CONSIDERAŢII PRIVIND SECURITATEA CIBERNETICĂ A SISTEMELOR DE COMANDĂ ŞI PROTECŢIE ÎN REŢELELE ELECTRICE

Dr. ing. **Dragos DANUBIANU** [1], Dr. ing. **Alexandru MIRON** [2], Dr. ing. **Marian DRAGOMIR** [1], Prof. dr. ing. **Radu PENTIUC** [2], Conf. dr. ing. **Cezar POPA** [2], Conf. dr. ing. **Elena BOBRIC** [2]

[1] CN Transelectrica SA, [2] Universitatea „Ștefan cel Mare" din Suceava

REZUMAT. Întreruperile alimentării de energie electrică pot fi catastrofale asupra securităţii naţionale şi a economiei. Datorită complexităţii activelor dispersate şi interdependenţa dintre calculatore, sistemele de comunicaţie, şi sistemele energetice, cerinţa satisfacerii securităţii informatice este o problemă dificilă. Această lucrare se referă la problemele legate de securitate cibernetică necesare pentru sistemele de protecţie, automatizare, control şi comunicaţii din staţiile de transformare, precum şi metode ce ar putea fi utilizate, în scopul prevenirii unor atacuri informatice care pot avea un impact semnificativ asupra disponibilităţii sistemului electroenergetic cu consecinţe grave privind întreruperile pe arii extinse.

Cuvinte cheie: securitate cibernetică, protecție prin relee, amenințare cibernetică, risc.

ABSTRACT. Interruptions of electricity supply can be catastrophic on national security and the economy. Due to the complexity of assets dispersed and computers communication systems and energy systems interdependence, satisfying the requirement of cyber security is a difficult problem. This work relates to issues of cyber security required for protection, automation, control and communications in substations and methods that could be used in order to prevent attacks that may have a significant impact on electricity system availability, which could have serious breakdown consequences on extensive areas.

Keywords: cyber security, relay protection, cyber threat risk.

1. INTRODUCERE

Astăzi producerea, transportul, şi distribuţia energiei electrice sunt tot mai dependente de sistemele digitale, inclusiv sistemele de informaţii şi reţele de comunicaţii.

Această evoluţie introduce noi vulnerabilităţi in fiabilitatea alimentării cu energie electrică, bazate pe introducerea şi expunerea de vulnerabilităţi în sistemele digitale, şi de comunicaţii [1].

Sistemele de automatizare, protecţie şi control din staţii s-au schimbat în mod semnificativ în ultimul deceniu şi continuă să se schimbe ca urmare a progresele tehnologice. Sistemele au devenit mai interconectate oferind utilizatorilor finali informaţii multiple permiţând o fiabilitate mult mai mare şi niveluri de control mult mai mari. Interoperabilitatea între diferite sisteme şi produse ale furnizorilor a fost realizată prin dezvoltarea produselor şi soluţiilor bazate pe standarde deschise şi prin folosirea diferitelor tehnologii ca de exemplu tehnologia Ethernet standard. Schimbarea tehnologiilor electromecanice cu cele bazate pe microprocesor în sistemele de protecţii, control şi automatizare, a adus beneficii importante din punct de vedere al exploatării şi mentenanţei. În acelaşi timp această schimbare a permis acestor sisteme, abordarea problemelor de securitate cibernetică care nu exista în tehnologia clasică [2].

Cuvântul "securitate" a fost evocat în trecut ca fiind un sentiment ce aducea de imaginea de confort, protecţia fizică oferită de familie şi prieteni, perspectivele financiare stabile şi liniște sufletească. Cu toate acestea, în ultimii ani, imaginea cuvântului „securitate" s-a schimbat prin utilizarea acestuia în raport cu zona de calculatoare – ceea ce este cunoscut sub numele de securitate cibernetică. Securitatea nu a fost un subiect de îngrijorare când calculatoarele erau în fază incipientă lor, dar acum fiind o parte obişnuită şi integrantă a vieţii de zi cu zi în societatea noastră a devenit, din păcate, subiectul unor atacuri frecvente rău intenționate şi de vandalism electronic [3].

Industria energetică, ca şi restul societăţii, a profitat din plin de imensa putere oferită de calculator şi de tehnologia bazată pe microprocesor. Echipamente de protecţie şi control, SCADA, controlul de la distanţă şi monitorizare, precum şi multe alte aplicaţii sunt puse în aplicare în mod obişnuit cu această tehnologie. Securitatea cibernetică pentru sisteme de automatizare şi control în sectorul energetic a devenit în momentul actual o problemă ce trebuie să ne

preocupe din ce in ce mai mult. Alimentarea cu energie electrică este prea important pentru a fi lăsată într-o stare de vulnerabilitate şi neglijare [3].

Deşi infrastructura complexă oferă capabilităţi excelente de funcţionare, de control, şi de analiză, acestea cresc riscurile de securitate, incluzând securitatea informatică ameninţările şi vulnerabilităţile. Un atac cibernetic asupra sistemelor de calculatoare dintr-un centru de comandă şi ccontrol (dispecer zonal, teritorial), ar putea duce la operaţiuni de comutare nedorite, care ar conduce la întreruperi de energie electrică pe scară largă. Un alt scenariu de atac cibernetic îl constituie pătrunderea în staţiile de transformare a personalului neautorizat şi modificarea setărilor releelor de protecţie, ceea ce ar putea duce la acţiuni de comutare nedorite. În prezent, sistemul poate să nu prezinte măsuri puternice împotriva atacurilor cibernetice şi, prin urmare, există vulnerabilităţi. În consecinţă, există o cerere crescândă de a aborda aceste probleme cibernetice într-un mod cuprinzător şi sistematic [5].

IEEE şi alte standarde disponibile, răspund acestor cerinţe de securitate cibernetică . Este important să se ia în considerare aplicarea acestor standarde la IED-uri (Intelligent Electronic Devices) care sunt integrate în staţii şi echipamente de alimentare pentru a oferi comunicaţii securizate.

Privind la organizaţiile implicate în menţinerea securităţii sistemului de utilităţi (furnizori, distribuitori, utilizatorii finali) este corect să spunem că securitatea este o „problemă a tuturor“. În măsura în care aceste organizaţii cooperează una cu cealaltă de-a lungul ciclului de viaţă al sistemului, securitatea va fi îmbunătăţită. În acelaşi timp, poate cel mai important aspect de securitate pentru diferiţii actori din sistemul energetic este acela de a păstra în minte ideea că securitatea este o călătorie şi nu o destinaţie. Vor exista mereu noi ameninţări. Sistemul de control trebuie să fie pregătit pentru a se proteja de aceste ameninţări şi ia în considerare diferiţii adversari, hackeri, teroriști cibernetici, angajaţii nemulţumiţi sau neglijenţi / angajaţi slab pregătiţi. Cu toate acestea, teama de securitate cibernetică nu trebuie să împiedice introducerea sistemelor moderne de protecţie, control şi automatizare şi de comunicaţii în sistemele electroenergetice.

Vigilenţa, cooperarea şi expertizele tehnice, atunci când sunt aplicate la unison, oferă cea mai bună apărare.

2. PUNCT DE VEDERE PRIVIND SECURITATEA ŞI GESTIONAREA RISCURILOR

Securitatea informatică pentru sisteme de automatizare şi control a devenit un subiect foarte mare şi toată lumea pare să aibă o opinie cu privire la aceasta. Singurul lucru care pare să lipsească, este prin urmare o adevărată înţelegere a riscurilor reale. Informaţii detaliate privind incidentele reale sunt încă o raritate şi soluţiile se bazează de obicei pe decizii de tehnologie, mai degrabă decât pe o abordare bazată pe risc. Multe standarde, regulamente şi instrucţiuni există astăzi dar puţine dintre ele conţin o logică bazată pe evaluarea riscurilor sau modelare ameninţării. Factorul decisiv pentru dezvoltarea, achiziţionarea şi implementarea mecanismelor de securitate se bazează adesea pe respectarea reglementărilor, standardelor [2].

Pentru calcularea riscului, utilizatorii de servicii de electricitate au folosit în mod tradiţional următoarea formulă:

Riscul = Ameninţare × Vulnerabilitate × Impact

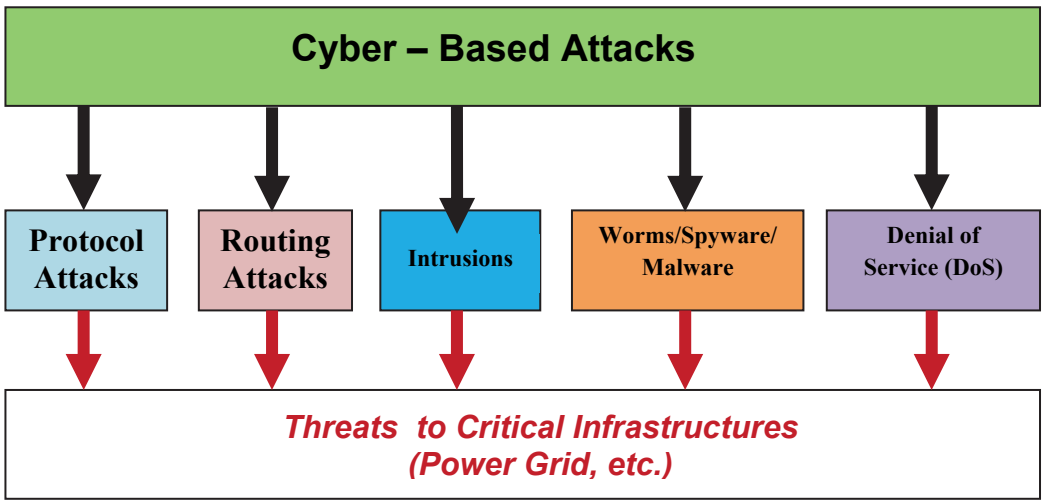
În această formulă variabilele utilizate pentru măsurarea riscului au următoarele explicaţii:

Ameninţare: Proliferarea unor atacuri informatice este de aşteptat să continue să crească în toate sectoarele economiei conectate digital. Pe măsură ce tot mai multe sisteme electroenergetice devin interconectate între ele şi cu alte domenii, expunerea la un potenţial atac cibernetic , devine din ce în ce mai mare.

Vulnerabilitate: Întotdeauna au existat o multime de vulnerabilităţi în reţelele electrice, dar în trecut au fost mai protejate în mod adecvat prin sisteme de protecţie fizică şi proceduri. Odată cu apariţia reţelei inteligente şi a altor reţele de informare şi comunicare, atacatorii nu mai au nevoie de ocolirea de protecţie pentru asigurarea securităţii fizice sau riscul de vătămare corporală. Sistemele moderne de protecţie, automatizare şi control oferă noi căi pentru hackeri pentru a ajunge la sistemele operaţionale critice. Vulnerabilitatea nu mai este specifică pentru locaţii şi echipamente folosite de către utilizatorii de servicii, şi atacurile pot fi lansate de oriunde din lume, cu o conexiune la internet.

Impact: Având în vedere faptul că energia electrică reprezintă o mare parte din viaţa modernă, distribuţia energiei electrice s-au concentrat asupra fiabilităţii, şi impactul potenţial de la orice fel de ameninţare de securitate a fost întotdeauna destul de mare. În trecut, ameninţările cibernetice nu constituiau o preocupare, deoarece atacatorii ar fi putut să ajungă la sistemele operaţionale importante. Astăzi, impactul asupra sistemelor critice privind încălcarea securităţii cibernetice creşte exponenţial astfel că operaţiunile sistemului electric deveni mai instrumentate şi interconectate [4].

Metodologiile de evaluare a riscului folosesc probabilitatea unei ameninţări şi impactul său potenţial ca un mijloc de a calcula riscul global.



Potențiali agenți de amenințare se întind de la intruziuni electronice, viruşi, malware etc., la terorismul cibernetic (fig. 1).

Terorismul cibernetic ar putea fi o amenințare reală. Este posibil, de asemenea, să nu fie, nu există pur şi simplu suficiente date pentru al confirma sau al nega. Adevărul este undeva la mijloc; securitatea cibernetică este o problemă reală, agenţi de amenintare există şi amenințările sunt o realitate.

3. SECURITATEA NU ESTE PERFECTĂ

Securitatea nu este perfectă şi nu va fi niciodată. Toate persoanele interesate în dezvoltarea şi îmbunătăţirea sistemelor de automatizare, protecţie şi control din staţiile de transformare trebuie să înţeleagă că aceste sisteme complexe vor avea vulnerabilităţi şi că securitate 100% nu este posibilă.

Faptul că nu există securitate 100%, înseamnă că vor exista întotdeauna încălcări şi incidente de securitate. Prin urmare, este extrem de important pentru a pune nu numai mecanisme de protecţie în loc, dar, de asemenea, mecanisme pentru detectarea rapidă de incidente şi care sunt în măsură să se reacţioneze în mod eficient în izolarea abuzurilor privind securitatea [2].

4. ACCESUL LA BAZELE DE DATE ALE DISPOZITIVELOR DE AUTOMATIZARE, PROTECȚIE ŞI CONTROL

Dispozitivele de protecţie, control şi automatizare amplasate în staţiile de transformare sunt dispersate în întregul sistemul energetic. Accesul la bazele de date ale acestor dispozitive este necesar pentru: evaluarea în mod continuu a stării de sănătate a sistemului; recunoaşterea problemelor de dezvoltare care pot afecta în mod negativ capacitatea sistemului de a rămâne operaţional; analiza funcţionării dispozitivelor de protecţie pentru a asigura corectitudinea şi menţine coordonarea pentru a preveni întreruperile în cascadă; identificarea unor posibile îmbunătăţiri ale sistemelor de protecţie; verificarea preciziei modelului sistemului, pentru a facilita studii de planificare.

Dispozitivele pentru care este nevoie de acces sunt:

- relee de protecţie bazate pe microprocesor;
- perturbografe digitale ;
- monitoare pentru perturbaţii dinamice;
- unităţi de măsură a fazorului (PMUs);
- RTU şi SCADA;
- calculatoarele staţiei;
- sisteme de securitate (incendiu, efractie etc).

Nivelul de acces necesar depinde de funcţia locului de muncă. Personalul de exploatare din centralele electrice şi staţiile de transformare trebuie să ştie în orice moment ce s-a întâmplat şi unde (modificări ale stării întreruptorului, sarcina elementelor sistemului, funcţionările releelor de protecţie şi semnalizările acestora, alarme, etc.).

Inginerii de protecţie de obicei au nevoie şi trebuie să intervină în sistemele de protecţii în scopul citirii datelor stocate (ale releului, perturbografului, înregistrări de evenimente şi înregistrările de setare, etc), în scopul de a analiza perturbaţiile sistemului, coordonarea regimurilor de protecţie, schimbări de reglaje de protecţie ca urmare a modificării configuraţiei sistemului energetic, etc.

Personalul de exploatare din staţii şi centrale electrice au acces la citire la toate dispozitivele de protecţie, şi automatizare. De asemenea în unele cazuri pot realiza unele setări determinate de inginerii de protecţie, pentru funcţionarea corectă a acestora.

Accesul la datele disponibile din sistem se face de la faţa locului dar de cele mai multe ori prin intermediul internetului. Poate fi de asemenea utilizată şi o conexiune dial-up pentru cerinţe mai puţin stricte. Accesul la reţeaua de date a companiei prin intermediul internetului ridică cel mai înalt nivel de preocupare pentru securitatea informatică [3].

Accesul la sistemele de protecţie şi consideraţii privind setările acestora

Relee de protecţie sunt punctele critice pentru sistemul energetic. Setările într-un releu determină răspunsul (sau non-răspunsul) dispozitivului şi setările incorecte poate avea efecte serioase asupra funcționării sistemului energetic.

În mod obişnuit, setările de releu sunt permise a fi schimbate doar de către personal de protectie, dar natura multifuncțională a releelor cu microprocesor a extins utilizarea dispozitivelor de protecție la alte grupuri.

Un releu modern poate înlocui un RTU dintr-o staţie furnizând pe lângă funcţia de protecţie, date de măsurare şi funcţii de control pentru deschiderea şi închiderea întreruptoarelor şi alte comutatoare. Releul modern poate fi de asemenea conectat la un calculator din stație care îndeplinește funcții de automatizare și control. Multifuncționalitatea releelor de protecţie moderne poate conduce la extinderea privilegiilor de setare a releelor şi de către alţi ingineri decât cei de protecţie ceea ce creează o provocare în plus pentru inginerul de protecție pentru a urmări, documente și de a verifica setările releului.

Proiectanţii de relee moderne recunosc nevoia de acces sporit la dispozitive și ofere unele mijloace pentru a ajuta inginerul de protecţie cu privire la modificările setărilor. Câteva exemple sunt:

- modificarea setărilor releelor bazate pe microprocesor trebuie să se facă cu parole.
- trebuie să existe un plan de reglaj pentru modificarea setărilor releului, iar releul trebuie să emită o alarmă atunci când a fost facută o setare a releului.
- mai multe niveluri de acces, cu diferite parole pentru fiecare nivel. de obicei, există un nivel numai pentru citire care pot fi accesate de către un număr mai mare de utilizatori, în timp ce nivelul superior pentru stabilirea modificări pot fi accesate numai de inginerul de protecţii.
- în releele cu mai multe grupuri de setări, setările în grupurile preverificate pot fi făcut de către personalul nespecialist în protecţii prin relee, în timp ce schimbarea parametrilor individuali trebuie făcută numai de inginerul de protecţie.

În timp ce procedurile de restricționare a accesului în staţia de transformare sau centrala electrică sunt bine stabilite, a crescut accesul de la distanţă la relee cu microprocesor care este mai puțin reglementată.

În releele de protecţie multifuncţionale inginerul de protecţii ar trebui să fie persoana responsabilă pentru toate setările de relee de protecție și documentare – inginerul de automatizare lucrând prin inginerul de protecție la implementarea setărilor de automatizare necesare.

De preferință, parolele de acces a releului ar trebui să fie stabilite pentru a permite accesul numai în vizualizare, pentru inginerii de automatizare, personalul de întreținere, operatorii de rețele, etc.

Un al doilea nivel, mai securizat, în care pot fi făcute schimbări de reglaje ca urmare a schimbărilor apărute în configuraţia sistemului, sau testări de echipamente, ar trebui să fie rezervate pentru ingineri de protecţii şi tehnicienii care fac testările.

Personalul contractor care testează echipamentele de protecţie prin relee pot utiliza parole temporare pentru a finaliza modificări ale setărilor şi testările necesare [3].

5. ABORDĂRI LA NIVEL ÎNALT ALE SECURITĂŢII

Securitatea sistemelor de automatizare, protecţie şi control din staţie trebuie să acopere atât aspectele fizice cât şi cele informatice. Protecția fizică include de exemplu, înființarea limitelor fizice, de exemplu, un gard, dulapuri închise sau instalarea de camere video în scopul monitorizării. Atât protecțiile fizice, cât şi cele cibernetică sunt necesare, dar în continuare vom pune accentul pe aspectele cibernetice.

Orice arhitectură de securitate trebuie să fie adaptată la instalația specifică și trebuie să se bazeze pe o evaluare a riscului de securitate.

Orice element mai slab dintr-un sistem de automatizare, protecţie şi control, trebuie să fie la fel de sigur ca şi elementele importante ale sistemului. Un atacator va încerca să găsească elementul cel mai slab, prin urmare, trebuie să se depună eforturi pentru a realiza o rezistență de apărare echilibrată între toate componentele sistemului și vectori de atac. Unul dintre primii paşi ar trebui să fie întotdeauna acela de a face o evaluare a arhitecturii sistemului, care include identificarea componentelor critice si toate conexiunile externe. Un sistem tipic de automatizare, protecţie şi de control modern dintr-o staţie, va avea cel puţin dispozitive la nivel de celulă, care utilizează protocoale de comunicare în timp real și sunt responsabile pentru furnizarea de informații sistemelor de calcul la nivel de staţie, care sunt folosite ca HMI sau gateway-uri pentru entități externe sau unități terminale îndepărtate care se conectează la centrelor de dispecer al sistemului energetic [2].

Principalele abordări ale securității sistemelor de protecţie, automatizare şi control împotriva atacurilor cibernetice sunt:

1. Apărare în profunzime. Cel mai important principiu pentru orice arhitectură de securitate este apărare în profunzime. Având un singur strat de apărare este destul de uşor ca orice mecanism de securitate să poată fi depăşit de către un atacator, şi prin urmare este recomandat arhitectului într-un mod oarecare ca cele mai sensibile părţi ale sistemului să

fie protejate prin mai multe inele de apărare care toate trebuie să fi încălcate de către atacator pentru a ajunge la zona protejată.

În plus, ar trebui să fie implementate nu numai mecanisme de protecţie, ci, de asemenea, mijloace de detectare a atacurilor. Aceasta include atât măsuri tehnice, cum ar fi sisteme de detectare a intruziunilor, precum şi măsuri procedurale, cum ar fi cele de revizuire a fişierelor jurnalului sau drepturilor de acces.

2. Separarea reţelei. Orice reţea de calculatoare ar trebui să fie împărţit în zone diferite, în funcţie de caracterul critic al nodurilor în cadrul fiecărei zone. Astfel, în cadrul sistemelor de automatizare, protecţie şi control din staţiile de transformare, ar putea fi prevăzute zone de separare pentru dispozitivele la nivel de celule, pentru dispozitivele la nivel de staţie şi pentru calculatoare. Zonele ar trebui să fie separate printr-un firewall, gateway, sau ceva similar.

În plus, reţeaua de automatizare pentru statii, protecţie şi control trebuie să fie clar separate de orice reţea externă. Acest lucru poate fi realizat prin utilizarea de exemplu a unui firewall pentru a controla accesul datelor la reţeaua de comandă. În scopul de a autentifica accesarea entităţilor, combinaţia dintre un firewall cu un gateway VPN (Virtual Private Network) este o soluţie bună. O arhitectură mai sigură este de a lucra cu o aşa-numită DMZ (zona demilitarizată); o zonă care serveşte ca un proxy între reţelele externe şi sistemul de control [2].

3. Perimetrul electronic. O altă soluţie de securitate a sistemelor de automatizare, protecţie şi control o constituie un perimetru electronic larg unde atacurile informatice pot fi filtrate şi traficul nedorit stopat înainte de a ajunge la poarta de acces a reţelei a zonei de separare. Acest perimetru extins poate fi format prin mai multe dispozitive IDS (Intrusion Detection Systems) de-a lungul unei arii largi. Volume mari de trafic pot fi manipulate de către un perimetru extins, astfel că ar fi posibil de a opri atacurile mai departe de reţeaua protejată. În plus, dispozitivele IDS de-a lungul perimetrului electronic ar putea forma o reţea de suprapunere (de exemplu, o reţea virtuală privată pe Internet) şi funcţionând într-un mod distribuit şi de colaborare, sprijinindu-se reciproc mai eficient în lupta împotriva atacurilor. Configurarea poate fi privită ca un gard electronic sau o barieră de protecţie perimetrală care permite numai traficul legitim pentru a ajunge la poarta de acces a reţelei [5].

4. Cele mai bune practici de securitate. Practicilor de securitate, cum ar fi politicile de funcţionare a calculatoarelor şi de gestionare a reţelei trebuie să fie definit în conformitate cu liniile directoare ale standardelor şi procedurilor specifice, cum ar fi: alegerea parolelor şi data expirării lor; utilizarea unui număr limitat de conturi de calculator privilegiate şi dezactivarea restului; închiderea porturi de comunicare nedorite şi computere; punerea în aplicare a mecanismelor de control al accesului; actualizarea frecventă a bazelor de date de semnături anti-virus.

6. CONCLUZII

Operaţiuni moderne de sistem electroenergetic sunt puternic dependente de tehnologia sistemelor informatice (IT), dintre care multe operează în timp real. Introducerea concurenţei şi separarea a adus multe organizaţii noi in sectorul energetic. O mare parte din interacţiunea între participanţii la sectorul energiei electrice se realizează prin intermediul sistemelor informatice. Există o mare varietate de mecanisme prin care ameninţările cibernetice - viruşi, viermi, etc. se pot propaga şi pot afecta integritatea sistemelor informatice. Este important ca fiecare entitate organizaţională în sectorul energiei să devine conştient de ameninţările la adresa securităţii cibernetice [6].

Securitate cibernetică a sistemelor de protecţii, automatizare şi control este o problemă extrem de importantă în sistemul energetic.

Securitatea este un proces în evoluţie şi nu este statică. Este nevoie de muncă continuă şi educaţie pentru a ajuta procesele de securitate pentru a ţine pasul cu cerinţele care vor fi plasate în sistemele electrice. Securitatea va continua să fie o cursă între politicile de securitate ale companiei şi entităţi ostile. Procesele şi sistemele de securitate vor continua să evolueze în viitor. Prin definiţie, nu există sisteme de comunicare care să fie 100% sigure. Întotdeauna vor exista riscuri reziduale care trebuie luate în considerare şi gestionate. Astfel, în scopul de a menţine securitatea, sunt necesare vigilenţă şi monitorizarea constantă, precum şi adaptarea la schimbările din mediul global.

BIBLIOGRAFIE

[1] J. Zerbs, L.R.Jouppi, G.Dondossola, C.Poirier, P.Sitbon, D.Holstein – *Status of cybersecurity* – Electra no.276, october, 2014.

[2] S.Kunsman, M.Braendle, Bart de Wijs, F.Hohlbaum – *Replacing Fear with Knowledge - Cyber Security for Substation Automation, Protection and Control Systems* – Texas A&M University, 68th Annual Conference for Protective Relay Engineers, 2015.

[3] S. Ward, J. O'Brien, B. Beresh, G. Benmouyal, a.s.o. - *Cyber Security Issues for Protective Relays* - Power Engineering Society General Meeting, IEEE, 2007.

[4] IBM - *Best practices for cyber security in the electric power sector* - http://www-935.ibm.com/services/multimedia/WR928534SF

[5] C.W.Ten, M.Govindarasu, C.Liu, - *Cyber-security for Electric Power Control and Automation Systems*- Systems, Man and Cybernetics, 2007. ISIC. IEEE International Conference.

[6] P. Roche - *Cyber security considerations in power system operations* - https://www.Documents/Downloads/Cyber+security+considerations+in+Power+system+operationID41VER28%20(3).pdf