Sistem de Securitate pentru Zonele de Acces din Instalațiile Electrice de Distribuție

Security System for Access Areas in Electrical Distribution Installations

Cristina Gabriela Sărăcin[1], Cornel-Ovidiu Ivan[1]

[1]Universitatea Polithnica din București
Splaiul Independenței Nr.313
E-mail: cristina.saracin@upb.ro, icornel14@yahoo.com

Rezumat.– *Această lucrare prezintă o soluție viabilă pentru asigurarea securității instalațiilor fixe de alimentare ale sistemului de distribuție electrică. Transmisia energiei electrice către consumatori casnici sau industriali se face prin rețele locale private și prin rețeaua publică. În aceste condiții, devine posibil accesul persoanelor neautorizate la instalațiile electrice de distribuție. Având în vedere acest aspect, lucrarea pune accentul pe securitatea distribuitorilor de energie electrică și metodele lor de securizare a zonelor de acces în instalațiile de distribuție a energiei electrice. Pentru fiecare zonă din cadrul unei instalații de distribuție electrică este identificat nivelul ei de accesibilitate rezultat din gradul de vulnerabilitate. Având în vedere acest aspect, trebuie luate măsuri de securizare a stațiilor de distribuție pentru a preveni potențialele consecințe negative asupra sistemului de distribuție a energiei electrice. Securitatea instalațiilor de distribuție electrică în contextul managementului de energie electrică în timp real din cadrul unui dispecerat energetic, conduce la creșterea nivelului de protecție al infrastructurilor critice naționale și europene.*

Cuvinte cheie: instalații electrice de distribuție, securitate zone de acces

Abstract.– *This paper presents a viable solution for ensuring the security of the fixed power supply installations of the electrical distribution system. The transmission of electricity to domestic or industrial consumers is done through local private networks and through the public network. Under these conditions, it becomes possible for unauthorized persons to access the electrical distribution installations. Given this aspect, the paper focuses on the security of electricity distributors and their methods of securing access areas in electricity distribution facilities. For each area within an electrical distribution installation, its level of accessibility resulting from the degree of vulnerability is identified. In view of this, measures must be taken to secure the distribution stations in order to prevent potential negative consequences for the electricity distribution system. The security of electricity distribution installations in the context of real-time electricity management within an energy dispatcher, leads to increasing the level of protection of national and European critical infrastructures.*

Key words: electrical distribution installations, security access areas

1. Introducere

Riscul raţional sau acceptat reprezintă modalitatea de acţiune bazată pe perceperea în cunoştinţă de cauză a gradului de ameninţare şi de vulnerabilitate. Riscul se minimizează în măsura în care alegerea variantei de contracarare a pericolului se optimizează. Securitatea reprezintă conceptul care poate răspunde dorinţelor de siguranţă şi stabilitate necesare bunei funcţionări a sistemelor. [3]

Sistemul de securitate constă în ansamblul de echipamente, dispozitive şi subsisteme specifice care asigură protecţia instalaţiilor electrice de distribuţie. Subsistemele specifice, interconectate constructiv şi procesual, îndeplinesc următoarele funcţii: protecţie perimetrală, control acces, detecţie şi avertizare la efracţie, supraveghere prin CCTV, detecţie şi semnalizare/stingere la incendii, inundaţii şi alte pericole, comunicaţii de securitate, monitorizare, comandă şi control. [4]

Din ameninţările uzuale, putem evidenţia următoarele: factorul uman, echipamentele electrice, reţeaua de transmisie a informaţie.

Vulnerabilităţile pot fi datorate următoarelor [5]:

- protecţie fizică slabă a obiectivelor;
- sisteme tehnice neperformante (surse de alimentare, unităţi de procesare, servere de baze de date , software necontrolat , etc);
- protecţie informaţională inadecvată.

2. Sistemul de control acces al staţiei de distribuţie

Sistemul de control acces monitorizează intrarea în staţiile de distribuţie. Scopul acestuia este de a oferi acces rapid persoanelor autorizate, restricţionând accesul persoanelor neautorizate. Prima variantă studiată o reprezintă sistemul realizat cu controlere principale şi secundare (figura 1).

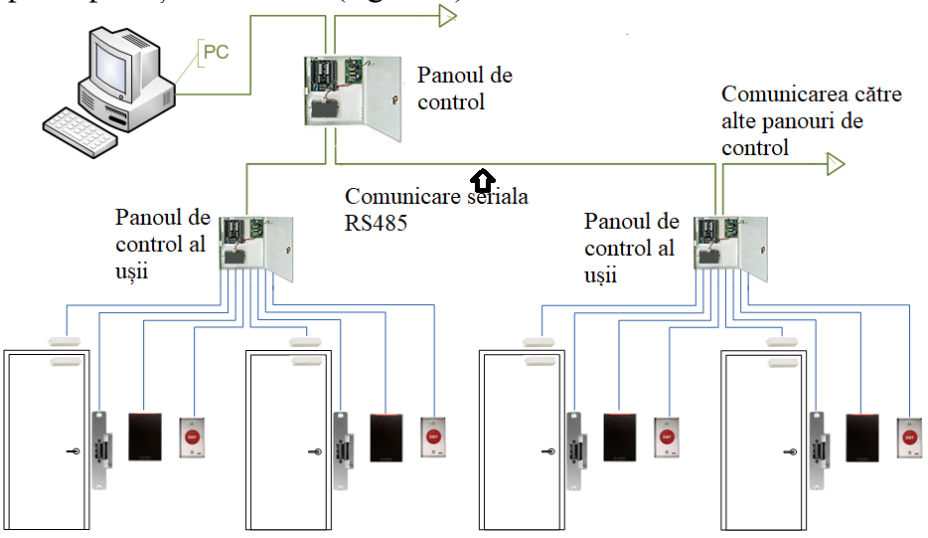

Fig. 1. Schema de conectare a controlerelor principale şi secundare

Toate echipamentele pentru uși sunt conectate la controlere secundare (de ușă sau interfețe pentru uși). Controlerele secundare, de obicei, nu iau decizii privind accesul și înaintează toate cererile controlorilor principali. Pentru control acces se utilizează cititorul de identitate. Rolul acestuia este de a căuta într-o bază de date un anumit indicativ. În cazul identificării se acționează electric yala și se permite accesul în cameră.

A doua variantă studiată este compusă din controlere principale seriale și cititoare inteligente (figura 2). Toate echipamentele pentru uși sunt conectate direct la cititoare inteligente sau semi-inteligente. Cititorii de obicei nu iau decizii de acces și înaintează toate cererile către controlorul principal. Doar dacă conexiunea cu controlerul principal nu este disponibilă, cititorii vor utiliza baza lor de date internă pentru a lua decizii de acces și a înregistra evenimente. Cititorul semi-inteligent, care nu are o bază de date și nu poate funcționa fără controlerul principal poate fi utilizat în zone care nu necesită securitate înaltă. Criteriile de risc sunt stabilite în funcție de destinația încăperilor aferente stației de distribuție.

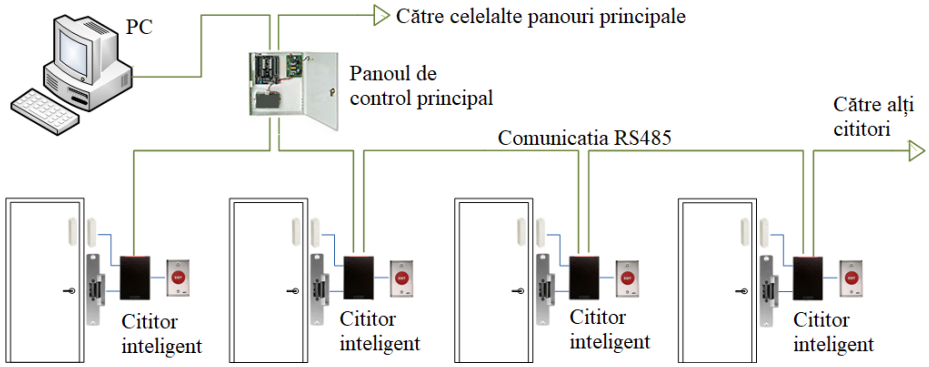

Fig. 2. Schema de conectare a controlerelor principale cu cititori inteligenți

A treia variantă studiată este compusă din controlere seriale cu servere terminale (figura 3).

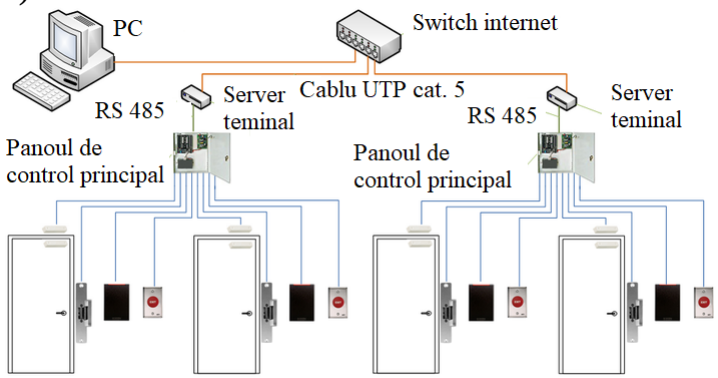

Fig. 3. Schema controlerelor seriale cu servere terminale si panouri ce conțin adrese IP

Avantajele acestui sistem de control acces sunt următoarele:

- utilizează infrastructura de rețea existentă;

- utilizează un număr nelimitat de controlori;
- comunicarea cu controlerele se realizează la viteza rețelei;
- în cazul unei alarme, controlerele pot iniția conexiunea cu PC-ul gazdă.

Orice sistem de control acces prezintă și dezavantaje. Acestea constau în:

- întârzieri în caz de defecțiuni de trafic intens și de echipamente de rețea;
- accesul hackerilor la rețeaua stațiilor electrice;
- distanța maximă de la hub la controler de peste100 de metri.

3. Proiectarea sistemului de control acces

Proiectarea sistemului de control acces implică definirea zonelor pentru care se realizează acest sistem. Arhitectura sistemul (figura 4) a fost creată în programul AUTOCAD 2D.

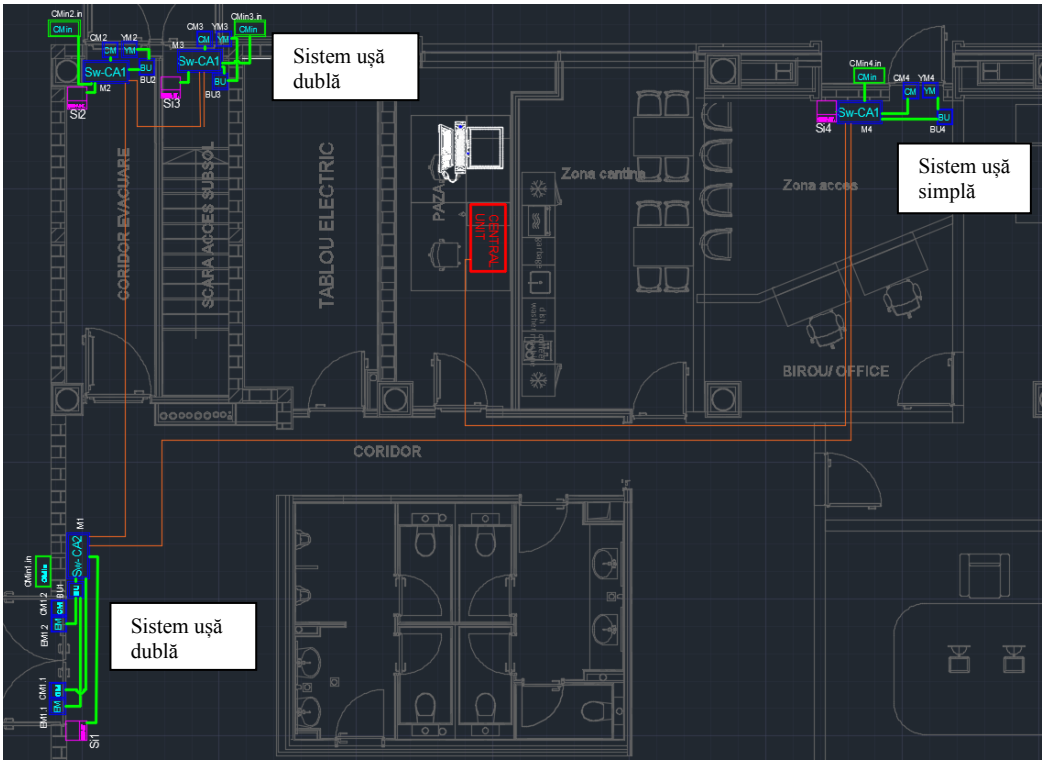

Fig. 4. Integrarea sistemului de control acces

Stația electrică conține o zonă de comandă unde se supraveghează buna desfășurare a procesului de distribuție a energiei electrice. Totodată se mai regăsesc camere tehnice, zone de birou și zone de depozitare. Există trei uși de acces către exterior pentru care se realizează sistemul de control acces.

Filtrele de control acces sunt de tip unidirecțional cu cititoare de carduri prevăzute la intrarea în spațiu, ieșirea realizându-se apăsând butonul de ieșire ce se regăsește pe interiorul fiecărei uși. Ușile vor fi prevăzute și cu o sirenă cuplată la sistemul de control acces pentru a avertiza persoanele din zona atunci când ușa se deschide. Sistemul va fi configurat astfel încât orice utilizare a ușilor să fie

semnalizată. Uşile de evacuare sunt prevăzute cu Panic-bar şi vor fi echipate cu yală electromagnetică astfel încât acționarea Panic-bar-ului să întrerupă alimentarea cu energie electrică a yalei electromagnetice.

Modulele de control acces pentru una sau două uşi, vor fi prevăzute cu sursă şi acumulator de 5Ah inclus şi comunicație RS485 cu centrala de control acces. În cazul apariției unui incendiu în această zonă, sistemul de control acces va primi o comandă de la sistemul de detecție incendiu prin care, uşile vor fi deblocate, permițând astfel evacuarea persoanelor în cel mai scurt timp. Această comandă va fi transmisă către sistemul de control acces printr-un releu cu o ieşire integrată în sistemul de detecție incendiu.

4. Sistem de securitate antiefracție şi protecție perimetrală

Elementele constitutive ale sistemului de securitate sunt următoarele: senzorii de efracție, centrala, echipamentele periferice ale centralei, dispozitivele de avertizare locală şi dispozitivele de comunicare la distanță.

Senzorii preiau o informație de tip stare de alarmă. Centrala procesează informațiile preluate de la senzori în funcție de starea sistemului (activat, dezactivat). Echipamentele periferice ale centralei sunt modulele de expandare şi interfețele de comandă. Modulele de expandare au rolul de a extinde numărul de intrări şi/sau de ieşiri ale centralei pentru configurarea unor sisteme de capacitate sporită. Interfețele de comandă au rolul de a permite utilizatorilor să comande diferite funcțiuni ale sistemului. Aceste interfețe pot fi contacte cu o cheie specială de securitate, tastaturi sau cititoare de tag-uri de acces, cititoare biometrie, etc.

Dispozitivele de avertizare locală pot fi optice, acustice sau opto-acustice (mixte). Rolul acestor dispozitive este de a semnaliza o stare de alarmă.

Dispozitivele de avertizare la distanță sunt comunicatoare care utilizează diferite canale de comunicație pentru a semnaliza o alarmă la un dispecerat de monitorizare şi intervenție.

Pentru stația electrică există următoarele zone:

- instantanee – declanşează instantaneu o alarmă;
- temporizată –activarea generează o temporizare internă a sistemului (zonele de intrare/ieşire respectiv, urmărire);
- de panică-atac la persoană– declanşează o alarmă silențioasă;
- de sabotaj/defecțiune tehnică – sunt zone de 24 de ore utilizate pentru monitorizarea securității sistemului (contactele anti sabotaj ale dispozitivelor).

Realizarea unui sistem de securitate la efracție şi control acces este un proces structurat pe mai multe etape şi-anume [11,12]:

a) Evaluarea nevoilor obiectivului implică necesitatea de supraveghere (totală sau parțială);

b) Planificarea şi proiectarea se realizează prin: selectarea tipurilor de detectoare şi poziționarea acestora; partiționarea sistemului de securitate; asigurarea

mijloacelor pentru controlul sistemului și pentru afișarea indicațiilor sale; asigurarea surselor de alimentare; realizarea circuitelor.

În ceea ce privește unitățile centrale, cele de multiplexare, interfețele de acces și interfețele om–mașină, criteriile sunt următoarele:

a. pentru centrale, multiplexoare și interfețe de acces, acestea vor fi amplasate în spații protejate și accesibile numai personalului tehnic de întreținere. Dacă există camere tehnice dedicate amplasarea elementelor de structură a sistemului antiefracție va fi făcută în cadrul acestora în măsura în care distanțele maxime specificate pentru dispozitive față de unitățile de multiplexare nu sunt depășite.

b. interfețe om-mașină – tastaturile de control și cititoarele de taguri de acces sau identificatoarele biometrice vor fi amplasate ergonomic și accesibil utilizatorilor. Înălțimea de montaj recomandată este de 1,40 m față de pardoseală. O atenție deosebită se va acorda poziționării cititoarelor de „taguri" RFID astfel încât acestea să nu interfereze electromagnetic, atât între ele cât și cu alte echipamente potențial generatoare de zgomot RF cum ar fi monitoarele TV.

Pentru sistemele de securitate antiefracție [3,6], afișarea mesajelor generate de sistem se face de regulă prin intermediul tastaturilor. Acestea trebuie amplasate în zone supravegheate (protejate de senzori de mișcare) pentru a preveni tentativele de accesare frauduloasă. Numărul acestor tastaturi depinde de partiționarea şi funcționarea sistemului. Unele obiective au prevăzute dispecerate locale de pază la care, chiar dacă sistemul este monitorizabil prin intermediul unui PC, este obligatorie instalarea unei tastaturi de sistem pentru asigurarea funcționării în caz de avarie electrică. În afară de tastaturi de sistem și pachete software pentru interfețele grafice pot fi utile și panouri sinoptice pentru o mai bună localizare a alarmelor.

Unul din aspectele cele mai importante în asigurarea funcționării corecte a sistemelor de securitate antiefracție şi control al accesului îl reprezintă alimentarea cu energie electrică. La stabilirea soluției de alimentare trebuie avute în vedere următoarele reguli:

a. toate sursele de alimentare se conectează pe aceeași fază printr-o siguranță dedicată în tabloul general. De preferință, în camera tehnică va fi amplasat un al doilea tablou de siguranțe dedicate diferitelor subsisteme de securitate.

b. pot fi luate în considerare diferite modalități de asigurare a backup-ului. Pentru sistemele antiefracție și control al accesului backup-ul se realizează pe partea de joasă tensiune cu acumulatoare tampon dar, pentru sisteme mari se pot lua în calcul UPS-uri pe alimentarea cu $230V_{AC}$.

c. dimensionarea raportului secțiune/lungime pentru cablurile de alimentare trebuie atent analizată pentru a păstra tensiunea de alimentare a echipamentelor în limitele impuse de producător. O atenție deosebită trebuie acordată în cazul alimentării pe sursa de back-up (acumulator) – în cazul acesteia, tensiunea furnizată scade până la 10,8V, valoare la care acumulatorul este considerat descărcat.

Amplasarea modulară a surselor de alimentare pe tronsoane (segmente) de sistem trebuie să țină cont de încărcarea maximă a fiecărei surse și de posibilitatea de a asigura încărcarea acumulatoarelor tampon. În consecință, calculul energetic va fi efectuat pe fiecare segment de sistem alimentat de o sursă. Se efectuează un calcul

energetic pentru a estima întreg consumul sistemului, după care, în funcție de necesități, acesta va fi segmentat și alimentat din mai multe surse. În cazul utilizării mai multor surse de alimentare, masa întregului sistem va fi comună. Faza va fi separată, astfel fiecare tronson de sistem va fi alimentat dintr-o sursă distinctă (este de preferat evitarea conectării în paralel a surselor chiar dacă echilibrarea tensiunilor se realizează pe rezistența cablurilor de alimentare).

Proiectarea cablajului unui sistem de securitate presupune o înțelegere complexă a fenomenelor electromagnetice cum ar fi: căderile de tensiune pe rezistența electrică a circuitului, cuplajul inductiv, apariția capacităților parazite și efectele negative ale buclelor de masă.

În proiectarea cablajelor, se va urmări respectarea următoarelor reguli:

- separarea traseelor de curenți tari și curenți slabi;
- alegerea tipurilor adecvate de cabluri pentru fiecare tip de semnal în parte: cabluri de semnalizare pentru senzori, contacte, yale electromagnetice etc., cabluri de date (cu impedanța caracteristică standard de 120 ohmi) pentru magistralele de comunicație de tip RS 485 și cabluri cu secțiune corespunzătoare pentru tipurile de magistrale care nu folosesc acest standard;
- se vor evita zonele în care există perturbații electromagnetice puternice (mediu industrial cu mașini electrice sau procese electrochimice), încăperi pentru stații de radio-emisie etc.

Situații grave pot apare datorită căderii unor componente sau întreruperii magistralelor. Se consideră ca fiind prag critic funcțional un defect în urma căruia parametrii funcționali ai sistemului scad la 70,7% din valorile nominale. Totodată există anumite funcționalități critice în utilizarea unui sistem, cum ar fi în cazul control-accesului funcționarea ușii principale de acces într-un obiectiv.

După cum am exemplificat în paragraful de mai sus, pentru zona de acces a stației de distribuție s-au stabilit zonele de risc astfel încât, amplasarea echipamentelor sistemului de efracție să fie amplasate corect. Astfel, pentru ușile ce au rol de acces dinspre exterior se folosesc contacte magnetice pentru a împiedica accesul persoanelor neautorizate. Pentru ca sistemul să fie redundant, fără să apară breșe de securitate, în fiecare zonă de acces se amplasează detectori de mișcare.

Centrala de efracție se va poziționa în zona dispeceratului de pază, pentru a putea monitoriza în timp real. În apropierea centralei de efracție se va amplasa tastatura de armare/dezarmare. Având în vedere programul de lucru al personalului stației se pot separa anumite filtre pentru a se arma la ore diferite pentru a nu primi alarmă falsă. Contactul magnetic se va amplasa pe fiecare ușa care se consideră că ar fi de risc.

4. Concluzii

În aceasta lucrare s-a ales, ca studiu de caz în proiectarea sistemelor de securitate, o stație de distribuție a energiei electrice deoarece aici se regăsesc încăperi cu destinații diferite ce necesită un grad de protecție sporit.

Funcționând în parametrii nominali, cele două sisteme de securitate prezentate, contra incendiu si antiefracție, reduc posibilitatea apariției unui eveniment neplăcut ce poate afecta negativ procesul de distribuție al energiei electrice.

Echipamentele centrale ale celor două sistemelor de securitate, centrala antiincendiu și antiefracție s-au amplasat în camera dispeceratului local, deoarece acestea sunt monitorizate în permanență de un personal calificat, iar în cazul unei alarme de foc sau efracție, acestea vor fi rezolvate în cel mai scurt timp. Având în vedere că sunt distanțe mici de la unitatea centrală până la fiecare echipament de securitate aflat în dotarea stației de distribuție electrică, nu apar probleme datorită căderilor de tensiune.

Sistemul de control acces și cel de securitate antiefracție pot dialoga cu sistemul de detecție al incendiului printr-o interfață comună. În momentul în care este confirmat un incendiu în zona stației de distribuție, centrala sistemului de detecție incendiu transmite un semnal către releul ce este conectat atât la centrala de comunicare a sistemului de efracție cât și la sistemul de control acces, iar acest impuls are rolul de a decupla toate ușile de acces pentru a permite evacuarea personalului în cel mai scurt timp.

Sistemul de control al accesului, pe lângă funcția de bază de a restricționa accesul poate fi utilizat și ca echipament de pontaj, reducând astfel costurile prin achiziționarea de echipamente auxiliare.

Referinţe

[1] C. G. Sărăcin, M. Sărăcin, V.V. Golea, „Sisteme de telemăsurare”, Editura Matrix ROM, 2004.
[2] C. G. Sărăcin, „Instalații electrice”, Editura Matrix ROM, 2009.
[3] Tiberiu Urdăreanu, Gheorghe Ilie, Mircea Blaha: Securitatea Instituţiilor Financiar Bancare, EdituraUTI , 1998
[4] MIL-HDBK-1013: Ghid de proiectare pentru securitatea fizică a obiectivelor
[5] Harold F. T., Mickey K., editors: Information Security Management Handbook
[6] Dr. Ing. Gheorghe Ilie: Securitatea mediului de afaceri, Editura UTI Press, 2006
[7] http://www.unitedtecgroup.com/access-control-systems.html
[8] https://vividcomm.com/2018/04/13/cctv-video-management-systems/
[9] Dr. Ing. Gheorghe Ilie, Ing. Adrian Roşca: Determinarea riscului de securitate; Revista ALARMA,NR. 2/2010 .
[10] Adrian Roşca: Curs pentru ingineri de sisteme de securitate; ARTS: 2009- 2010.
[11] Legea nr.333/2003 privind paza obiectivelor, bunurilor, valorilor şi protecţia persoanelor, republicată în 2014;
[12] H.G. nr.301/2012 pentru aprobarea Normelor metodologice de aplicare a prevederilor proiectului Legii, modificată şi completată de HG nr.1002/2015.
[13]https://www.designingbuildings.co.uk/wiki/Access_control_in_buildings
[14]http://www.rollsoft.ro/sisteme-control-acces-hotelier-biometric/