, iar VoLL reprezintă doar valoarea economică a energiei neconsumate, nu și daunele provocate de oprirea alimentării cu energie electrică pentru industria națională, care sunt previzibile și, probabil, mult mai mari, dar care nu se pot calcula (N. D. Fîță 2019).

Concluzii

Un posibil și nedorit black-out național aduce daune extreme cetățenilor, societății, industriei și economiei naționale, instituțiilor abilitate cu situațiile de urgență, sanitare, ordine publică și securitate națională etc., provocând crize devastatoare și catastrofale, care pot aduce atingeri la adresa securității și bunăstării naționale.

Black-outul din 10 mai 1977 a avut efect de domino și a afectat următoarele sisteme și infrastructuri critice: sistemul medical (pierderi de vieți omenești), serviciile de urgență, poliția, pompierii, ambulanța, sistemul industrial (pierderi de vieți omenești, pierderi mari de producție din întreprinderi, fabrici, combinate siderurgice, combinate miniere etc.), ferme de animale, sistemul de alimentare cu apă potabilă, serviciul IT și comunicațiile, sistemul de extracție a petrolului și a gazelor naturale, sistemul financiar - bancar, sistemul de transport (aeroporturi, gări, porturi, metrou etc.), restaurantele, magazinele etc.

Cuantificarea acestor daune s-a raportat doar la lipsa alimentării cu energie electrică a consumatorilor finali, neluându-se în calcul interdependențele tuturor sistemelor critice ale economiei naționale față de energia electrică, acestea fiind necuantificabile.

O asemenea analiză și evaluare a pierderilor financiare, produse de un black-out electroenergetic, este absolut necesară pentru a înțelege importanța protejării infrastructurilor critice energetice, iar în acest context strategic, Parlamentul European și Consiliul European au emis *Regulamentul 941/05.06.2019 privind pregătirea pentru riscuri în sectorul energiei electrice.*

Prezentul regulament stabilește norme pentru cooperarea dintre statele membre în vederea prevenirii crizelor de energie electrică, pregătirii pentru astfel de crize și gestionării acestora, în spiritul solidarității și al transparenței, luând în considerare pe deplin cerințele unei piețe interne competitive a energiei electrice, în cadrul ENTSO-E, prin următoarele acțiuni majore:

Evaluarea riscurilor:

- evaluarea riscurilor la adresa siguranței alimentării cu energie electrică;
- metodologia de identificare a scenariilor regionale de criză de energie electrică;
- identificarea scenariilor regionale de criză

de energie electrică;

● identificarea scenariilor naționale de criză de energie electrică;

● metodologia pentru evaluările adecvării pe termen scurt și sezoniere;

● evaluările adecvării pe termen scurt și sezoniere.

Planurile de pregătire pentru riscuri:

● stabilirea planurilor de pregătire pentru riscuri;

● conținutul planurilor de pregătire pentru riscuri în ceea ce privește măsurile naționale;

● conținutul planurilor de pregătire pentru riscuri în ceea ce privește măsurile regionale și bilaterale;

● evaluarea planurilor de pregătire pentru riscuri.

Gestionarea crizelor de energie electrică:

● alerta timpurie și declararea unei crize de energie electrică;

● cooperare și asistență;

● respectarea normelor pieței.

Evaluare și monitorizare:

● evaluare ex post;

● monitorizarea;

● tratarea informațiilor confidențiale.

BIBLIOGRAFIE

Bănică, Alexandru, și Ionel Muntele. 2015. *Reziliență și teritoriu – operaționalizare conceptuală și perspective metodologice.* Iași: Editura Terra Nostra.

Comisia Europeană. 2017. „Comunicare comună către Parlamentul European și Consiliu.” *O abordare strategică privind reziliența în cadrul acțiunii externe a U.E.* http://www.cdep.ro/eu/examinare_pck.fisa_examinare?eid=528.

Fîță, Daniel Nicolae, Mihai Sorin Radu și Dragoș Păsculescu. 2021. *Asigurarea, controlul și stabilitatea securității energetice în contextul creșterii securității industriale și naționale.* Petroșani: Editura Universitas.

Fîță, Nicolae Daniel. 2020. *Cercetări privind identificarea vulnerabilităților infrastructurilor critice din cadrul Sistemului Electroenergetic Național de ultra și foarte înaltă tensiune cu conexiune internațională.* Teză de doctorat. Petroșani: Universitatea din Petroșani.

—. 2019. *Identificarea vulnerabilităților infrastructurilor critice din cadrul Sistemului electroenergetic național în contextul creșterii securității energetice.* Petroșani: Editura Universitas.

Fîță, Nicolae Daniel, Dragoș Păsculescu, Cristina Pupăză și Emilia Grigorie. 2022. „Metodologia de identificare, desemnare, analiză, evaluare, protecție și reziliență a infrastructurilor critice electroenergetice.” În *Managementul rezilienței în societatea contemporană*, de Olga Maria Cristina Bucovețchi (coordonatori) Diana Elena Ranf, 180-201. Sibiu: Editura Academiei Forțelor Terestre „Nicolae Bălcescu”.

Fîță, Nicolae Daniel, Sorin Mihai Radu, Dragoș Păsculescu, și Emilia Grigorie. 2021. „Abordarea infrastructurilor critice energetice naționale corelată rezilienței societale și sustenabilității.” În *Managementul sustenabilității și sustenabilitatea managerială între paradigme clasice și moderne*, de Olga Maria Cristina Bucovețchi, Dorel Badea (coordonatori) Diana Elena Ranf, 37-58. Sibiu: Editura Academiei Forțelor Terestre „Nicolae Bălcescu”.

MCEER. 2008. *Earthquake Engineering to Extreme Event – University at Buffalo.* http://www.buffalo.edu/mceer.