EVALUAREA SIGURANȚEI SISTEMELOR DE SUPRAVEGHERE ȘI CONTROL A TRENURILOR BAZATE PE COMUNICAȚII (CBTC)

SAFETY ASSESSMENT OF SURVEILLANCE AND CONTROL SYSTEMS OF TRAINS BY COMMUNICATIONS (CBTC)

Alexandru BADEA[1], Gabriel POPA[2], Adrian Ioan MUNTEAN[3]
Victor Mihai POPA[4], Constantin BIBIRE[5], George DUMITRU[6]

[1]Universitatea Politehnica București, Splaiul Independenței nr. 313, București, România
e-mail: Alexandru BADEA: alexsinaia@yahoo.com

[2,5]Universitatea Politehnica București, Splaiul Independenței nr. 313, București, România
e-mail: Gabriel POPA: gabi21popa@yahoo.com; Constantin BIBIRE: constantin.bibire@yahoo.com
[3,6]Autoritatea Feroviară Română - Calea Griviței nr. 393, sectorul 1, București, România,
e-mail: Adrian Ioan MUNTEAN: adrianmuntean67@yahoo.com; George DUMITRU, george.dumitru.cfr@gmail.com
[4]Cargo Trans Vagon SA, str. „Vaselor", no. 34, sectorul 2, București, România,
e-mail autor: Victor Mihai POPA: pvmmihai@yahoo.com,

Rezumat: *Sistemele de control al trenurilor bazate pe comunicații (CBTC) nu mai sunt izolate de lumea exterioară și deoarece folosesc alte rețele pentru creșterea eficienței și îmbunătățirea randamentului, ele sunt expuse la amenințări cibernetice foarte mari. În această lucrare se propune un model generalizat de rețea Petri stohastică (GSPN) pentru a capta interacțiunea dinamică dintre agresor și apărător pentru a evalua securitatea sistemelor CBTC. În funcție de caracteristicile sistemului și de metodele de atac - apărare, modelul a fost împărțit în două faze: penetrare și perturbare. În fiecare fază, s-au furnizat mijloace eficiente de atac și măsurile defensive corespunzătoare, iar starea sistemului a fost determinată în mod corespunzător. În plus, au fost propuse o platformă de simulare semifizică și un model de joc pentru a ajuta la parametrizarea modelului GSPN. Cu probabilitatea la starea de echilibru a rezultatelor sistemului din model, propunem mai mulți indicatori pentru evaluarea securității sistemului. În cele din urmă, s-a comparat securitatea sistemului cu măsuri defensive unice și cu măsuri defensive multiple. Evaluările au indicat importanța măsurilor defensive și gravitatea situației de securitate a sistemului..*
Cuvinte cheie: *atac, comunicații, penetrare, perturbare, rețea, risc, siguranță, sisteme.*

Abstract: *Communication-based train control systems (CBTC) are no longer isolated from the outside world and because they use other networks to increase efficiency and improve efficiency, they are exposed to very high cyber threats. This paper proposes a generalized model of stochastic Petri net (GSPN) to capture the dynamic interaction between the aggressor and the defender to assess the security of CBTC systems. Depending on the characteristics of the system and the methods of attack - defense, the model was divided into two phases: penetration and disruption. In each phase, effective means of attack and appropriate defensive measures were provided, and the state of the system was determined accordingly. In addition, a semi-physical simulation platform and a game model were proposed to help parameterize the GSPN model. With the equilibrium probability of the system results in the model, we propose several indicators for evaluating the system security. Finally, the security of the system was compared with single defensive measures and multiple defensive measures. The assessments indicated the importance of defensive measures and the seriousness of the security situation of the system.*
Keywords: *attack, communications, penetration, disruption, network, risk, safety, systems.*

1. INTRODUCERE

Traficul urban feroviar a cunoscut o dezvoltare considerabilă, odată cu progresul modernizării urbane și a evoluțiilor tehnologice în domeniul transporturilor.

Drept consecință a dezvoltării zonelor urbane și creșterii semnificative a populației, traficul urban feroviar este supus unei presiuni deosebite [1]. Cercetătorii au creat sistemul de control al trenurilor bazat pe comunicații, îmbinând comunicațiile moderne, tehnologie de control, software dedicat, computere și tehnologia tradițională de semnalizare pentru a dezvolta eficiența și capacitățile operaționale [2, 3].

Sistemul CBTC are multe caracteristici în comparație cu sistemele de semnalizare feroviare tradiționale, cum ar fi calcularea cu precizie a locației trenului, independent de circuitele de cale și comunicații de date bidirecționale, de mare capacitate prin sistemul de culegere a datelor de la marginea căii [4]. Acesta este un sistem automat de control al trenurilor care utilizează o varietate de tehnologii, software și echipamente avansate pentru a se asigura că trenurile operează la distanțe minime de siguranță pentru o capacitate maximă de transport [5-7]. Sistemul CBTC, are în prezent peste 100 de instalații în întreaga lume și este unul dintre cele mai populare sisteme de semnalizare printre operatorii de transport feroviar de astăzi [8].

Sistemul CBTC conține multe informații și are un număr extrem de mare de componente în rețea, riscul atacurilor cibernetice fiind inevitabil [9]. Vulnerabilitățile tehnologiei fără fir, viruși de rețea, amenințările persistente avansate și vulnerabilitățile cu risc ridicat în dispozitive sunt câteva dintre problemele de securitate cu care se confruntă acest sistem. Incidentele de securitate a informațiilor în traficul feroviar urban nu au întârziat să apară. La începutul anului 2012 au fost atacate, sistemul de eliberare a informațiilor stației de metrou Shanghai Shentong și rețeaua wireless a sistemului de operare și expediere. În noiembrie 2012, sistemul de semnalizare a metroului Shenzhen a fost perturbat, ceea ce a dus la frânări de urgență frecvente la mai multe trenuri în timpul mersului. În 2016, hackerii au atacat sistemul informatic de tarife al metroului din San Francisco și l-au folosit pentru a șantaja. Aceste incidente au avut un impact uriaș asupra traficului urban, au perturbat ordinea traficului și au adus pierderi economice uriașe.

Traficul urban feroviar este o infrastructură urbană semnificativă, care este strâns legată de viața oamenilor. Când apar probleme de securitate la traficul feroviar urban, frânările de urgență sunt inevitabile, și poate perturba funcționarea trenului, crește presiunea traficului urban și poate cauza pierderi economice uriașe. În plus, pot avea loc deraieri sau coliziuni ale trenurilor, ceea ce va duce la vieți nemăsurabile și daune materiale. Prin urmare, este semnificativ să surprindem interacțiunile dintre atac și apărare și să analizăm securitatea sistemelor CBTC. În acest fel, mai mulți cercetători și experți din industrie pot realiza importanța securității pentru sistemul CBTC și cum să îmbunătățească securitatea sistemului.

Traficul urban feroviar este o infrastructură urbană semnificativă, care este strâns legată de viața oamenilor. Când apar probleme de securitate în tranzitul feroviar urban, frânarea de urgență poate apărea pe tren, ceea ce poate perturba funcționarea trenului, crește presiunea traficului urban și poate cauza pierderi economice uriașe. În plus, pot avea loc deraieri sau coliziuni ale trenurilor, ceea ce va duce la pierderi de vieți omenești și daune materiale. Prin urmare, este semnificativ să surprindem interacțiunile dintre atac și apărare și să analizăm securitatea sistemelor CBTC. În acest sens, mai mulți cercetători și experți din industrie pot realiza importanța securității pentru sistemul CBTC și cum să îmbunătățească securitatea sistemului.

Pe baza continuității serviciilor de operare de tranzit feroviar urban, Wang et al. [10] a propus o abordare de evaluare a securității bazată pe reziliență care împarte riscurile de securitate în trei faze: pre-atac, atac și post atac. În [11], a fost propusă o metodă de analiză cuprinzătoare a securității și siguranței bazată pe defecte extinse. Această lucrare a sintetizat caracteristicile de siguranță și securitate ale sistemului de control al trenului în traficul feroviar urban, a analizat cuprinzător amenințările și vulnerabilitățile de securitate și sursele de pericol ale sistemului de control al trenului și a analizat relația dintre riscurile de securitate și riscurile de siguranță.

Dong și colabotatorii [12] a folosit de atacul pentru a evalua vulnerabilitatea unui sistem CBTC pe baza topologiei rețelei, a structurii redundante și a principiilor de funcționare. Evaluările au acoperit stările actuale de securitate, auditarea porturilor, politicile de parole și protocoalele de comunicare ale sistemelor. Ferrari și colaboratorii [13] au propus un model de rețele de activitate stohastică (SAN) pentru a efectua o evaluare a disponibilității sistemelor CBTC. Lee și colaboratorii [14] au definit cerințele de securitate luând în considerare caracteristicile sistemului de control ale trenului și au analizat riscul de atac.

Sistemul CBTC este un tip de sistem ciber-fizic (CPS) format din două componente majore: un proces fizic și un sistem cibernetic [15]. Pentru a analiza impactul comportamentului ofensiv și defensiv asupra sistemelor CBTC, ne referim și la rezultatele cercetării sistemelor ciber-fizice. În [16], a fost utilizată o metodă de cerințe nefuncționale (NFR) pentru a evalua siguranța și securitatea CPS. Intuitivitatea abordării NFR a permis să identificăm motivele pentru securitatea slabă și să identificăm tehnicile care vor ajuta la îmbunătățirea securității. Mitchell și colaboratorii [17] a simulat interacțiunea dinamică între comportamentul de atac și apărare al sistemelor ciber-fizice pe baza unui model stohastic de rețele Petri. În plus, lucrarea a analizat impactul intervalului de detectare a intruziunilor și al puterii de atac asupra mediei timpului total de funcționare (MTTF) al rețelei electrice modernizate. În plus, în [18, 19], autorii au folosit teoria jocurilor pentru a descrie procesul de schimbare a stării CPS sub strategiile atacatorilor și apărătorilor. Mai mulți indicatori cantitativi, cum ar fi probabilitatea la starea de echilibru și MTTF, au fost aplicați pentru a evalua fiabilitatea sistemului. Depoy și colaboratorii [20] a descris o metodologie de evaluare funcțională de sus în jos pentru evaluarea riscurilor sistemului în cadrul a patru tipuri de atacuri: atacuri cibernetice numai fizice, atacuri fizice activate cibernetic, doar cibernetice și atacuri cibernetice activate fizic. În [21, 22], a fost utilizat un model Markov ascuns (HMM) pentru a descrie dinamica stohastică a CPS-urilor în scenariul de atac. În plus, autorii din [23-25] au analizat o situație de securitate a rețelei inteligente bazată pe Q-learning, care poate afișa bine procesul de confruntare atac-apărare.

Referindu-ne la procesul de atac în mai multe etape pentru CPS, am împărțit procesul de atac al sistemelor CBTC în două faze: faza de penetrare și faza de perturbare [26]. În faza de penetrare, atacatorul invadează sistemul printr-o abordare cu fir sau fără fir, iar sistemul nu va fi deteriorat substanțial. După invazia reușită, atacatorul lansează daune fizice substanțiale sistemului, iar atacul intră în faza de perturbare. În această lucrare, putem înțelege mai bine vulnerabilitatea sistemului prin cercetarea etapizată a procesului de atac.

În această lucrare, am utilizat o rețea Petri stohastică generalizată (GSPN) pentru a descrie comportamentul de atac și apărare și schimbările în starea sistemului [27-28]. Am ales câteva atacuri tipice împotriva sistemului CBTC și apărările corespunzătoare pentru a îmbogăți modelul. Spre deosebire de lucrările despre analiza securității CPS, s-au folosit strategii concrete de atac și apărare în loc de strategii generale, cum ar fi atac și fără atac. Modelul propus nu numai că se conformează caracteristicilor CPS, dar combină și

caracteristicile CBTC cu schimbările de stat și alegerile de strategie. Pentru a simula mai precis atacul și apărare în sistemul CBTC, s-a apelat la teoria jocului.

Rezolvând echilibrul Nash [29], s-a obținut probabilitatea ca atacatorul și sistemul să aleagă strategia de atac și apărare, care este cea mai probabilă alegere de comportament pentru factorii de decizie de ambele părți sub premisa rațională. Făcând acest lucru, putem obține un model GSPN complet. Am efectuat exerciții de atac și apărare pe platforma de simulare semi-fizică a laboratorului pentru a ajuta la parametrizarea modelului. Modelul nostru GSPN poate fi combinat cu un proces Markov în timp continuu. Putem obține probabilitatea la starea de echilibru a sistemului în fiecare stare prin rezolvarea lanțului Markov. În final, se pot propune câțiva indicatori de securitate pentru a evalua securitatea sistemelor CBTC în confruntare atac-apărare pe baza rezultatelor soluției model.

2. STRATEGIILE DE ATAC-APĂRARE ÎN SISTEMELE CBTC

2.1. Sistemul CBTC propriu zis

Sistemul CBTC este compus în principal din echipamente de bord și echipamente de la marginea căii (figura 1) [30-31]. Echipamentele de bord includ echipamente de protecție automată a trenului (ATP) și echipamente de operare automată a trenului (ATO) pentru monitorizarea funcționării trenurilor, poziționarea măsurării vitezei și interacțiunea om-calculator. Echipamentele de pe marginea căii includ un controler de zonă (ZC), supraveghere automată a trenului (ATS), interblocare cu computer (CI) și o unitate de stocare a bazei de date (DSU).

ATS este împărțit în ATS central și ATS stație.

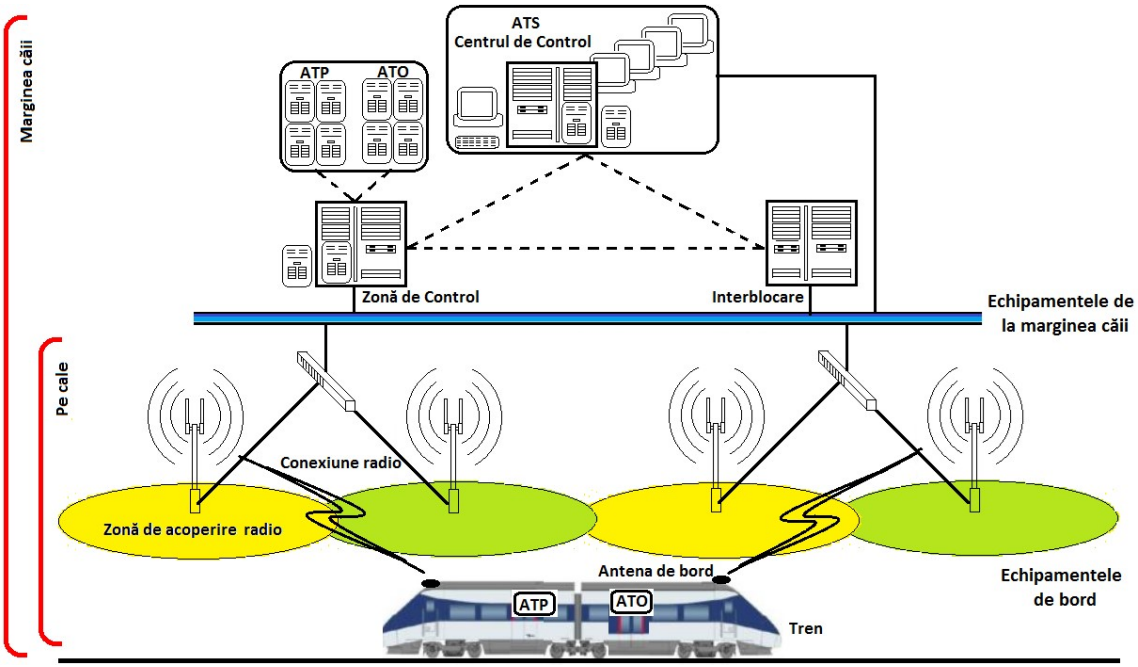

Fig. 1. Componente CBTC (ATS - Supravegherea automată a trenurilor;
ATO - Operare automată a trenului; ATP - Protecție automată a trenului).

Sistemul de comunicare de date (DCS) al sistemului CBTC este format din două părți: rețeaua principală și rețeaua de acces radio. Rețeaua principală oferă canale transparente de

transmisie a datelor pentru echipamentele de la sol. Majoritatea rețelelor de acces fără fir existente ale sistemului CBTC utilizează echipamente de rețele locale fără fir (WLAN) bazate pe IEEE 802.11 pentru a realiza transmisia în timp real a informațiilor bidirecționale și de mare capacitate ale vehiculului. Pentru a îndeplini cerințele de înaltă disponibilitate ale sistemului CBTC, DCS adoptă o arhitectură de redundanță a rețelei de inel. Atunci când o rețea nu poate funcționa normal din cauza defecțiunii echipamentului, sistemul poate trimite și primi date printr-o altă rețea. În același timp, rețeaua backbone de la sol este împărțită în mai multe subrețele diferite în funcție de diferite subsisteme. În general, este împărțit în cinci rețele, două rețele de semnalizare redundante, două rețele ATS redundante și o rețea de întreținere. Rețeaua ATS conectează ATS central și stația ATS și comunică cu rețeaua de semnal prin gateway-ul ATS. Rețeaua de întreținere constă în distribuirea mașinilor de întreținere și centre de întreținere pentru diagnosticarea defecțiunilor și întreținerea de rutină.

2.2. Riscurile de securitate în sistemele CBTC

Un număr mare de componente de rețea și informații sunt utilizate în sistemul CBTC, cum ar fi tehnologia de comunicație, tehnologia computerelor generale, tehnologia de control, Windows comercial, un sistem de operare VxWorks și protocoale de comunicație standard TCP/IP. Utilizarea acestor tehnologii avansate a îmbunătățit considerabil nivelul de automatizare și informare al sistemului CBTC, dar a introdus și noi riscuri de securitate în sistem. Principalele riscuri de securitate a informațiilor ale sistemului CBTC sunt următoarele:

- riscuri legate de protocolul de comunicare. În prezent, DCS-urile utilizează tehnologia WLAN pentru a finaliza comunicarea fără fir. WLAN funcționează în banda medicală științifică industrială deschisă (ISM) și există vulnerabilități în tehnologiile cheie, cum ar fi autentificarea, criptarea și transmisia [32]. Punctele slabe ale rețelelor WLAN în sine oferă posibilitatea atacurilor de tip denial of service (DoS) și a atacurilor de bruiaj [33];
- riscuri ale sistemului de operare. Unele servere și gazde din sistemul CBTC folosesc sisteme comerciale precum Windows și VxWorks. Aceste sisteme comerciale au multe vulnerabilități. Prin exploatarea vulnerabilităților, atacatorul poate obține privilegii de sistem, sisteme de blocare și execuție de cod la distanță [34];
- riscurile echipamentelor de rețea [35]. Sistemul CBTC utilizează un număr mare de echipamente de rețea ca noduri pentru schimbul de informații, cum ar fi comutatoare sau gateway-uri. Dacă aceste noduri de schimb de informații cheie sunt atacate, comunicarea în rețea va fi afectată.

Hackeri care folosesc aceste riscuri de securitate pot cauza defecțiuni ale echipamentelor, întreruperi ale comunicării și opriri ale serviciului. Datorită designului redundant și principiului de siguranță al sistemului CBTC, siguranța traficului urban feroviar poate fi garantată. Cu toate acestea, sub atac, mecanismul sensibil de siguranță va reduce eficiența trenului și va perturba traficul. Când echipamentul eșuează sau comunicarea este întreruptă, mecanismul de siguranță va porni frânarea de urgență a trenului, ceea ce poate introduce pierderi economice uriașe. Prin urmare, analiza de securitate pentru sistemele CBTC este un semnificativă.

2.3. Strategia de atac-apărare a sistemelor CBTC

Pentru a simula în mod realist procesul de interacțiune dintre atacator și apărător, am selectat mai multe metode de atac pentru sistemul CBTC și am dezvoltat măsuri defensive

corespunzătoare.

Conform vulnerabilității WLAN [39], atacatorii pot sparge parola WLAN pentru a invada rețelele wireless. Datorită rețelei fără fir și rețelei cu fir din rețeaua de semnal fiind conectate, atacatorul a invadat cu succes intranetul CBTC, punând bazele următoarelor lor daune fizice. Punctul slab al tehnologiei WLAN constă în metoda sa de criptare: Wi-Fi protected access (WPA) [36]. Pachetele de handshake WPA care sunt transmise în text clar includ mulți parametri, cum ar fi adresa MAC a clientului, BSSID (identificatorul de set de servicii de bază) al AP, MIC (codul de integritate a mesajului) și așa mai departe. MIC-ul clientului care este egal cu MIC-ul AP este obținut prin parola WLAN și acești parametri printr-un algoritm specific. Prin urmare, putem folosi dicționarul de parole pentru a calcula MIC-ul în combinație cu parametrii din pachet și îl putem compara cu MIC-ul AP-ului (punctul de acces). Dacă cele două sunt la fel, parola este parola rețelei wireless, ceea ce indică că am invadat rețelele de semnalizare. Condiția prealabilă pentru spargerea cu succes a parolei este ca sistemul să folosească o parolă slabă. O parolă complexă necesită un dicționar extins și mult timp pentru a se sparge. Prin urmare, strategia de apărare împotriva acestui atac este schimbarea dinamică a parolelor puternice.

Sistemul de operare VxWorks este utilizat pe scară largă în echipamentele de semnalizare, iar vulnerabilitatea de depanare eoliană (WDB) este o vulnerabilitate specifică sistemului care poate fi utilizată de un atacator pentru a citi sau modifica locații de memorie arbitrare, pentru a efectua apeluri de funcție sau pentru a gestiona sarcini. Dispozitivele care utilizează sistemul de operare VxWorks se vor reporni dacă exploatăm vulnerabilitatea pentru a iniția programul de repornire. S-a simulat acest tip de atac împotriva controlerului de bord al vehiculului (VOBC) pentru a întrerupe comunicarea dintre AP și VOBC. Pentru a face față acestui atac, putem instala un anumit patch.

ARP spoofing este o tehnologie de atac pentru un protocol de rezoluție a adresei Ethernet (ARP). Acest tip de atac permite unui atacator să obțină pachete în LAN sau chiar să modifice pachetul și poate împiedica un anumit computer sau toate computerele din rețea să se conecteze corect. S-a adoptat un atac de falsificare ARP pentru a întrerupe comunicarea dintre ZC și CI. Mai întâi, s-a trimis un pachet de răspuns ARP, care conține IP-ul real și adresa MAC falsă a ZC, către CC (controlerul de comunicare) al CI.

Un atac SYN flood este un atac de tip denial of service (DoS) bazat pe defectele protocolului TCP. Când TCP inițiază o conexiune, trebuie să treacă prin trei constrângeri. Dacă un client trimite un număr mare de solicitări SYN către server și nu returnează între timp un pachet ACK, atunci va exista un număr mare de solicitări SYN pe partea serverului, ceea ce va afecta un număr mare de servere, aceste resurse fiind ocupate, astfel încât alți utilizatori normali să nu poată accesa serverul în mod normal. S-a folosit extensia fluxului SYN pentru a epuiza resursele serverului CC din ZC pentru a atinge scopul de a întrerupe comunicarea ZC. S-a folosit un firewall pentru a apăra atacul. Un cookie este atribuit fiecărei adrese IP a conexiunii de solicitare. Dacă un pachet SYN duplicat al aceluiași IP este primit într-o perioadă scurtă de timp, pachetul de la adresa IP va fi eliminat.

Cele de mai sus sunt metoda de atac și apărare pentru sistemul CBTC din această lucrare. Prin urmare, se stabilesc seturile de strategii ale atacatorului și al apărătorului în faza de penetrare și faza de perturbare.

3. SECURITATEA SISTEMULUI CBTC ÎN CAZ DE ATACURI -APĂRARE

Propunem un model analitic al securității sistemului în cazul atacurilor și schemelor de contra-apărare. Cadrul general al modelului este prezentat în figura 2. S-a folosit

probabilitatea în stare de echilibru a sistemului obținută prin modelul GSPN pentru a analiza și evalua mai mulți indicatori ai securității sistemului.

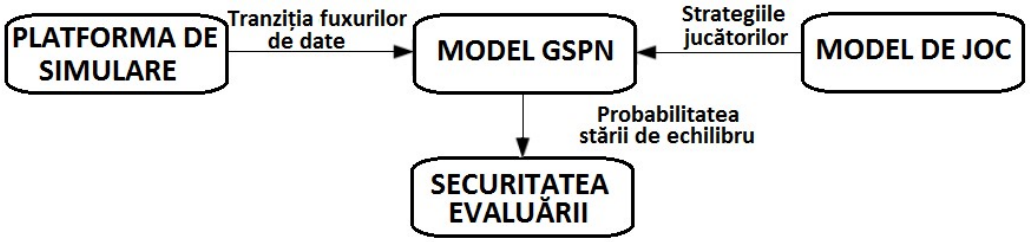

Fig. 2. Cadrul general al modelului.

3.1. Modelul rețelei Petri stohastice generalizate

Rețelele Petri sunt potrivite pentru descrierea modelelor de sisteme asincrone, concurente [37]. SPN este folosit în mod uzual pentru a modela anumite procese de afaceri în pe toată durata desfășurării acestora [38-40]. Modelul propus analizează disponibilitatea sistemului prin descrierea schimbărilor în starea sistemului în confruntarea atac-apărare.

Modelul a fost împărțit în două faze: penetrare și perturbare, în funcție de procesul de atac al atacatorului. Faza de penetrare este procesul prin care un atacator invadează din extranet către intranet. Numai prin accesarea la rețeaua de control intern a sistemelor CBTC, cum ar fi rețelele ATS și rețelele ATC, atacatorii pot deteriora sistemele. Este bine cunoscut faptul că sistemele de control industrial, cum ar fi sistemele CBTC, sunt relativ apropiate în comparație cu Internetul. De fapt, odată cu integrarea continuă a industrializării și informatizării, sistemele de control industrial folosesc din ce în ce mai mult protocoale de comunicații standardizate și hardware și software, precum și controlul de la distanță și operarea prin Internet, rupând închiderea și specializarea sistemului original [41, 43]. Prin urmare, este posibil ca un atacator să invadeze o rețea de control industrial. Chiar dacă rețeaua de control industrial este complet izolată fizic de rețeaua externă, mai avem o modalitate de a o scăpa. Virusul Stuxnet din SUA este un exemplu [44].

Rețeaua de transmisie fără fir între tren și sol a devenit abordarea noastră de a invada sistemul CBTC. Am folosit vulnerabilitățile WLAN [45] pentru a accesa rețelele de control CBTC, și anume rețelele de semnalizare. În plus, există următoarele metode de intruziune: virus transmis prin disc flash USB și conexiune la rețea prin cablu. Pentru a simplifica modelul pentru cercetare, s-a adoptat metoda intruziunii wireless. În schimb, avem și mai multe modalități de a combate acest atac. În ceea ce privește hardware-ul, NFC (comunicarea în câmp apropiat) este utilizat în unele telefoane mobile pentru a lega magnetic date într-un interval de doar un inch și ar putea fi integrat în sistemele de alimentare ale trenului, așa cum ar putea asigura în mod similar „sinapsele” optice la legăturile dintre vagoanele trenului. În plus, o antenă ELF (frecvență extrem de joasă) nou dezvoltată ar putea fi capabilă să evite majoritatea tentativelor de hacking, permițând în același timp o legătură de date de comunicație fără fir de lungimea trenului. În ceea ce privește software-ul, metoda utilizată în această lucrare este de a îmbunătăți puterea parolei rețelei wireless.

Modelul fazei de penetrare este prezentat în figura 3, iar descrierea parametrilor este prezentată în tabelul 1. La început, sistemul este într-o stare normală P_N, ceea ce înseamnă că sistemul CBTC funcționează normal. Apoi, atacatorul își va decide strategia și își va alege comportamentul. În mod corespunzător, apărătorul își va decide strategia și își va alege comportamentul.

Acesta este un proces de confruntare între atacator și apărător. Dacă atacatorul lansează un atac de intruziune fără fir și apărătorul nu are rezistență, sistemul va intra în starea de intruziune P_I, ceea ce indică faptul că atacatorul a intrat cu succes în intranetul sistemului CBTC. În schimb, dacă apărătorul ia măsuri defensive, atacatorul va eșua. În acest caz, sistemul nu va fi afectat de atac, iar atacatorul trebuie să suporte pierderea atacului eșuat.

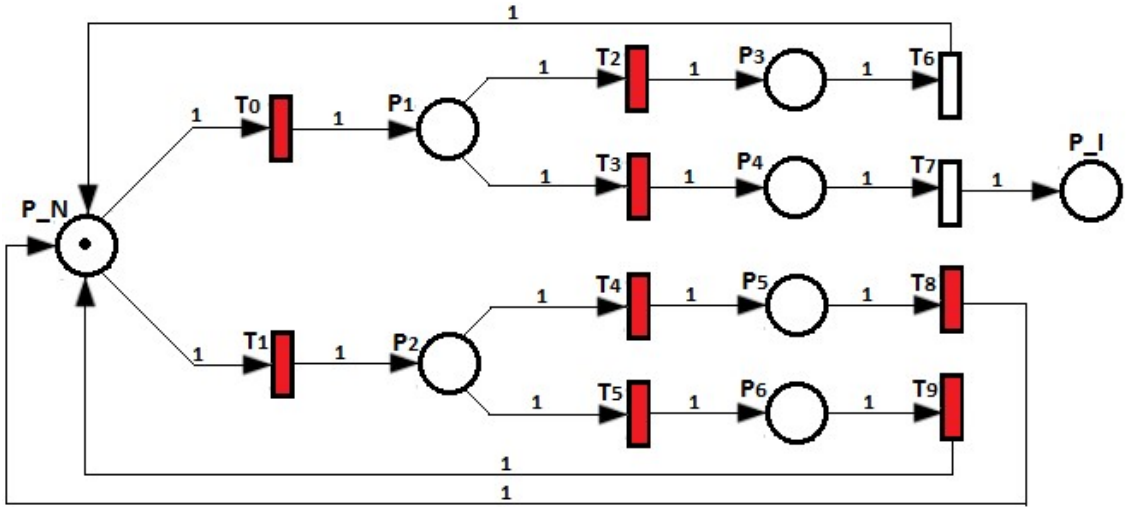

Fig. 3. Model de confruntare atac-apărare în faza de penetrare.

Tabelul 1. Parametrii modelului în faza de perturbare.

Parametri	Tip	Sens fizic
P_N	Locație	Sistemul este într-o stare normală
P1/ P2/ P3/ P4/ P5/ P6	Locație	Stare intermediară de confruntare atac-apărare
P_I	Locație	Atacatorul invadează cu succes sistemul
T0	Tranziție imediată	Atacatorul alege să inițieze un atac de intruziune fără fir
T1	Tranziție imediată	Atacatorul nu lansează un atac
T2/ T4	Tranziție imediată	Apărătorul adoptă o parolă puternică în rețeaua wireless
T3/ T5	Tranziție imediată	Apărătorii nu iau măsuri defensive
T8/ T9	Tranziție imediată	Sistemul rămâne normal fără atac
T6	Tranziție cronometrată	Procesul de atac cu succes
T7	Tranziție cronometrată	Procesul atacului eșuat

Faza de perturbare se bazează pe faptul că sistemul a fost invadat. Nu are rost să se ia în considerare faza de întrerupere dacă starea sistemului nu poate trece la starea de intruziune. În faza de penetrare, atacatorul nu a efectuat încă atacul dăunător împotriva sistemului și, prin urmare, atacatorul trebuie să efectueze atacuri dăunătoare specifice asupra sistemului. Datorită contribuției fazei de penetrare, atacatorul poate iniția daune pe intranetul sistemului CBTC. Diverse vulnerabilități ale sistemului sunt expuse atacatorului, în special unul care are o înțelegere a arhitecturii interne a sistemului în faza de perturbare.

Modelul fazei de perturbare este prezentat în partea dreaptă a figurii 4, iar descrierea parametrilor este prezentată în tabelul 2. La fel ca în faza de penetrare, atacatorul alege comportamentul de atac, iar apărătorul ia contramăsuri, iar apoi starea sistemului se schimbă. Faza de întrerupere începe de la locul P_I, ceea ce indică faptul că atacatorul a intrat în rețeaua internă a sistemului. În acest caz, atacantul și apărătorul aleg comportamente pentru jocul atac-apărare cu o anumită probabilitate.

Costul atacului ia în considerare calea atacului, complexitatea atacului și dacă este necesară autentificarea. Costul apărării ia în considerare complexitatea apărării și apărarea

împotriva efectelor negative. Pierderea sistemului în faza de întrerupere este determinată de pierderea distanței de rulare în cazul frânării de urgență și a funcționării degradate.

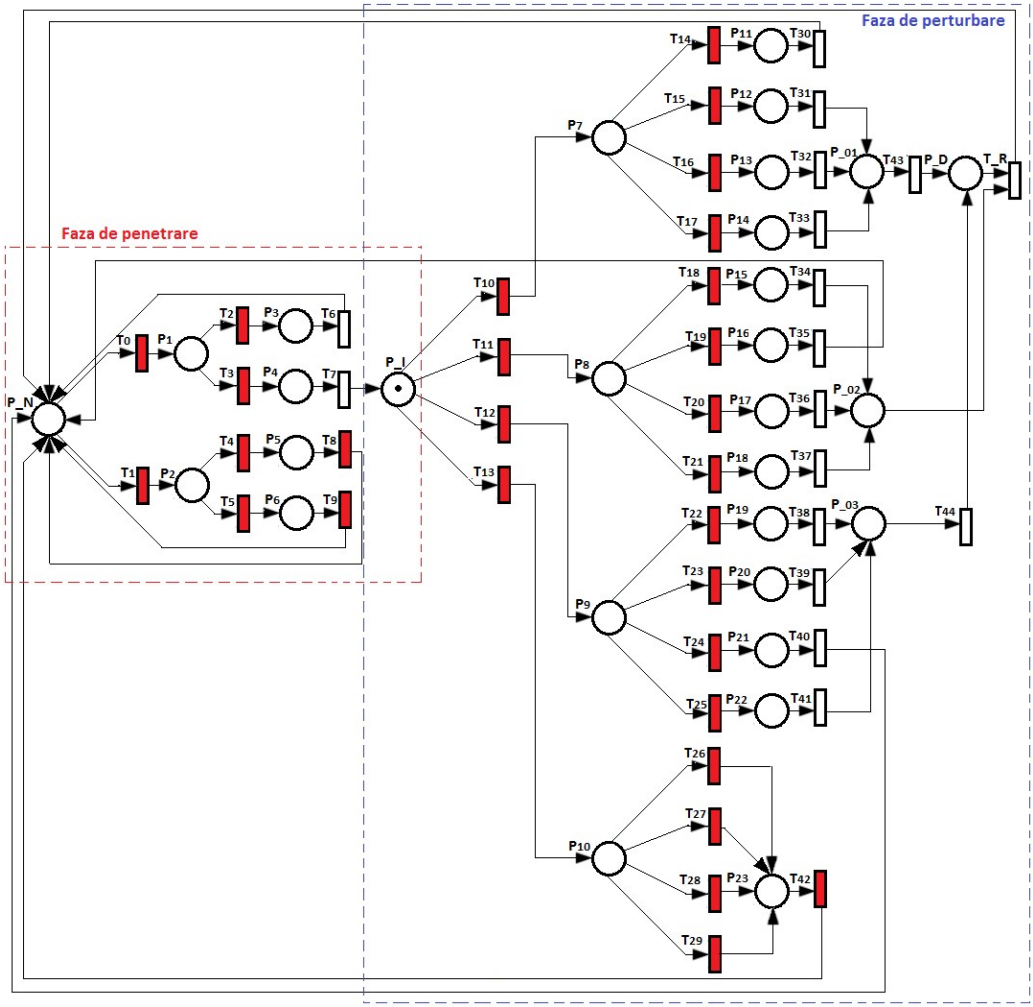

Fig. 4. Model de confruntare atac-apărare.

Următorul proces de confruntare atac-apărare este următorul:

- dacă atacatorul adoptă un comportament (A) și apărătorul nu răspunde cu un comportament defensiv corect, frânarea de urgență a trenului este iminentă, deoarece comunicarea dintre VOBC și AP este întreruptă. Trenul poate fi repornit, după oprire, și își poate relua mersul în modul BLOC (control bazat pe blocuri);
- dacă atacatorul adoptă un comportament (B) și apărătorul nu răspunde cu un comportament defensiv corect, atacatorul întrerupe comunicarea dintre ZC și CI, ceea ce face ca sistemul să ordone frânarea de urgență a trenului. Mai mult decât atât, trenul nu poate funcționa în modul BLOC deoarece CI nu poate controla sistemul în mod automat;
- dacă atacatorul adoptă un comportament (C) și apărătorul nu răspunde cu un comportament defensiv corect, sistemul CBTC va intra din nou în starea de frânare de urgență, deoarece ZC este anihilat de către atacator. În acest caz, trenul poate fi repornit, după oprire, și poate funcționa în modul BLOC (control bazat pe blocuri);
- dacă măsura defensivă a apărătorului funcționează, starea sistemului va reveni la starea normală. O măsură defensivă funcționează doar pentru un tip de atac (în general);

- după o defecțiune a sistemului, acesta va reveni în cele din urmă la normal după o perioadă, care este descrisă de tranzitul temporizat T_R.

Tabelul 2. Parametrii modelului în faza de perturbare.

Parametri	Tip	Sens fizic
P_N	Locație	Sistemul este într-o stare normală
P11-23/ P7-10	Locație	Stare intermediară de confruntare atac-apărare
P_I	Locație	Atacatorul invadează cu succes sistemul
P_B1/ P_B2/ P_B3	Locație	Starea de frânare de urgență a trenului
P_D	Locație	Stare de funcționare degradată a trenului
T10	Tranziție imediată	Atacatorul inițiază un atac de vulnerabilitate WDB
T11	Tranziție imediată	Atacatorul inițiază un atac de falsificare ARP
T12	Tranziție imediată	Atacatorul inițiază un torent de atacuri
T13	Tranziție imediată	Atacatorul nu lansează nici un atac
T14/ T18/ T22/ T26	Tranziție imediată	Instalarea corecțiilor de către apărător
T15/ T19/ T23/ T27	Tranziție imediată	Legarea IP-MAC de către apărător
T16/ T20/ T24/ T28	Tranziție imediată	Protecții de apărare
T17/ T21/ T25/ T29	Tranziție imediată	Apărătorii nu iau măsuri defensive
T42	Tranziție imediată	Sistemul rămâne normal fără atac
T31-34/ T36-39/ T41	Tranziție cronometrată	Procesul de atac cu succes
T30/ T35/ T40	Tranziție cronometrată	Procesul atacului eșuat
T33/ T34	Tranziție cronometrată	Procesul de funcționare a trenului este degradat
T_R	Tranziție cronometrată	Procesul sistemului revine la normal

Deoarece modelul GSPN este izomorf cu lanțul Markov în timp continuu (CTMC), am găsit o modalitate de a rezolva modelul. Prin transformarea modelului în CTMC, putem analiza probabilitatea în stare de echilibru a modelului. În rețelele Petri trebuie eliminate stările care se asociază cu tranziția imediată [46]. Timpul în care simbolul rămâne în aceste stări se apropie de zero; prin urmare, aceste stări nu au probabilitate de stare staționară. Conform teoremei de corelare a distribuției staționare a lanțului Markov și a ecuației Chapman-Kolmogorov [47], obținem:

$$WQ = 0, W = \left[P(M_0), P(M_1)\right], ..., P(M_k) \tag{1}$$

$$\sum_{i}^{k} P(M_i) \tag{2}$$

unde W este vectorul de probabilitate în stare de echilibru al markerului de lanț Markov M_i care reprezintă starea de echilibru a sistemelor CBTC. Q este o matrice a vitezei de transfer cu elementul $q_{ij}(i, j = 0,1,...,k)$. Dacă $i \neq j$, q_{ij} este egal cu viteza de la M_i la M_j și când $i = j$, q_{ij} este egal cu inversul sumei ratei arcurilor M_i. În plus, rata de la M_i la M_j se obține prin înmulțirea ratei de tranziție λ cu probabilitatea alegerii unei tranziții imediate π. După cuantificarea parametrilor precum λ și π, putem obține probabilitatea la starea de echilibru.

3.2. Modelul jocului atac-apărare

Prin modelul jocului atac-apărare putem prezice comportamentul atacatorilor și apărătorilor și obținem strategiile ambilor jucători. Credem că atacatorul nu este o persoană nesăbuită care urmărește orbește veniturile, ci un om înțelept care ia în considerare pe deplin câștigurile și pierderile, iar apărătorul este rațional în mod similar. Pentru modelul de confruntare atac-apărare, ambii jucători sunt raționali în procesul jocului de atac-apărare și urmăresc să-și maximizeze veniturile, acesta fiind criteriul lor de alegere a comportamentului

de atac-apărare. Deoarece profitul atacantului și al apărătorului se bazează pe eliminarea adversarului, nu există nici un câștig între cei doi jucători, adică nu există un echilibru Nash de strategie pură. Pentru a prezice modul în care jucătorii raționali își vor alege comportamentele și vor juca jocul, trebuie să rezolvăm echilibrul Nash cu strategia mixtă.

$U^a\left(\Phi^{ai},\Phi^{dj}\right)$ reprezintă funcția de plată a atacatorului sub comportamentul atacatorului Φ^{ai} şi comportamentul apărător Φ^{dj}. $U^d\left(\Phi^{ai},\Phi^{dj}\right)$ reprezintă funcția de plată a apărătorului sub comportamentul atacatorului Φ^{ai} și comportamentul apărătorului Φ^{dj}. În aceste condiții se poate obține câștigul specific al atacatorului și al apărătorului prin următoarele ecuații:

$$U^a\left(\Phi^{ai},\Phi^{dj}\right)=R_a-C_a \tag{3}$$

$$U^d\left(\Phi^{ai},\Phi^{dj}\right)=R_d-C_d \tag{4}$$

unde C_a și R_a reprezintă costul și returnarea comportamentului de atac, iar C_d și R_d reprezintă costul și returnarea comportamentului de apărare.

CONCLUZII

În această lucrare, am propus un model generalizat de rețea Petri stohastică pentru a surprinde procesul de confruntare atac-apărare într-un sistem CBTC. Am împărțit acest proces în două faze, fază de penetrare și faza de perturbare în funcție de caracteristicile sistemului și metodelor de atac-apărare. Întregul model de analiză de securitate a constat din modelul GSPN, teoria jocurilor și platforma de simulare semi fizică. Folosind probabilitatea la starea de echilibru a rezultatelor sistemului din model, am propus mai mulți indicatori precum disponibilitatea și MTTSF pentru evaluarea securității sistemului.

Prin urmare, operatorul de sistem ar trebui să depună mult efort pentru a rezista invaziei atacatorului de la extranet la intranet, folosind un LTE-M mai eficient și mai sigur în locul rețelelor WLAN.

Apărarea fazei de distrugere este la fel de importantă deoarece atacatorii interni și anumite atacuri speciale de bruiaj pot sări direct faza de penetrare pentru a deteriora sistemul.

Pe baza etapelor atacurilor, metricile de reziliență sunt utilizate pentru a analiza nivelul de securitate al întregii linii de metrou, unde sunt luate în considerare atât spațiul cibernetic, cât și spațiul fizic. Rezultatele simulării arată că abordarea bazată pe reziliență poate evalua eficient nivelul de securitate al sistemelor CBTC în cadrul diferitelor atacuri.

Pentru un sistem urban de traficul feroviar care are legătură cu mijloacele de trai ale oamenilor, o astfel de securitate este prea scăzută. Se poate specula cauza acestui rezultat ca fiind aportul insuficient de apărare. În această lucrare apărătorii au folosit o singură măsură defensivă la un moment dat. Apoi, apărătorul folosește măsurile combinate pentru a finaliza procesul de confruntare atac-apărare. Deoarece metodele ofensive și defensive sunt unice în timpul fazei de penetrare, s-a realizat o combinație a metodelor de apărare din faza de perturbare.

Măsurile de apărare combinate pot într-adevăr îmbunătăți securitatea sistemului. Prin urmare, din motive de securitate, operatorii de tranzit feroviar urban ar trebui să investească masiv în apărarea sistemului. De exemplu, dezactivarea porturilor de echipamente neutilizate, instalarea de corecții de vulnerabilitate și implementarea de firewall-uri în perimetrul rețelei sunt semnificative pentru a îmbunătăți securitatea sistemului.

BIBLIOGRAFIE

[1] **S. Gao, Y. Hou, H. Dong, S. Stichel, S.; B. Ning,** „*High-speed trains automatic operation with protection constraints: a resilient nonlinear gain-based feedback control approach*", IEEE/CAA J. Autom. Sin. 2019, 6, 992-999.

[2] **X. Wang, L. Liu, T. Tang, W. Sun,** „*Enhancing Communication-Based Train Control Systems Through Train-to-Train Communications*", IEEE Trans. Intell. Transp. Syst. 2018, 20, 1544-1561.

[3] **A. Neacşa, D.B. Stoica,** *„*Aspects concerning the software applications in order to determine the technological systems reliability*",* MOCM The 13th International Conference of Fracture Mechanics, 4 (13), 2007.

[4] **C. Schifers, G. Hans,** „*IEEE standard for communications-based train control (CBTC) performance and functional requirements"*, In Proceedings of the Vehicular Technology Conference Proceedings, VTC, Tokyo, Japan, 15-18 May 2000; pp. 1581-1585.

[5] **X. Wang, R.Y. Fei, Z. Li, T. Tao, B. Ning,** „*Cognitive Control Approach to Communication-Based Train Control Systems*", IEEE Trans. Intell. Transp. Syst. 2015, 16, 1676-1689.

[6] **A. Neacsa, N.N. Antonescu, D.B. Stoica,** *„Software Applications for Complex Technological Systems Reliability",* Journal of the Balkan Tribological Association, 15 (1), 2009.

[7] **A. Neacsa, N.N. Antonescu, D.B. Stoica,** *„Modern Solutions for Selecting the Corresponding Machinery Dedicated to Technological Applications",* Journal of the Balkan Tribological Association, 15 (4), 2009.

[8] **J. Farooq, J. Soler,** „*Radio Communication for Communications-Based Train Control (CBTC): A Tutorial and Survey*", IEEE Commun. Surv. Tutor. 2017, 19, 1377-1402.

[9] **W. Knowles, D. Prince, D. Hutchison, J.F.P. Disso, K. Jones, K.** „*A survey of cyber security management in industrial control systems*", Int. J. Crit. Infrastruct. Prot. 2015, 9, 52-80.

[10] **H. Wang, M. Ni, S. Gao, F. Bao, H. Tang,** „*A Resilience-Based Security Assessment Approach for Railway Signalling Systems*", In Proceedings of the 2018 37th Chinese Control Conference (CCC), Wuhan, China, 25-27 July 2018; pp. 7724-7729.

[11] **S. Yi, H. Wang, Y. Ma, F. Xie, P. Zhang, L. Di,** „*A Safety-Security Assessment Approach for Communication-Based Train Control (CBTC) Systems Based on the Extended Fault Tree*", In Proceedings of the 2018 27th International Conference on Computer Communication and Networks (ICCCN), Hangzhou, China, 30 July-2 August 2018; pp. 1-5.

[12] **H. Dong, H. Wang, T. Tang,** „*An attack tree-based approach for vulnerability assessment of communication-based train control systems*", In Proceedings of the 2017 Chinese Automation Congress (CAC), Jinan, China, 20-22 October 2017; pp. 6407-6412.

[13] **A. Ferrari, M.L. Itria, S. Chiaradonna, G.O. Spagnolo,** „*Model-Based Evaluation of the Availability of a CBTC System*", In Software Engineering for Resilient Systems; Avgeriou, P., Ed.; Springer: Berlin/Heidelberg, Germany, 2012; pp. 165-179.

[14] **J. Lee, C. Jang, O. Yi,** „*Analysis of radio based train control system using LTE-R and analysis of security requirements: The security of the radio based train control system*", In Proceedings of the 2017 4th International Conference on Computer Applications and Information Processing Technology (CAIPT), Kuta, Bali, 8-10 August 2017; pp. 1-4.

[15] **E.K. Wang, Y. Ye, X. Xu, S.M. Yiu, L.C.K. Hui, K.P. Chow,** „*Security Issues and Challenges for Cyber Physical System*", In Proceedings of the IEEE/ACM Intl Conference on Green Computing & Communications & International Conference on Cyber, Beijing, China, 20-25 September 2010.

[16] **N. Subramanian, J. Zalewski,** „*Quantitative Assessment of Safety and Security of System Architectures for Cyberphysical Systems Using the NFR Approach*", IEEE Syst. J. 2016, 10, 397-409.

[17] **R. Mitchell, I. Chen,** „*Modeling and Analysis of Attacks and Counter Defense Mechanisms for Cyber Physical Systems*", IEEE Trans. Reliab. 2016, 65, 350-358.

[18] **K. Lalropuia, V. Gupta,** „*Modeling cyber-physical attacks based on stochastic game and Markov processes*", Reliab. Eng. Syst. Saf. 2019, 181, 28-37.

[19] **H. Orojloo, M.A. Azgomi,** „*A Stochastic Game Model for Evaluating the Impacts of Security Attacks Against Cyber-Physical Systems*", J. Netw. Syst. Manag. 2018, 26, 929-965.

[20] **J. Depoy, J. Phelan, P. Sholander, B. Smith, G.B. Varnado, G.;** *Wyss, „Risk assessment for physical and cyberattacks on critical infrastructures*", In Proceedings of the Military Communications Conference, Atlantic City, NJ, USA, 17-20 October 2005.

[21] **S. Zonouz, K.M. Rogers, R. Berthier, R.B. Bobba, W.H. Sanders,T.J. Overbye,** „*SCPSE: Security-Oriented Cyber-Physical State Estimation for Power Grid Critical Infrastructures*", IEEE Trans. Smart Grid 2012, 3, 1790-1799.

[22] **D. Shi, R.J. Elliott, T. Chen,** „*On Finite-State Stochastic Modeling and Secure Estimation of Cyber-Physical Systems*", IEEE Trans. Autom. Control 2016, 62, 65-80.

[23] **J. Wu, K. Ota, M. Dong, J. Li, H. Wang,** „*Big data analysis-based security situational awareness for smart grid*", IEEE Trans. Big Data 2016, 4, 408-417.

[24] **Z. Ni, S. Paul,** „*A Multistage Game in Smart Grid Security: A Reinforcement Learning Solution*", IEEE Trans. Neural Netw. Learn. Syst. 2019, 1-12.

[25] **Y. Chen, S. Huang, F. Liu, Z. Wang, X. Sun,** „*Evaluation of reinforcement learning-based false data injection attack to automatic voltage control*", IEEE Trans. Smart Grid 2018, 10, 2158-2169.

[26] **H. Orojloo, M.A. Azgomi,** „*A game-theoretic approach to model and quantify the security of cyber-physical systems*", Comput. Ind. 2017, 88, 44-57.

[27] **C.N. Eparu, S. Neacșu, A. Neacșa,** *„Correlation of Gas Quality with Hydrodynamic Parameters in Transmission Networks"*, MATEC Web of Conferences, 290 (1), 2019.

[28] **C.N. Eparu, S. Neacsu, A.P. Prundurel, R. Rădulescu, A. Neacșa,** *„Behaviour of transmission and distribution networks with big consumption, the stress test",* IOP Conference Series: Materials Science and Engineering, 595 (1), 2019.

[29] **B. Qu, J. Zhao,** „*Methods for solving generalized Nash equilibrium*", Journal of Applied Mathematics, 2013.

[30] **A. Badea, G. Popa, I.A. Muntean, M. Vălu, C.N. Badea, G. Dumitru,** „*Sisteme de comunicații radio pentru controlul trenurilor bazat pe comunicații - CBTC*", Sinteze de Mecanică Teoretică și Aplicată, Volumul 11 (2020), nr. 4, pp.249-272.

[31] **A. Neacsa, D.B. Stoica, N.N. Antonescu,** *„Studies on the Use of Implemented Databases on Web Platforms in Order to Verify Machines Compatibility with Working Conditions",* Journal of the Balkan Tribological Association, 18 (4), 2014.

[32] **L. Zhu, H. Liang, H. Wang, B. Ning, T. Tang,** *„Joint Security and Train Control Design in Blockchain-Empowered CBTC System",* IEEE Internet of Things Journal, Volume: 9, Issue: 11, 01 June 2022, page(s): 8119 – 8129.

[33] **X. Wang, H. Jiang, T. Tang, H. Zhao,** „*The QoS Indicators Analysis of Integrated EUHT Wireless Communication System Based on Urban Rail Transit in High-Speed Scenario*", Wirel. Commun. Mob. Comput. 2018.

[34] **L. Zhu, Y. Li, F.R. Yu, B. Ning, T. Tang, X. Wang** „*Cross-layer defense methods for jamming-resistant CBTC systems*", IEEE Transactions on Intelligent Transportation Systems (Volume: 22, Issue: 11, November 2021, pp. 7266 - 7278.

[35] **M.G. Petrescu, A. Neacsa, A. Dinita,** *„The Risk Management and the Decisional Activity",* Annales Universitatis Apulensis Series Oeconomica 3 (8), 2006.

[36] **W. Wu, B. Bu, W. Zhang,** „*Attacks and Counter Defense Mechanisms for CBTC Systems: System Modeling and Availability Analysis*", IEEE Intelligent Transportation Systems Conference (ITSC), 2019.

[37] **R. Robidoux, H. Xu, L. Xing, M. Zhou,** „*Automated Modeling of Dynamic Reliability Block Diagrams Using Colored Petri Nets*", IEEE Trans. Syst. Man Cybern. Part A Syst. Hum. 2010, 40, 337-351.

[38] **C.N. Eparu, A. Neacșa, A.P. Prundurel, R. Rădulescu, C. Slujitoru, N. Toma, M. Nițulescu,** *„Analysis of a high-pressure screw compressor performances"*, IOP Conference Series: Materials Science and Engineering, 595 (1), 2010.

[39] **C.N. Eparu, S. Neacsu, A. Neacșa, A.P. Prundurel,** *„The comparative thermodynamic analysis of compressor's energetic performance"*, Mathematical Modelling of Engineering Problems, 6 (1), 2019.

[40] **Y. Xia, X. Luo, J. Li, Q. Zhu,** „*A Petri-Net-Based Approach to Reliability Determination of Ontology-Based Service Compositions*", IEEE Trans. Syst. Man Cybern. Syst. 2013, 43, 1240-1247.

[41] **Y. Xia, Y. Liu, J. Liu, Q. Zhu,** „*Modeling and Performance Evaluation of BPEL Processes: A Stochastic-Petri-Net-Based Approach.*", IEEE Trans. Syst. Man Cybern. Part A Syst. Hum. 2012, 42, 503-510.

[42] **N.N. Antonescu, M.I.A. Naboulsi, M.G. Petrescu, A. Neacsa,** *„Behaviour of Metal-Rubber Couplings or any other Plastic Materials in Translational Motion under Wear Generating Conditions"*, Journal of the Balkan Tribological Association, 12 (4), 2006.

[43] **M. Taheri, N. Ansari, J.Feng, R. Rojas-Cessa, M. Zhou, M.,** „*Provisioning Internet Access Using FSO in High-Speed Rail Networks*", IEEE Netw. 2017, 31, 96-101.

[44] **L. Zhu, Y. Li, F.R. Yu, B. Ning, T. Tang, X. Wang** „*Cross-layer defense methods for jamming-resistant CBTC systems*", IEEE Transactions on Intelligent Transportation Systems, Volume: 22, Issue: 11, November 2021, pp. 7266 - 7278.

[45] **W. Zhang, B. Bu, H. Wang,** „*An intrusion detection method of data tampering attack in communication-based train control system*", IEEE Intelligent Transportation Systems Conference (ITSC), 2019.

[46] **T. Xu, T. Tang,** „*The modeling and analysis of data communication system (DCS) in communication based train control (CBTC) with colored Petri nets*", Eighth International Symposium on Autonomous Decentralized Systems (ISADS'07), 2007.

[47] **W. Wu, B. Bu, W. Zhang,** „*Attacks and counter defense mechanisms for cbtc systems: System modeling and availability analysis*", IEEE Intelligent Transportation Systems Conference (ITSC), 2019.