Securitatea datelor în instalații fixe de alimentare ale sistemului de tracțiune electrică feroviară

Data security in fixed power installations of the railway electric traction system

Cristina Gabriela Sărăcin[1]

[1]Universitatea Polithnica din Bucureşti
Splaiul Independenței Nr.313, Romania
E-mail: cristina.saracin@upb.ro

Rezumat.– *Această lucrare prezintă o soluție viabilă pentru securitatea datelor în cadrul instalațiilor fixe de alimentare ale sistemului de tracțiune electrică feroviară. Transmiterea informațiilor din proces către structurile de control, supraveghere și achiziții de date (SCADA) se face prin rețeaua locală privată și prin rețeaua publică (servere cloud). În aceste condiții, devine posibil accesul persoanelor neautorizate la rețeaua feroviară. Având în vedere acest aspect, lucrarea pune accentul pe managementul distribuitorilor de energie feroviară și metodele lor de securitate date. Pentru fiecare echipament este identificat nivelul său de accesibilitate rezultat din gradul de vulnerabilitate. Având în vedere acest aspect, trebuie luate măsuri de securitate a datelor pentru a preveni potențialele consecințe negative asupra sistemului informatic. Atacurile cibernetice asupra rețelei de calculatoare din cadrul dispeceratelor feroviare pot avea loc intern (SCADA) și extern (protocoale și transmisii de date). Securitatea informațiilor, în contextul managementului traficului de date în timp real din cadrul dispeceratului energetic feroviar, conduce la creșterea nivelului de protecție al infrastructurilor critice naționale și europene.*

Cuvinte cheie: instalații fixe de alimentare, SCADA, cloud, transmisii de date

Abstract.– *This paper presents a viable solution for data security within the fixed power installations of the railway electric traction system. Transmission of process information to control, surveillance and data acquisition structures (SCADA) is done through the private local network and the public network (cloud servers). Under these conditions, unauthorized persons access to the railway network becomes possible. With this in mind, the paper focuses on the management of railway power distributors and their security methods. For each equipment, its level of accessibility resulting from the degree of vulnerability is identified. Therefore, data security measures must be taken to prevent potential negative consequences for the computer system. Cyber attacks on the computer network within the railway dispatchers can take place internally (SCADA) and externally (protocols and data transmissions). Information security, in the context of real-time data traffic management within the rail energy dispatcher, leads to an increase in the level of protection of national and European critical infrastructures.*

Key words: fixed power plants, SCADA, cloud, data transmissions

1. Introducere

Pentru a câștiga în cursa transformării digitale, personalul calificat și autorizat din cadrul dispeceratelor energetice feroviare va trebui să aplice noi norme de securitate şi să monitorizeze constant drepturile de acces ale utilizatorilor. În acest sens pot fi depistate posibile nereguli la nivelul sistemului de teleconducere.

Un obiectiv important pe linia asigurării interoperabilităţii infrastructurii căii ferate române cu infrastructura feroviară europeană îl constituie retehnologizarea instalaţiilor fixe de alimentare a liniei de contact. Soluţiile de modernizare din posturile centrale dispecer, substaţiile de tracţiune şi posturile căii, prevăd utilizarea automatelor programabile [1, 2], a sistemelor de tip Supervisory Control and Data Acquisition (SCADA) şi a calculatoarelor de proces. Volumul informaţiilor schimbate cu punctele controlate va permite exploatarea fără personal permanent a instalaţiilor fixe de tracţiune electrică. Astfel, vor fi preluate informaţiile referitoare la: telemăsurarea tensiunilor şi curenţilor din substaţiile de tracţiune şi din posturile de secţionare, precum şi telecontorizarea energiei electrice absorbite de la furnizor. Pentru situaţia în care funcţionează sistemul de protecţie dintr-o substaţie de tracţiune, echipamentul de telecontrol va permite în timp real reconfigurarea alimentării instalaţiilor fixe de tracţiune.

Sistemele SCADA asistă dispecerii în conducerea procesului de alimentare cu energie electrică a sistemului de tracțiune electrică feroviară, permit înregistrarea manevrelor, a convorbirilor operative şi a incidentelor survenite. În acest fel, bazele de date create vor putea fi accesate de la nivelurile superioare de conducere (Centrul de Electrificare, Divizia Electrificare şi respectiv Serviciul de Exploatare de la nivelul Electrificare CFR SA). Deşi căile de comunicaţie utilizate pentru transmisia informaţiilor fac parte dintr-o structură privată, în cadrul arhitecturii SCADA există calculatoare conectate într-o reţea locală publică care pot reprezenta o poartă de acces pentru personalul neautorizat.

2. Securitatea calculatoarelor de proces

Principalele metode de combatere ale vulnerabilităţii calculatoarelor de proces sunt următoarele:

- managementul complex al “patch-urilor” implică un plan al securității datelor pentru toate tipurile de sisteme de operare prezente în centrele de electrificare;
- accesul personalului la datele companiei necesită parole sigure la nivel de utilizator;
- sisteme de prevenire a intruziunii (Intrusion Prevention Systems) care controlează accesul la rețeaua IT și protejează de abuzuri și atacuri cibernetice. Aceste sisteme sunt concepute pentru a monitoriza datele de intrare și pentru a lua măsurile necesare pentru a preveni dezvoltarea unui atac cibernetic. Conform unui recent studiu, o treime din atacuri vor fi la nivelul resurselor IT [3];

- adoptarea tehnologiilor de autotestare a securității aplicațiilor, autodiagnosticare şi autoprotecție (RASP) care se realizează prin evaluarea şi remedierea vulnerabilităţiilor interne ale reţelei şi prin scanarea sistemului de operare, a serverelor de reţea, a staţiilor de lucru cât şi a imprimantelor pentru a descoperi ariile unde există o lipsă a protecţiei informatice [4];
- protecţia centralizată a desktop-urilor din rețea se efectuează printr-un software local sau bazat pe cloud. Cloud Access Security Broker (CASB) poate fi o soluție pentru monitorizarea activității din cadrul dispeceratelor energetice feroviare. Schimbul de date din cadrul sistemului de teleconducere va putea fi salvat pe un cloud, iar la nivelul acestuia să existe firewall de rețea, portal web securizat (SWG) și platforme firewall pentru aplicații web (WAF) [5];
- managementul regulilor de securitate în reţea asigură alinierea tuturor userilor la aceleaşi reguli de accesare rețea. Aceste reguli includ schimbarea regulată a parolelor, limitarea accesului/controlului pe staţiile de lucru a administratorului reţelei (introducerea tehnologiilor de recunoaștere utilizator) şi asigurarea că update-urile şi patch-urile sunt instalate la timp şi pe toate staţiile de lucru;
- adoptarea unei soluţii de management de tip IdaaS asociat cu Okta's Universal Directory bazat pe cloud care să se asigure că numai acei utilizatori care au permisiunile de securitate corecte pot accesa date restricționate. Acest tip de management are avantajul de a controla traficul de date senzitive (peer to peer) [6].

3. Stabilirea gradului de vulnerabilitate a echipamentelor și a sistemului informatic din instalaţiile fixe de alimentare ale tracțiunii feroviare

Sistemul informatic din instalaţiile fixe de alimentare ale tracțiunii feroviare prezintă un grad ridicat de accesibilitate asupra informaţiilor. Acest sistem trebuie controlat şi securizat împotriva atacurilor cibernetice de orice tip, deoarece orice intruziune poate avea efecte nedorite. Astfel trebuiesc identificate echipamentele cu grad ridicat de vulnerabilitate din cadrul sistemului informatic, vulnerabilităţile sistemului de protecţie al aplicaţiilor SCADA şi riscurile apariţiei evenimentelor în cadrul reţelei feroviare.

Stabilirea gradului de vulnerabilitate al unui echipament utilizat în cadrul instalaţiilor fixe de tracţiune feroviară va fi determinat pe baza nivelul de accesibilitate şi control de la distanţă. Pentru aceasta este implementat un model topologic de reţea, sub forma unui graf orientat, în cadrul căruia fiecărui element (dispozitiv electronic, automat programabil, releu de protecţie) i se atribuie un anumit grad de vulnerabilitate.

Echipamentele primare controlate de la distanţă din cadrul sistemului de teleconducere pot reprezenta ţinte vulnerabile în cadrul unui atac informatic. În acest sens se va urmări evidenţierea echipamentelor cu grad ridicat de vizibilitate din partea "hacker"-ului, cât şi legătura către echipamentul primar care poate fi activată de către acesta şi gradul de vulnerabilitate.

În categoria echipamentelor controlate de la distanţă sunt incluse dispozitivele de acţionare ale aparatajului primar, releele numerice de protecţie, automatele programabile, echipamentele electronice inteligente şi calculatoarele de proces din substaţii.

Prezența mai multor tipuri de protocoale la nivelul circuitelor secundare ale echipamentelor inteligente distribuite conduce la creşterea gradului de dificultate privind implementarea unui sistem de protecţie împotriva atacurilor cibernetice.

Fiecare canal de comunicaţie existent în cadrul sistemului permite echipamentelor comunicaţia între acestea în diverse moduri utilizând porturi şi protocoale specifice. În acelaşi timp aceste canale de comunicaţie logice sporesc gradul de vizibilitate al echipamentelor către “hacker”.

În figura 1 este prezentată schema bloc de principiu a unui sistem de teleconducere, prezentându-se și căile de acces de la distanţă:

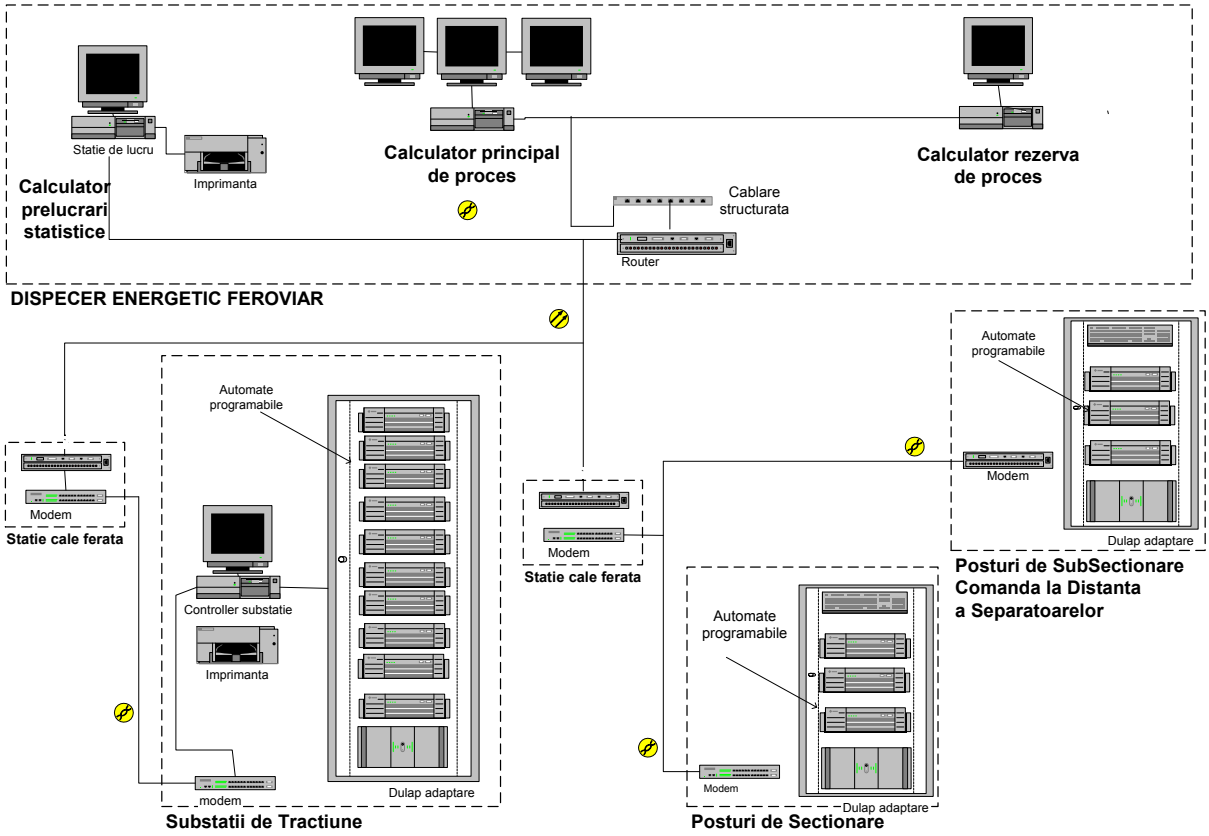

Fig. 1. Schema sistemului de teleconducere

Achiziția de date reprezintă procesul de preluare și măsurare a informațiilor din sistem (substațiile de tracțiune, posturile de secționare, posturile de subsecționare, comanda la distanță a separatoarelor din stațiile de cale ferată). Aceste informaţii pot deveni variabile țintă. Captarea informațiilor de calitate, transformarea lor în analize bogate oferă dispecerului energetic feroviar seturi de date eficiente și credibile.

În figura 2 sunt prezentate rețelele de comunicație prezente în cadrul sistemului de teleconducere.

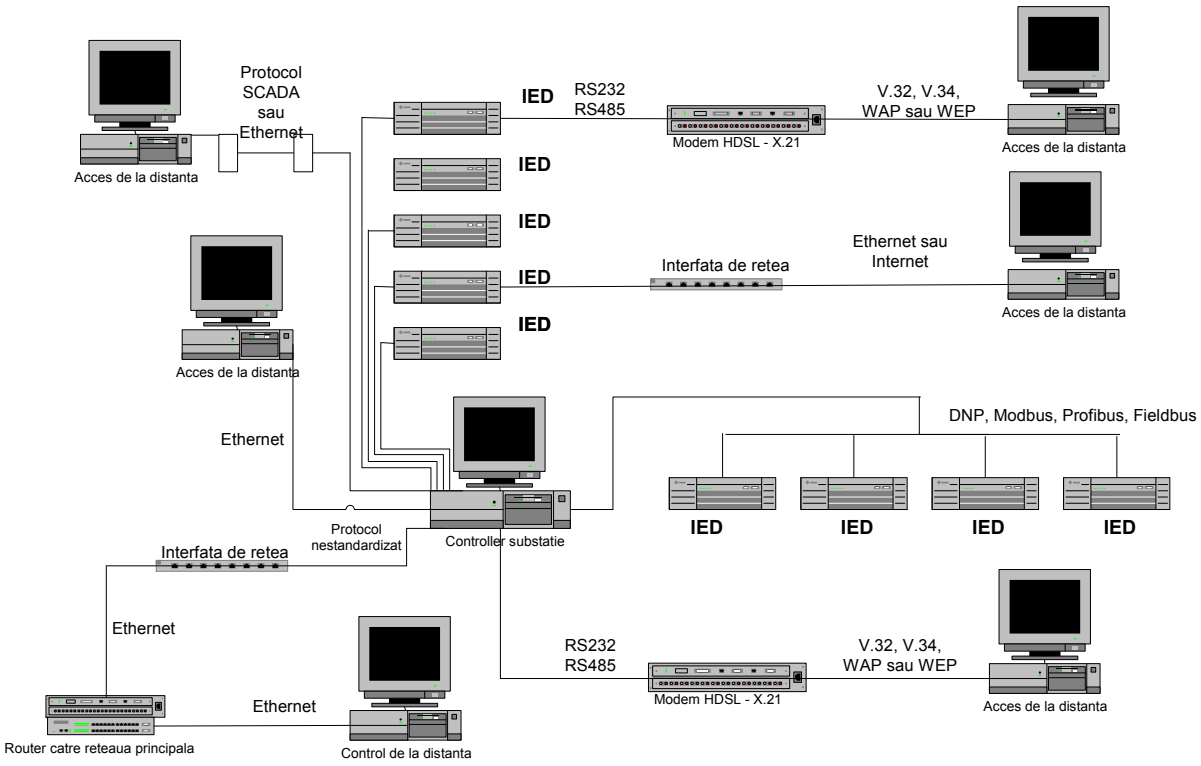

Fig. 2. Schema bloc a rețelelor de comunicații din cadrul sistemului de teleconducere

Procesul de achiziție a datelor necesită o infrastructură IT convergentă pentru fiecare instalație (software, rețea, server și stocare) prin care:

- se vor colecta și stoca datele primite de senzori, de automatele programabile, de dispozitivele electronice inteligente (IED) și de alte surse externe;
- se vor efectua analize în timp real asupra stării sistemului;
- se vor partaja prin diversele metode de conectivitate toate datele obținute de la proces. Aceste date sunt procesate (extragere, transformare, validare) și apoi salvate la nivelul controller-ului din substația de tracțiune.

Pentru o achiziție în timp real a datelor, echipamentele trebuie să poată fi interfațate între ele astfel încât toate informațiile primite din teren de la substațiile de tracțiune să ajungă la calculatorul de proces din dispeceratul energetic feroviar (figura 1).

Prin utilizarea de către dispeceri a unei interfețe grafice cât mai intuitive pot fi prelucrate datele obținute din mai multe surse și transformate în informații care să permită experților din domeniu o analiză detaliată asupra sistemului de alimentare cu energie electrică a căii ferate. Utilizând un instrument bun de integrare a datelor, această mapare este reprezentată vizual pe un monitor în dispeceratele electrice feroviare, în așa fel încât, să fie ușor de urmărit calea datelor (de unde vin, modul în care sunt procesate sau transformate pe măsură ce trec prin sistem și unde merg).

Procesul de transformare și integrare a datelor oferă date într-un format standardizat. Astfel, prin algoritmi potriviți se codifică informațiile obținute din datele

inițiale. Procesul abordează problema datelor primite și stocate din mai multe locuri și în mai multe formate.

Prin *evaluarea datelor,* experții analizează datele și caută modele care prezic defecțiuni potențiale cu ajutorul unor algoritmi avansați verificați prin expertize în domeniu. Faza de evaluare a datelor se ocupă atât de analiza pe termen scurt, cât și pe termen lung. Analiza pe termen scurt este realizată în timp real, în timp ce analiza pe termen lung oferă o viziune totală asupra sistemului de întreținere a securității datelor.

Sistemele SCADA utilizează rețele de comunicaţii proprii, însă ele efectuează și schimburi de informaţii cu calculatoarele din sistem ceea ce poate conduce la vulnerabilitatea datelor din cadrul rețelelor. Sistemele de securitate vor utiliza: nume utilizator, parolă, noi tehnologii de recunoaștere utilizator, limitare timp acces și protocoale de criptare.

Securitatea rețelelor a fost controlată în ultimii ani cu adoptarea rețelelor de control de supraveghere și de achiziție a datelor (SCADA) care au creat oportunități dar și provocări personalului din cadrul dispeceratelor energetice feroviare. Printre cele mai des întâlnite amenințări se numără:

- persoane sau grupuri rău intenționate care doresc să obțină acces la o rețea SCADA și să o controleze din interior;
- programe malware utilizate pentru perturbarea rețelelor și proceselor (virușii de calculator, programele spyware);
- atacuri teroriste pentru a obține acces la o rețea SCADA;
- eroarea interioară bazată pe soluţii greşite (software sau hardware) alese de dispecerul energetic feroviar.

Punctele slabe și vulnerabilitățile SCADA constau în:

- angajații nu sunt instruiți în monitorizarea, identificarea și prevenirea potențialelor amenințări la adresa securității sistemului;
- atacuri care pot apare la actualizarea sau modificarea unui sistem SCADA. Această vulnerabilitate poate fi eliminată prin introducerea soluțiilor Cloud Access Security Broker;
- sistemele de teleconducere complexe sunt controlate cu aplicații standard de rețea;
- monitorizarea în timp real a informaţiilor. Pentru o bună protecţie a datelor ar trebui utilizate Firewall-urile Enterprise și un sistem de detectare a intruziunilor;
- lipsa de întreținere a rețelei. Aceasta vulnerabilitate poate fi soluționată prin actualizări periodice hardware, corecții software și administrare corespunzătoare a rețelei.

Rețelele în sine se schimbă, apare comunicația la nivel de cloud și astfel arhitectura de rețea online este tot mai deschisă amenințărilor de securitate și vulnerabilităților.

Profilul de protecţie al unui sistem de teleconducere industrial este prezentat în figura 3.

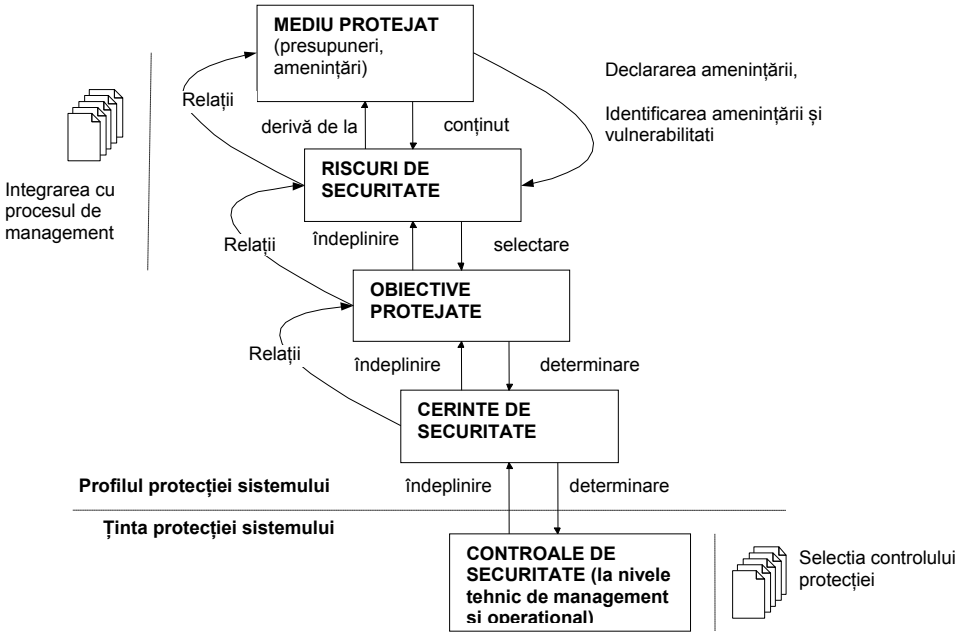

Fig. 3. Profilul protecţiei sistemului de teleconducere

Mediul protejat este descris prin agenţii de ameninţare care conduc un atac asupra bunurilor. Fiecare agent este particularizat prin resursele disponibile necesare înscenării atacului şi motivaţiile acestuia. Atacul este descris prin metoda utilizată, vulnerabilităţile exploatate pentru accesul la echipamentul protejat şi prin oportunitatea existenţei unei breşe prin intermediul căreia să se producă atacul.

Riscurile de securitate sunt date de totalitatea riscurilor din sistemul informaţional. Fiecare risc este dat de valoarea echipamentului, de nivelul de pericol asociat, de vulnerabilităţile asociate. Riscul reprezintă potenţialul ca un pericol dat să exploateze vulnerabilităţile cauzate de pierderile şi defectele la un echipament sau grup de echipamente.

Obiectivele protejate se referă la identificarea echipamentelor care compun sistemul de control informaţional.

Cerinţele de securitate determină selecţia controalelor de securitate necesare pentru a asigura protecţia echipamentelor sistemului ţintă.

Profilul protecţiei sistemului de teleconducere industrială trebuie realizat în conformitate cu standardele specifice transmisiilor de date din substaţiile feroviare ISO/IEC 15408-1:2009[7], IEC 60850:2014 [8], IEC60870:2018 [9],[10].

Controalele de securitate sunt prezentate la nivel de management operaţional şi tehnic [11] şi constau în măsurile de reacţie dintr-un sistem informaţional [12]. Acestea păstrează confidenţialitatea, integritatea şi accesibilitatea unui sistem şi a informaţiilor din cadrul acestuia.

4. Concluzii

Metodologia elaborării unei astfel de lucrări a constat în: identificarea echipamentelor cu grad ridicat de vulnerabilitate din instalaţiile fixe de tracţiune electrică, identificarea reţelelor de comunicaţii, identificarea şi clasificarea atacurilor informatice, identificarea utilizatorului prin parole, noi tehnologii de recunoaştere a utilizatorului, limitarea timpului de acces, cuantificarea riscurilor apariţiei evenimentelor în cadrul reţelei feroviare, realizarea unui model pentru sistemul informatic, securitatea prin utilizarea protocoalelor de criptare pentru modem, securitatea reţelelor de comunicaţie, implementarea unui sistem de protecţie al unui sistem de teleconducere industrial.

Ultimul deceniu a evidențiat o creștere a numărului dar și a nivelului de complexitate al atacurilor cibernetice îndreptate împotriva infrastructurilor critice industriale, în funcție de țara și de producătorul sistemului industrial. S-au semnalat cazuri deosebit de grave de perturbări ale proceselor critice și chiar distrugerea sistemelor de teleconducere industriale. Creșterea securității datelor în sistemele de control industrial reprezintă o nevoie imperioasă pentru tot mai multe organizații la nivel mondial. Pe de altă parte, administratorii de rețea evită protejarea on line a sistemelor de tracțiune electrică feroviară prin introducerea unor sisteme de tip IPS datorită posibilității de degradare accidentală sau de blocare a sistemelor. Totodată, soluțiile menționate pot afecta performanța acestor sisteme. De aceea, este necesară o nouă abordare a securității datelor în sistemele de control industrial care să respecte cu strictețe standardele actuale de protecție. Această nouă implementare trebuie să reunească tehnologiile de bază într-un mod în care să prevină chiar și atacuri cibernetice avansate. Integrarea acestei noi soluții de securitate a datelor cu sistemele de teleconducere existente trebuie să permită existența unei interfețe care să efectueze acțiuni de securitate date în mod automat.

Această lucrare prezintă o imagine de ansamblu asupra capabilităților de bază care ar trebui să definească sistemul de securitate date pentru instalațiile fixe de alimentare ale sistemului de tracțiune electrică feroviară.

Referinţe

[1] C. G. Sărăcin, M. Sărăcin, V.V. Golea, „Sisteme de telemăsurare”, Editura Matrix ROM, 2004.
[2] C. G. Sărăcin, „Instalaţii electrice”, Editura Matrix ROM, 2009.
[3] https://www.gartner.com/smarterwithgartner/top-10-security-predictions-2016/
[4] https://www.immun.io/blog/how-rasp-works-in-a-devops-environment
[5] https://www.netskope.com/company/about-casb
[6] https://www.okta.com/identity-101/idaas/
[7] https://www.iso.org/obp/ui/#iso:std:iso-iec:15408:-1:ed-3:v2:en
[8] https://webstore.iec.ch/publication/3685,
[9] https://webstore.iec.ch/publication/3755
[10] https://download.beckhoff.com/download/document/automation/twincat3/TF6500_TC3_IEC60870-5-10x_EN.pdf
[11] https://www.iso.org/obp/ui/#iso:std:iso-iec:15408:-1:ed-3:v2:en
[12] https://www.hitachivantara.com/en-us/pdfd/white-paper/use-iot-to-advance-railway-predictive-maintenance-whitepaper.pdf