(19) OFICIUL DE STAT
PENTRU INVENŢII ŞI MĂRCI
Bucureşti

ROMÂNIA

(11) RO 129963 A2
(51) Int.Cl.
G06Q 40/02 (2012.01)

(12) # CERERE DE BREVET DE INVENŢIE

(21) Nr. cerere: **a 2013 00379**

(22) Data de depozit: **20.05.2013**

(41) Data publicării cererii:
30.12.2014 BOPI nr. **12/2014**

(71) Solicitant:
• **CONIC DESIGN S.R.L.**,
*INTRAREA STEGARULUI NR. 45,
SECTOR 1, BUCUREŞTI, B, RO*

(72) Inventatori:
• **GRIGORE ALEXANDRU TRAIAN**,
*INTRAREA STEGARULUI NR. 45,
SECTOR 1, BUCUREŞTI, B, RO*

(74) Mandatar:
INVENTA - AGENŢIE DE PROPRIETATE INTELECTUALĂ S.R.L.,
*BD. CORNELIU COPOSU NR.7, BL.104,
SC.2, AP.31, SECTOR 3, BUCUREŞTI*

(54) # ECHIPAMENT DE CITIRE ŞI EVALUARE A CIPURILOR CARDURILOR BANCARE INTEGRABIL ÎN SISTEMELE DE CONTROL ACCES PRIN PROTOCOL DE COMUNICARE WIEGAND

(57) **Rezumat:**

Invenţia se referă la un echipament de citire şi evaluare a cipurilor cardurilor bancare, integrabil în sistemele de control acces, utilizat în domeniul sistemelor de securitate electronică, în special în domeniul bancar, pentru controlul accesului către zone importante sau de înaltă securitate. Echipamentul conform invenţiei este format dintr-un cititor de carduri, un automat programabil, un convertor, nişte surse de alimentare dual㠠, o carcasă externă, un software şi o unitate de control acces.

Revendicări: 1
Figuri: 4

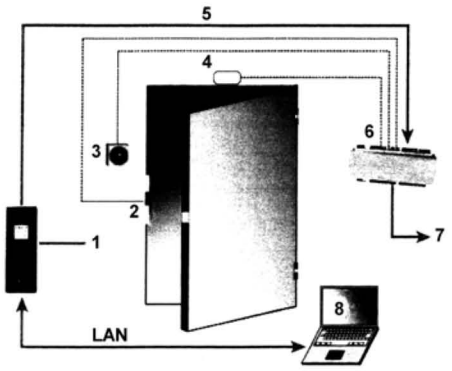


Fig. 1

RO 129963 A2

a. TITLUL INVENTIEI:

Echipament de citire si evaluare a cipurilor cardurilor bancare integrabil in sistemele de control acces prin protocol de comunicatie wiegand

b. DOMENIUL TEHNIC LA CARE SE REFERA INVENTIA:

Inventia se refera la domeniul sistemelor de securitate electronica, in special la sistemele de control al accesului. Este destinata in principal domeniului bancar pentru controlul accesului catre zone importante sau de inalta securitate.

c. STADIUL TEHNICII:

Sistemele de control acces realizeaza accesul selectiv catre un anumit spatiu sau resursa. Selectia se face pe baza elementelor de autentificare prezentate, actiunea de „acces" insemnand intrare, consum sau permisiune de utilizare. Permisiunea de accesare a unei resurse poarta denumirea de „autorizare".
Sistemele traditionale de control acces sunt compuse din urmatoarele elemente de baza:
-elemente de autentificare: parole, cartele, carduri, elemente biometrice sau combinatii de doua sau mai multe astfel de elemente
-elemente de citire: tastaturi, cititoare de proximitate sau de contact (banda magnetica sau cip electronic), sau combinatii de tastaturi si cititoare
-unitatea de evaluare: unitate dedicata de analiza, calculator cu baza de date sau ansamblu format din ambele elemente
-element de restrictionare a accesului: incuietoare mecanica, incuietoare electrica, element de acces rotativ de tip turnichet

Pe carduri sunt stocate elemente care identifica respectivele persoane in sistem . Toate deciziile se iau apoi pornind de la acele elemente de autentificare(numere, coduri, serii, etc), in cele mai multe cazurii asociindu-se un anumit cod unei anume persoane.

In cazul citirii cartelei de catre cititor, acesta transmite informatia asociata utilizatorului cartelei catre unitatea de evaluare care compara informatia citita cu lista de acces, ia decizia de autorizare sau refuzare a accesului si transmite rezultatul deciziei catre istoricul de evenimente intern care va putea fi consultat de catre administratorul sistemului. In cazul in care informatia citita de pe card este regasita in baza de date de acces, unitatea de evaluare actioneaza automat un releu care actioneaza mecanismul electric de deschidere a usii, in caz contrar, acest releu nefiind actionat. Cele mai multe cititoare de acces furnizeaza o informatie primara privind autorizarea accesului, precum afisarea unui LED verde in cazul primirii autorizarii si a unui LED rosu in cazul refuzului autorizarii.

Solutiile actuale de control acces bazate pe citirea cardurilor bancare sunt urmatoarele:
-cititoare ale benzilor magnetice ale cardurilor care evalueaza informatiile continute de suportul magnetic si ofera acces in functie de aceasta
-cititoare care recunosc cipurile oricaror tipuri de carduri cu cip(smart card) si ofera acces in functie de prezenta sau absenta acestui cip.

Exemplul cel mai apropiat de produsul inventat: ansamblu de acces cu cititor de banda magnetica si recunoasterea prezentei cipului smart cardului: http://www.keba.com/en/banking-and-service-automation/kebin-access-control/system-solutions/kebin-s6/downloads/

d. PROBLEMA TEHNICA PE CARE URMARIM SA O REZOLVAM CU AJUTORUL INVENTIEI

-autorizarea pe baza informatiilor continute in cipurile cardurilor bancare de tip smart card (nu prin recunoasterea cipurilor)

-posibilitatea selectarii tipurilor de carduri care pot avea acces, in functie de emitentii cardurilor(Ex: Visa, Mastercard, American Express, etc.).

-interactiunea cu utilizatorii/posesorii cardurilor bancare prin mesaje de tip text si pictograme afisate in oricare limba cunoscuta in acest moment in lume

-utilizarea istoricului de evenimente intern de mare capacitate, si inregistrarea amprentelor de timp pentru toate evenimentele aparute in sistem

-integrarea cu orice tip de unitate de evaluare de control acces care utilizeaza protocoale de comunicatie cunoscute: Wiegand(cel mai utilizat), RS485, clock data, Ethernet.

e. EXPUNEREA INVENTIEI:

Echipamentul de citire si evaluare a cipurilor cardurilor bancare integrabil in sistemele de control acces prin protocol de comunicatie wiegand, conform inventiei, pentru controlul accesului catre zone importante sau de inalta securitate, este format dintr-un
-cititor de carduri de tip smart card MAGTEK, cod I65 **(A)**
- un automat programabil , cod XV-102 **(B)**
- un convertor RS232->Wiegand GIGA TMS, cod CON100iB. **(C)**
-surse de alimentare duala(12/24V) CONSONS, cod PAT150 **(E)**
-o carcasa externa , cod SACD 100
-un software CONIC DESIGN si
-o unitate de control acces- **(D)**

f. AVANTAJELE INVENTIEI IN RAPORT CU STADIUL TEHNICII:

Autorizarea pe baza informatiilor continute in cipurile cardurilor bancare de tip smart card (nu prin recunoasterea lor), are avantajul major de a permite citirea cipurilor cardurilor cu dispozitive care respecta standardul EMV de utilizare a cipurilor. Modalitatea de citire a cipurilor cardurilor bancare

este o alternativa mult mai sigura impotriva citirii neautorizate si a clonarii cardurilor comparativ cu modalitatea citirii benzii magnetice a cardurilor. Standardul EMV reglementeaza utilizarea globala a cardurilor bancare echipate cu cip, detalii se gasesesc pe site-ul oficial: www.emvco.com
Posibilitatea selectarii tipurilor de carduri care pot avea acces, in functie de emitentii cardurilor(Ex: Visa, Mastercard, American Express, etc.) reprezinta un avantaj major din punct de vedere al flexibilitatii utilizarii produsului, actualizarea codurilor AID specifice fiecarui emitent de carduri facandu-se prin conexiune Internet, in timpul functionarii.
Selectia accesului se face dupa unul sau mai multe criterii in functie de aplicatie :

- numele si prenumele tiparite pe cardul bancar;
- numarul cardului bancar;
- tipul cardului bancar (ex. Visa, Visa Electron)
- banca (doar clientii respectivei banci vor avea acces)
- data expirarii cardului.

Interactiunea cu utilizatorii/posesorii cardurilor bancare prin mesaje de tip text si pictograme afisate in oricare limba cunoscuta in acest moment in lume reprezinta un avantaj major in vederea utilizarii echipamentului in orice tara din lume, sistemele actuale similare fiind limitate la afisarea mesajelor text cu caractere latine. Un alt avantaj este acela ca echipamentul poate afisa simultan mesaje de tip text in mai multe limbi, limitarea constand in dimensiunea ecranului si tipul caracterelor utilizate.
Utilizarea informatiilor inregistrate in istoricului de evenimente intern de mare capacitate impreuna cu amprenta specifica de timp(data/ora), reprezinta un avantaj major comparativ cu echipamentele actuale similare care transmit evenimentele curente pentru a fi inregistrate in unitatile de evaluare externe sau in baze de date centralizate in computere care salveaza aceste inregistrari.
Integrarea cu orice tip de unitate de evaluare de control acces care utilizeaza protocoalele de comunicatie cunoscute, reprezinta un avantaj major comparativ cu echipamentele actuale similare care functioneaza independent sau care nu permit integrarea cu alte echipamente de securitate care utilizeaza protocoale standard: Wiegand, RS232, Clock Data, Ethernet. Aceasta face posibila integrarea echipamentului in orice sistem de control acces, indiferent de generatie, utilizand protocolul Wiegand.

g. PREZENTAREA FIGURILOR

- fig.1, Schema de principiu a functionarii **echipamentului de citire si evaluare a cipurilor cardurilor bancare integrabil in sistemele de control acces prin protocol de comunicatie wiegand**:
- fig.2, Schema de conexiuni electrice a **echipamentului de citire si evaluare a cipurilor cardurilor bancare integrabil in sistemele de control acces prin protocol de comunicatie wiegand**:
- fig.3, Schema logica de functionare a **echipamentului de citire si evaluare a cipurilor cardurilor bancare integrabil in sistemele de control acces prin protocol de comunicatie wiegand;**
- fig.4, vedere a panoului frontal al echipamentului de citire a cardurilor bancare.

h. MOD DE REALIZARE A INVENTIEI:

Echipamentul de citire si evaluare a cipurilor cardurilor bancare integrabil in sistemele de control acces prin protocol de comunicatie wiegand, conform inventiei este format din :

-cititor de carduri de tip smart card MAGTEK, cod I65 (A)
-automat programabil EATON, cod XV-102 (B)
-convertor RS232->Wiegand GIGA TMS, cod CON100iB. (C)
-surse de alimentare duala(12/24V) CONSONS, cod PAT150 (E)
-carcasa externa CONIC DESIGN, cod SACD 100
-software creat de compania CONIC DESIGN
-unitate de control acces- OPTIONAL (D)

Terminologie:

PLC = automat programabil
AID = lista codurilor cipurilor specifice fiecarui emitent de carduri bancare(Ex: Visa, MasterCard, American Express, etc)
BLK = black list: lista cardurilor care ar putea fi refuzate la citire din motive de securitate dictate de administratorul sistemului
LOG = istoricul intern de evenimente
NTP = Network Time Protocol (este folosit pentru sincronizarea datei si orei intre doua echipamente/computere)
DNS = Domain Name System (este folosit pentru adresarea echipamentelor in retelele de comunicatii)
LAN = Local Area Network

i. Prezentarea modului in care inventia este susceptibila a fi aplicata

Functionarea echipamentului se bazeaza pe interconectarea componentelor electronice si interactiunea cu softul dedicat dezvoltat pentru realizarea secventelor logice descrise in schema logica de functionare a echipamentului, astfel:

Softul intern este lansat automat la pornirea automatului programabil prin includerea liniei **START \InternalStorage\Access\access.exe** in fisierul AUTOEXEC.BAT aflat pe PLC in \InternalStorage
Softul citeste fisierele de initializare (AID.ini, BLK.ini) si incearca sa comunice cu cititorul MagTek IntelliStripe 65, folosind protocolul ASCII

*la intreruperea comunicatiei dintre PLC si cititor, daca cititorul ramane in modul ASCII, timpul de resincronizare poate ajunge la 2-3 minute.

In acest timp, echipamentul afiseaza mesajul: **INCARCARE PROGRAM**
Mesajele afisate sunt imagini prelucrate in programe obisnuite de editare: word, paint, etc.
In starea de asteptare a introducerii cardului, sistemul afiseaza ledul aprins cu culoarea verde, pe ecranul LCD afisand mesajul: **PENTRU ACCES, INTRODUCETI CARDUL**

In momentul in care este detectata introducerea completa a unui card este actionat mecanismul de blocare a cardului, comandand ledul sa clipeasca intermitent cu culoarea verde, se incepe citirea cipului cardului si se afiseaza mesajul: **CITIRE CARD**
Citirea cardului poate avea 4 rezultate posibile:

- Acces permis – cardul este de tip SmartCard, are o aplicatie instalata cu un AID din fisierul AID.ini si:
  - Respecta standardul EMV, nu este expirat, nu se afla in BLK.ini
  - Nu respecta standardul EMV (nu se poate citi numarul de card si data de expirare)
- Citire nereusita
  - Cardul nu este de tip SmartCard – ex.: Card emis de un furnizor de servicii de transport sau de comunicatii sau card pentru aplicatii obisnuite de control acces
  - Cardul a fost extras (fortat) inainte sa poata fi citit
- Card refuzat – cardul este de tip SmartCard si:
  - Nu are un AID din fisierul AID.ini
  - Are un AID din AID.ini, respecta standardul EMV si numarul cardului se afla in fisierul BLK.ini
- Card expirat – cardul este de tip SmartCard, are un AID din fisierul AID.ini, respecta standardul EMV, numarul cardului nu se afla in fisierul BLK.ini si data de expirare (An/Luna) este anterioara datei curente (An/Luna)

  *cardurile care expira in luna curenta nu sunt considerate expirate

La terminarea citirii cardului se seteaza ledul sa fie aprins cu culoarea verde si se afiseaza mesajul:**RETRAGETI CARDUL**

Daca trece 1 minut de la afisarea mesajului de mai sus si cardul nu a fost retras, se seteaza ledul aprins intermitent cu culoarea rosie, se notifica sistemul de acces control cu mesajul „**4**", se afiseaza mesajul de mai jos si se asteapta extragerea cardului: **CARD UITAT, APELATI NUMARUL.....**
Dupa extragerea cardului, se revine la etapa: **PENTRU ACCES, INTRODUCETI CARDUL**, fara a se lua in considerare rezultatul citirii.
Daca extragerea cardului a fost facuta in mai putin de 1 minut de la afisarea mesajului **RETRAGETI CARDUL**, in continuare se trece la faza corespunzatoare rezultatului citirii (pentru 2 secunde), iar apoi se revine la faza initiala **PENTRU ACCES, INTRODUCETI CARDUL**.

- Acces Permis: se seteaza ledul aprins cu culoarea verde, se seteaza buzzerul sa produca un ton scurt (1.5 KHz – 160ms), se trimite mesaj catre unitatea de control acces cu mesajul „**1**" si se afiseaza mesajul: **ACCES PERMIS**
- Citire nereusita: se activeaza ledul aprins cu culoarea rosie, se activeaza buzzerul sa produca un ton lung (2.5 KHz – 2 secunde), se trimite mesaj catre unitatea de control acces cu mesajul „**0**" si se afiseaza mesajul: **CITIRE NEREUSITA**
- Card refuzat: se activeaza ledul aprins cu culoarea rosie, se activeaza buzzerul sa produca un ton lung (2.5 KHz – 2 secunde), se trimite mesaj catre unitatea de control acces cu mesajul „**2**" si se afiseaza mesajul: **CARD REFUZAT**
- Card expirat: se activeaza ledul aprins cu culoarea rosie, se activeaza buzzerul sa produca un ton lung (2.5 KHz – 2 secunde), se trimite mesaj catre sistemul acces control cu mesajul „**3**" si se afiseaza mesajul: **CARD EXPIRAT**

In faza de asteptare a introducerii unui card, intern se verifica in mod continuu daca exista fisierul **MSG.ini** in **\InternalStorage\Access** . Daca acesta exista, este citit si apoi sters, iar in functie de continutul lui se pot executa:

- **RESET** PLC – se afiseaza mesajul de eroare, se elibereaza resursele alocate (COM port, fisier log, se stinge LEDul) si se reseteaza PLC-ul
- **AID** – se copiaza fisierul ADI.ini din **\InternalStorage\Access\Update** in **\InternalStorage\Access** si se citeste din nou AID.ini
- **BLK** – se copiaza fisierul BLK.ini din **\InternalStorage\Access\Update** in **\InternalStorage\Access** si se citeste din nou BLK.ini
- **UPDATE** – se afiseaza mesajul de eroare, se elibereaza resursele alocate (COM port, fisier log, se stinge LED-ul), se lanseaza programul **update.exe** din **\InternalStorage\Access\Update** si se inchide programul. **Update.exe** copiaza programul nou **access.exe** din **\InternalStorage\Access\Update** in **\InternalStorage\Access** si il lanseaza
- **ROTATE** – se inchide fisierul de log **log.log** aflat in **\InternalStorage\Access** se redenumeste in **log_old.log** in aceeasi cale si se creaza un nou fisier de log

  *acest mesaj este generat automat de catre program in cazul in care fisierul de log depaseste o dimensiune prestabilita (5 MB)

In orice etapa a programului, daca apar erori in comunicatia echipamentului PLC cu cititorul, se elibereaza resursele alocate (COM port, fisier log), se incearca reluarea automata a comunicatiei, si se afiseaza mesajul: **SISTEM INDISPONIBIL**

Daca apar erori la deschiderea portului COM, intern se afiseaza mesajul de eroare, se asteapta 1 minut, se incearca din nou deschiderea portului COM si daca nici atunci nu reuseste, se reseteaza PLC-ul automat.

*perioada de 1 minut este utila operatorului care poate astfel modifica fisierul AUTOEXEC.BAT, astfel incat programul sa nu mai fie lansat la urmatoarea pornire si sa se poate identifica problemele/programele care impiedica accesul acestuia la portul COM

Instalarea si incarcarea softului intern:

i. Se copiaza intr-un director local (calea nu trebuie sa contina spatii – ex: e:\PLC_program) folderele (**INI_files, Log, Messages, Programs**) care contin programul si fisierele asociate
ii. Se completeaza in fisierul Excel asociat (**CONFIG**):

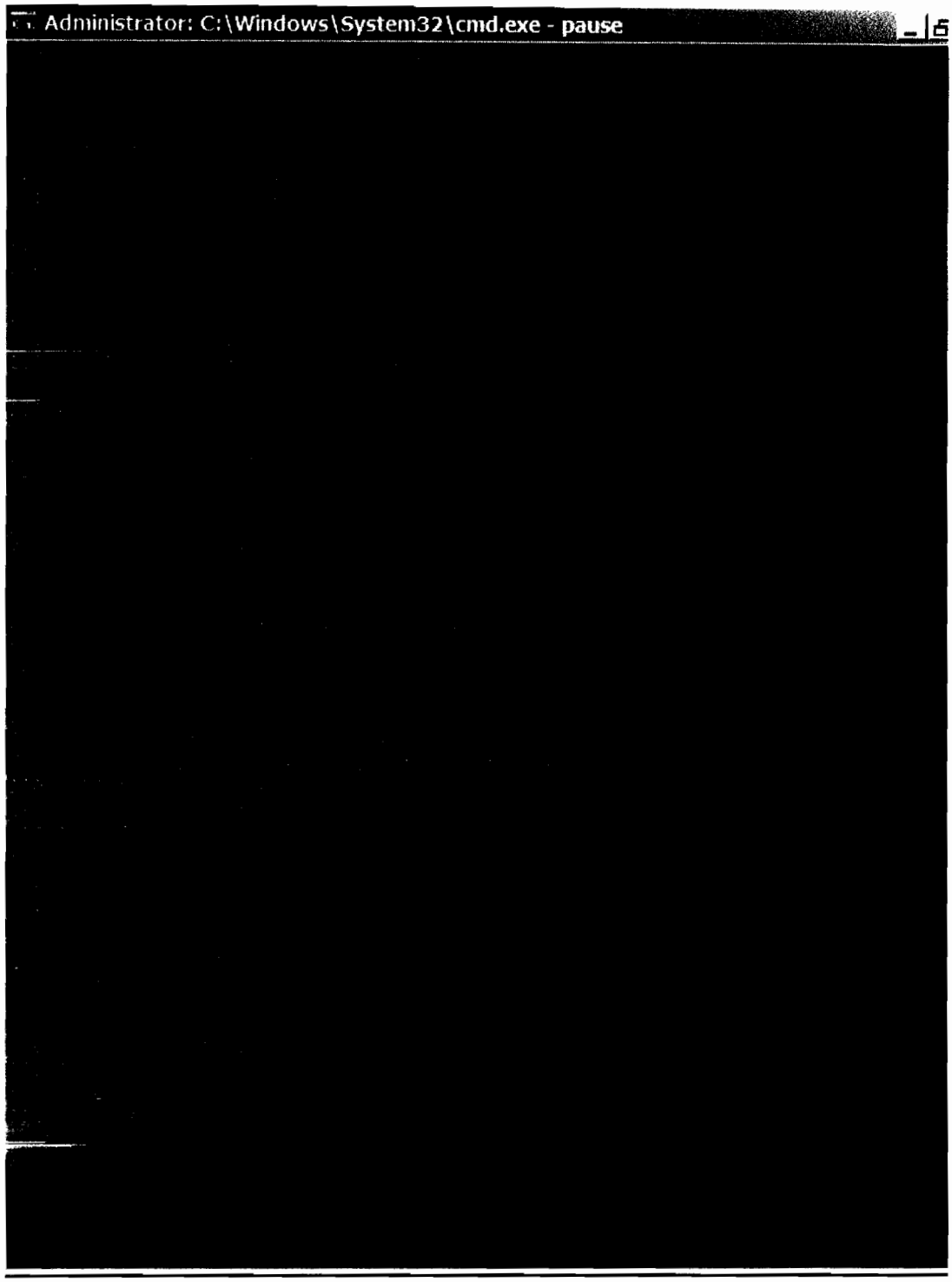
-in sheetul **Batch**, calea unde se afla fisierele necesare instalarii (**D1**)

-in casutele colorate in verde informatiile necesare (nume PLC – nu trebuie sa contina spatii, adresa IP PLC, parola pentru acces pe serverul de FTP de pe PLC)

*setarea unei parole pentru serverul de FTP reprezinta o masura de limitare a accesului la PLC (posibila prin setare manuala din PLC)

-se copiaza comenzile din coloana **Install Application** intr-o fereastra **CLI**

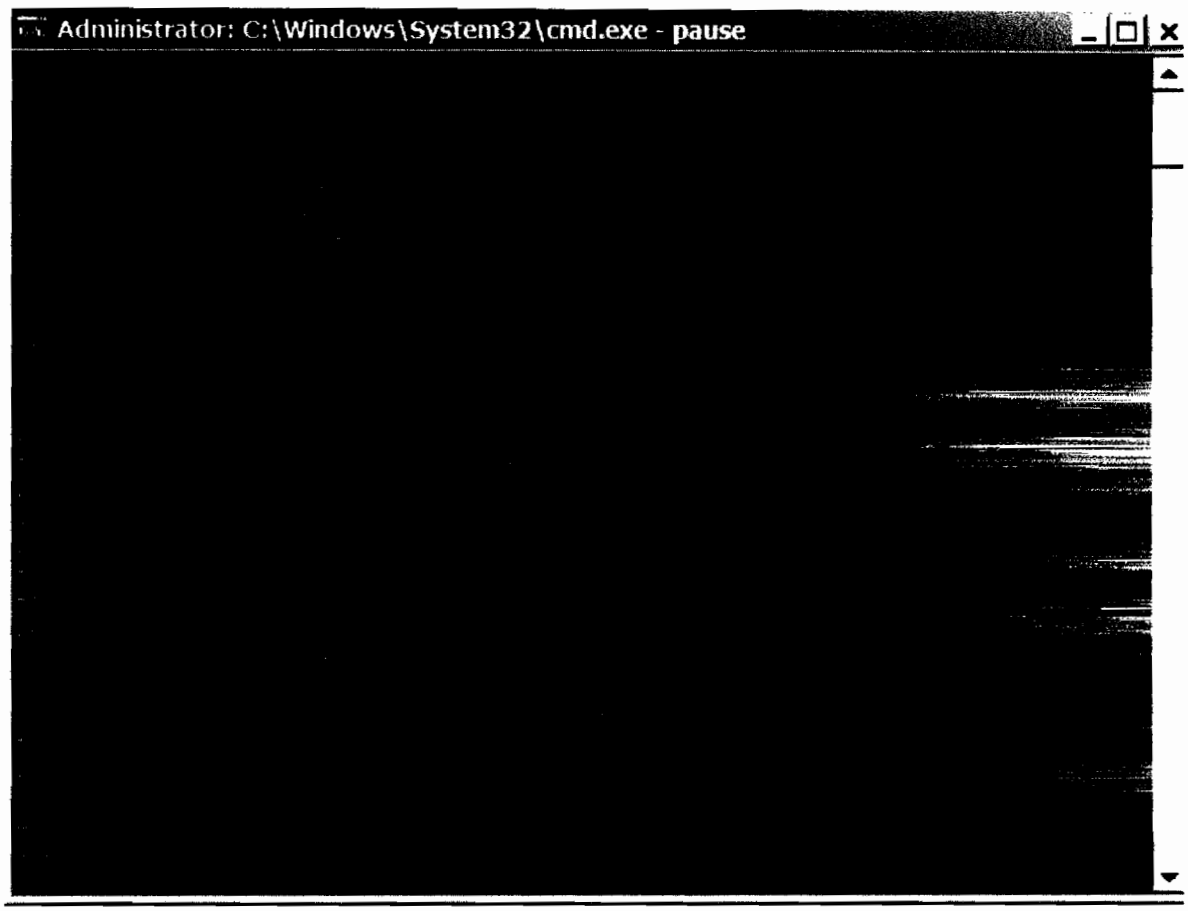
-se da reset la PLC (oprire alimentare)



Update program

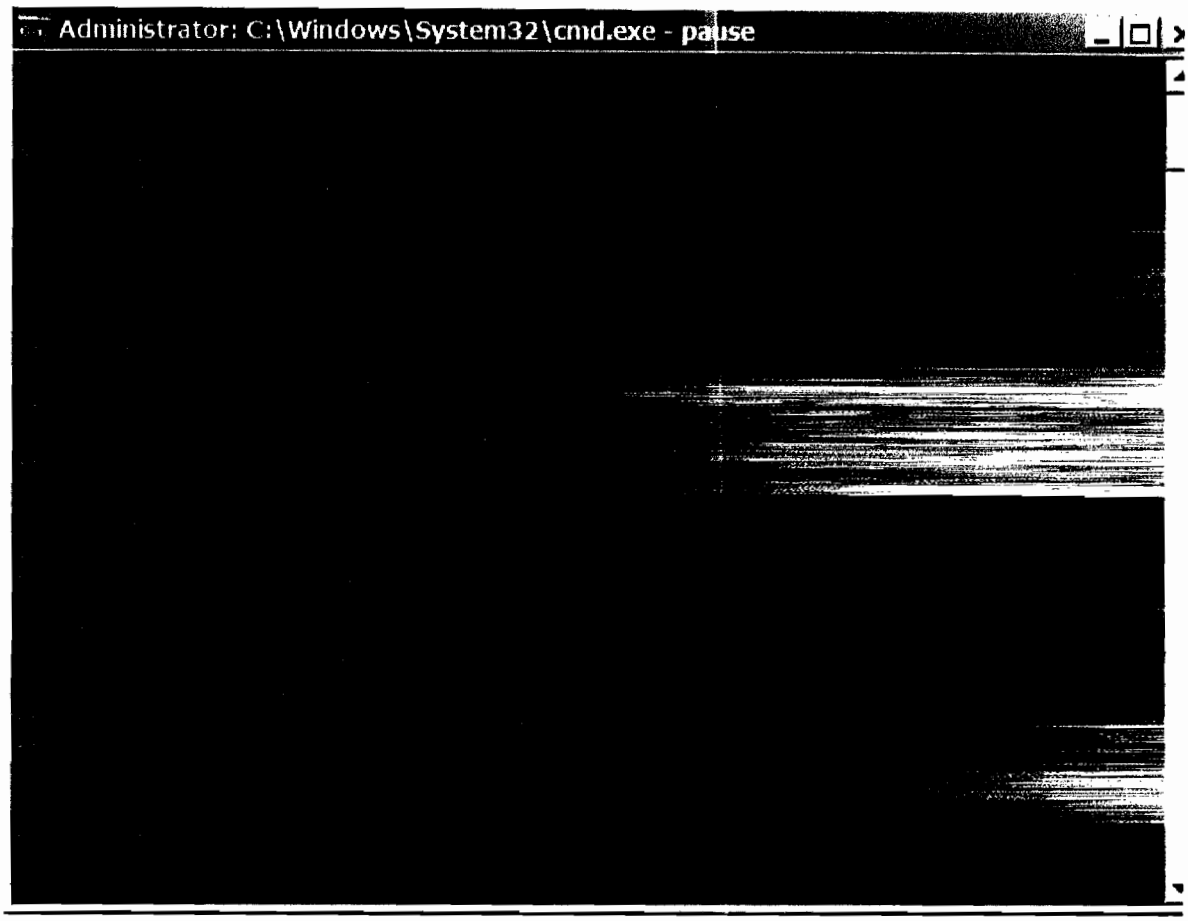
iii. Se copiaza executabilul nou (**access.exe**) in folderul **Programs**

iv. Se copiaza comenzile din fisierul excel **CONFIG,** coloana **Application Update** intr-o fereastra CLI



Update lista AID

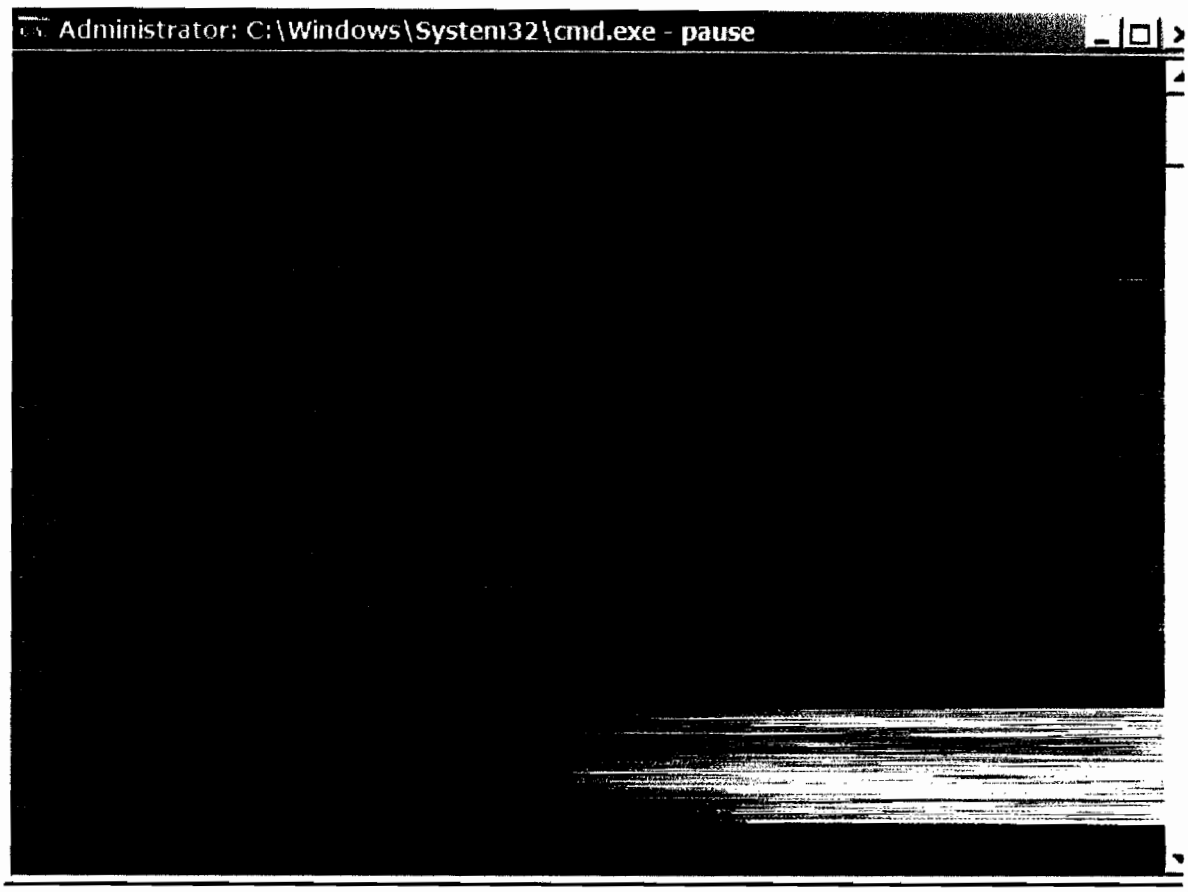
v. Se copiaza fisierul nou AID.ini in folderul **INI_files**
vi. Se copiaza comenzile din fisierul excel **CONFIG,** coloana **AID Update** intr-o fereastra CLI



Update lista BLK

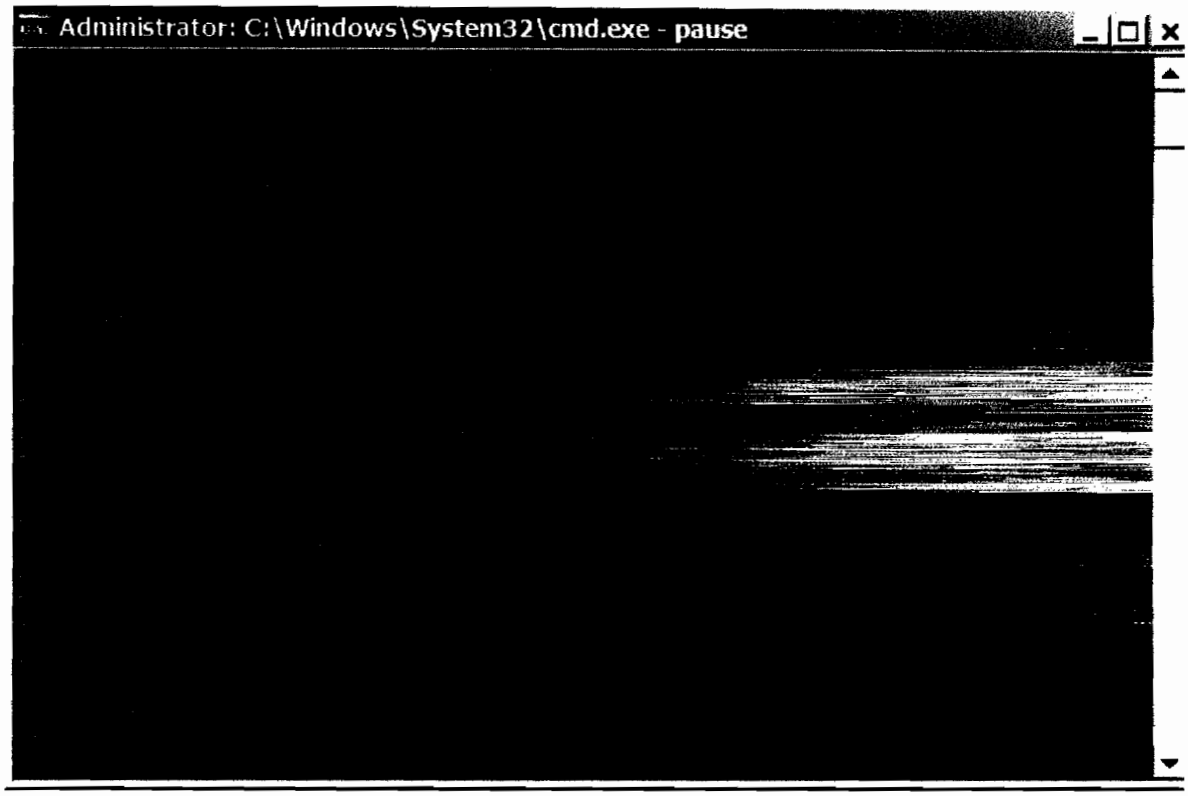
vii. Se copiaza fisierul nou **BLK.ini** in folderul **INI_files**

viii. Se copiaza comenzile din fisierul excel **CONFIG,** coloana **BLK Update** intr-o fereastra CLI



Rotatie LOG

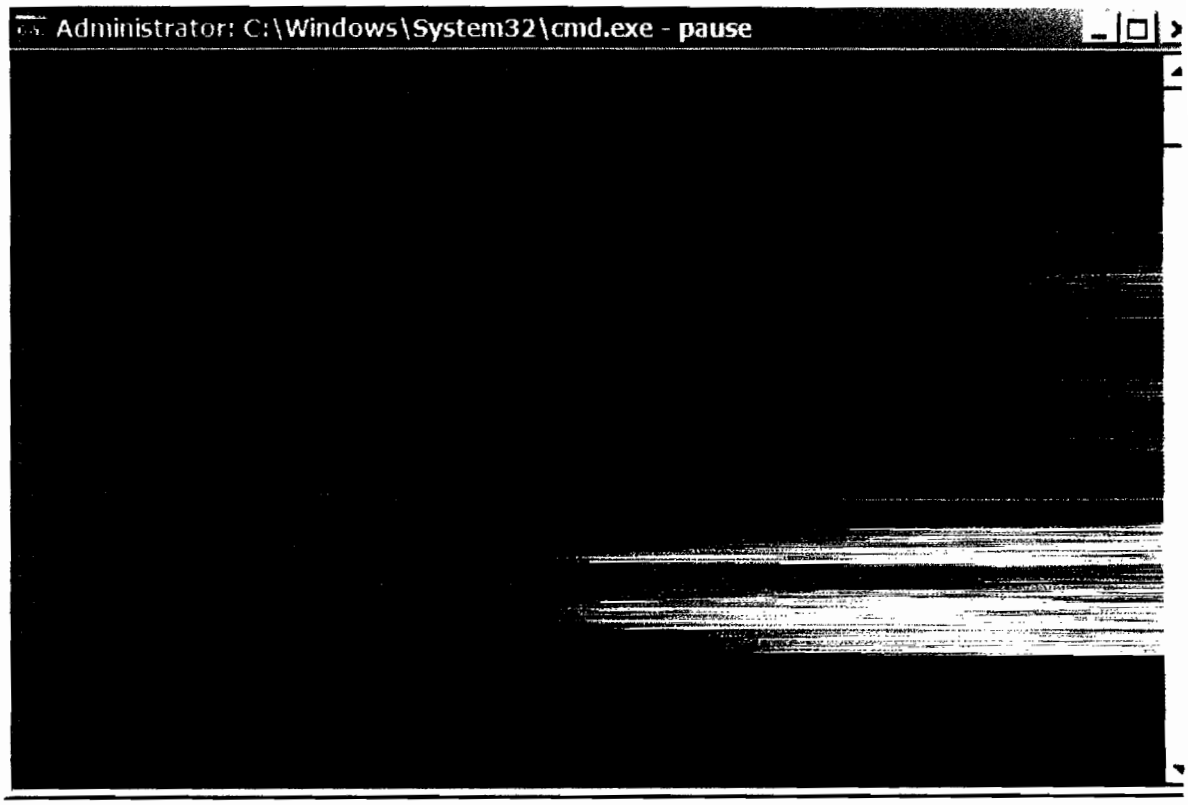
ix. Se copiaza comenzile din fisierul excel **CONFIG,** coloana **LOG Rotate** intr-o fereastra CLI



Copiere LOG

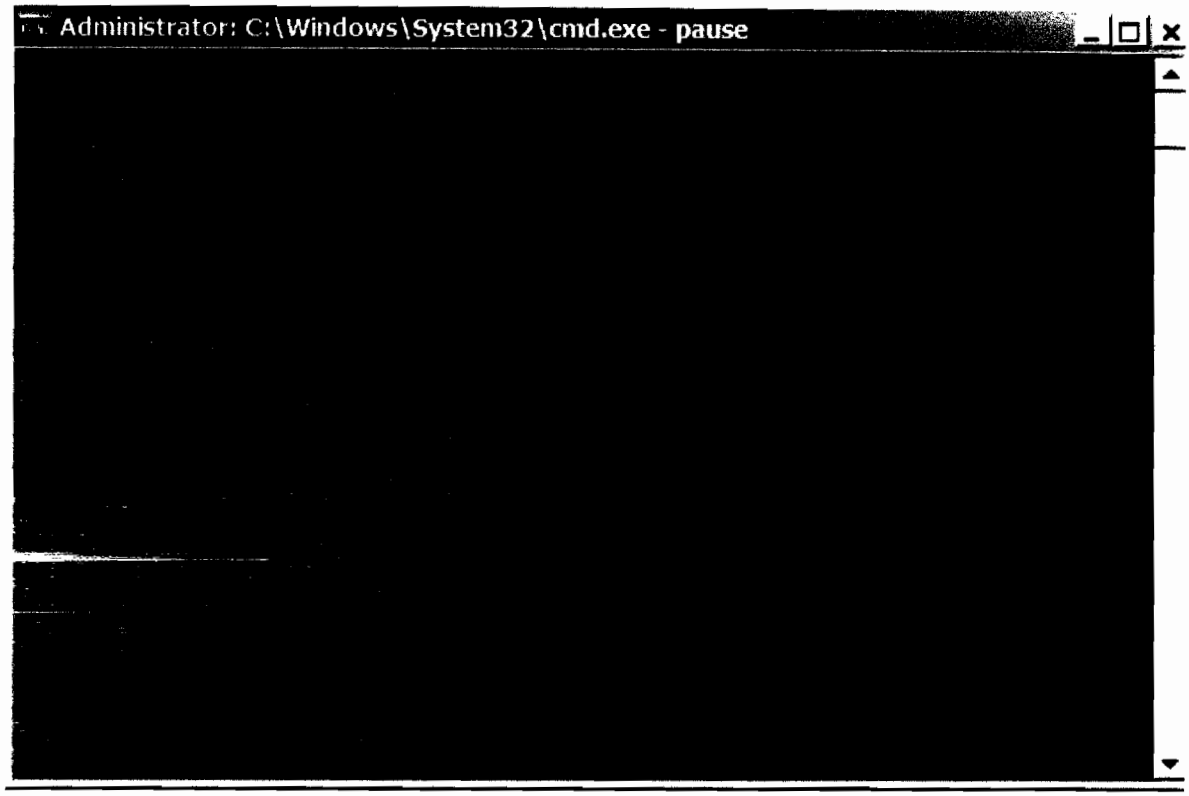
x. Se copiaza comenzile din fisierul excel **CONFIG,** coloana **LOG Copy** intr-o fereastra CLI

*se copiaza fisierul **log_old.log** de pe PLC in folderul **Log,** cu numele **%Nume PLC%log_old.log**



Reset PLC

xi. Se copiaza comenzile din fisierul excel **CONFIG,** coloana **RESET** intr-o fereastra CLI



Caracteristici tehnice:

xii. AID este limitat la un anumit numar de tipuri de carduri sau poate include toate tipurile de carduri emise de toti emitentii inregistrati si declarati in standardul EMV

xiii. BLK este limitat la 1000 inregistrari (valoarea poate fi marita daca nu se mai incarca lista de carduri in memorie, dar asta poate conduce la cresterea timpului necesar citirii si validarii cardului)

Pentru evaluarea corecta a informatiilor din LOG si pentru validarea cardurilor (comparatie data expirare – data curenta) este posibila sincronizarea PLC-ului cu un server NTP (preferabil in LAN) – poate fi defint in DNS-ul intern o inregistrare care sa foloseasca **tock.usno.navy.mil** sau **time.windows.com** pentru a directiona PLC-ul catre serverul de NTP.

a-2013-00379--
20-05-2013

REVENDICARE

Echipament de citire si evaluare a cipurilor cardurilor bancare integrabil in sistemele de control acces prin protocol de comunicatie wiegand, pentru controlul accesului catre zone importante sau de inalta securitate, **caracterizat prin acea ca** este format dintr-un

-cititor de carduri de tip smart card MAGTEK, cod I65 (**A**)

- un automat programabil , cod XV-102 (**B**)

- un convertor RS232->Wiegand GIGA TMS, cod CON100iB. (**C**)

-surse de alimentare duala(12/24V) CONSONS, cod PAT150 (**E**)

-o carcasa externa , cod SACD 100

-un software CONIC DESIGN si

-o unitate de control acces- (**D**)

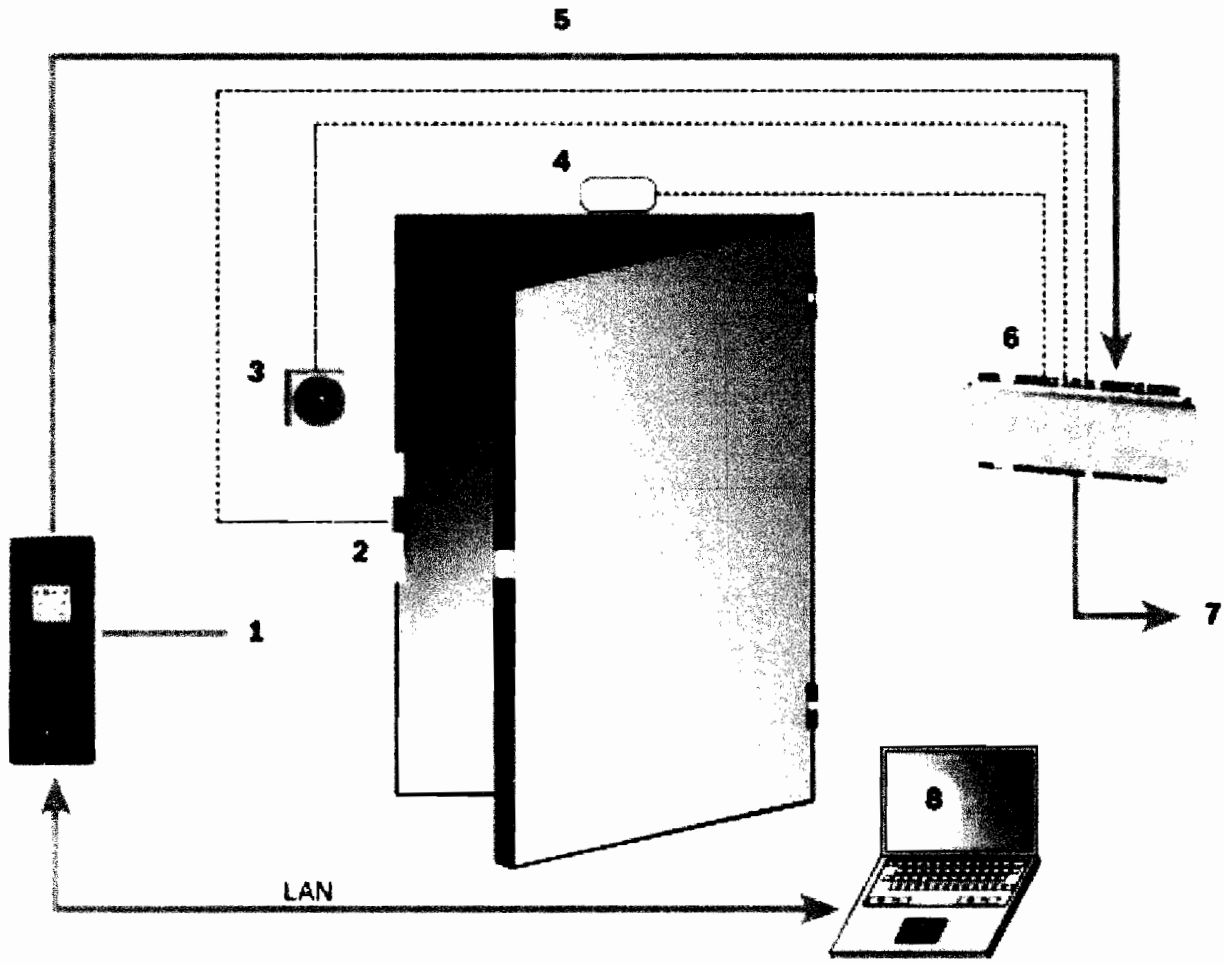


Fig. 1

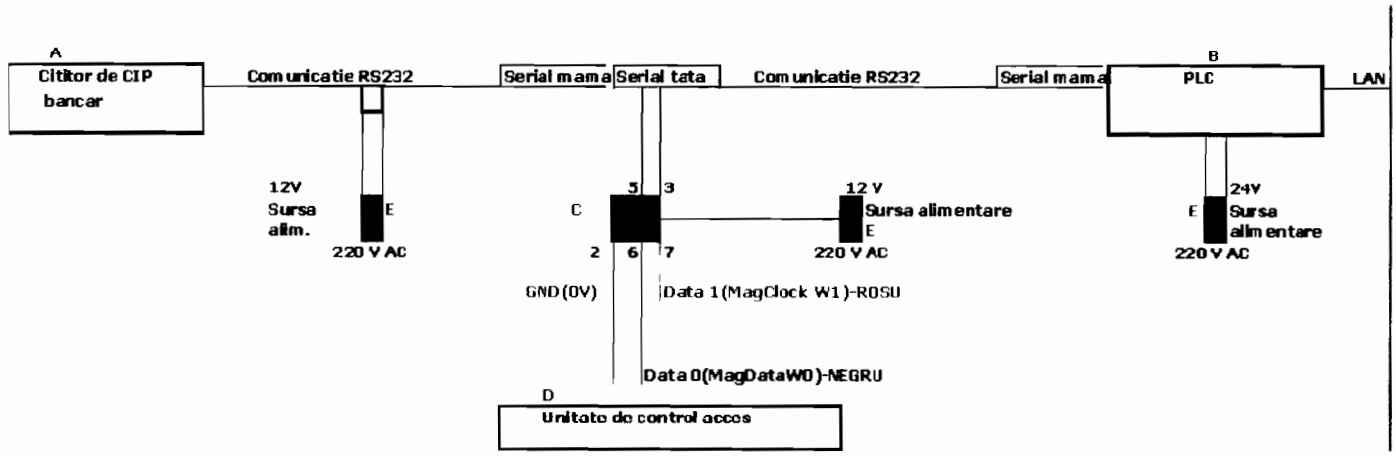

A
Cititor de CIP bancar
Comunicatie RS232
Serial mama
Serial tata
Comunicatie RS232
Serial mama
B
PLC
LAN
12V Sursa alim.
E
220 V AC
C
5
3
2
6
7
12 V
Sursa alimentare
E
220 V AC
E
24V
Sursa alimentare
220 V AC
GND (0V)
Data 1 (MagClock W1)-ROSU
Data 0(MagDataW0)-NEGRU
D
Unitate de control acces

Fig. 2

a-2013-00379--
20 -05- 2013

SCHEMA LOGICA DE FUNCTIONARE A ECHIPAMENTULUI

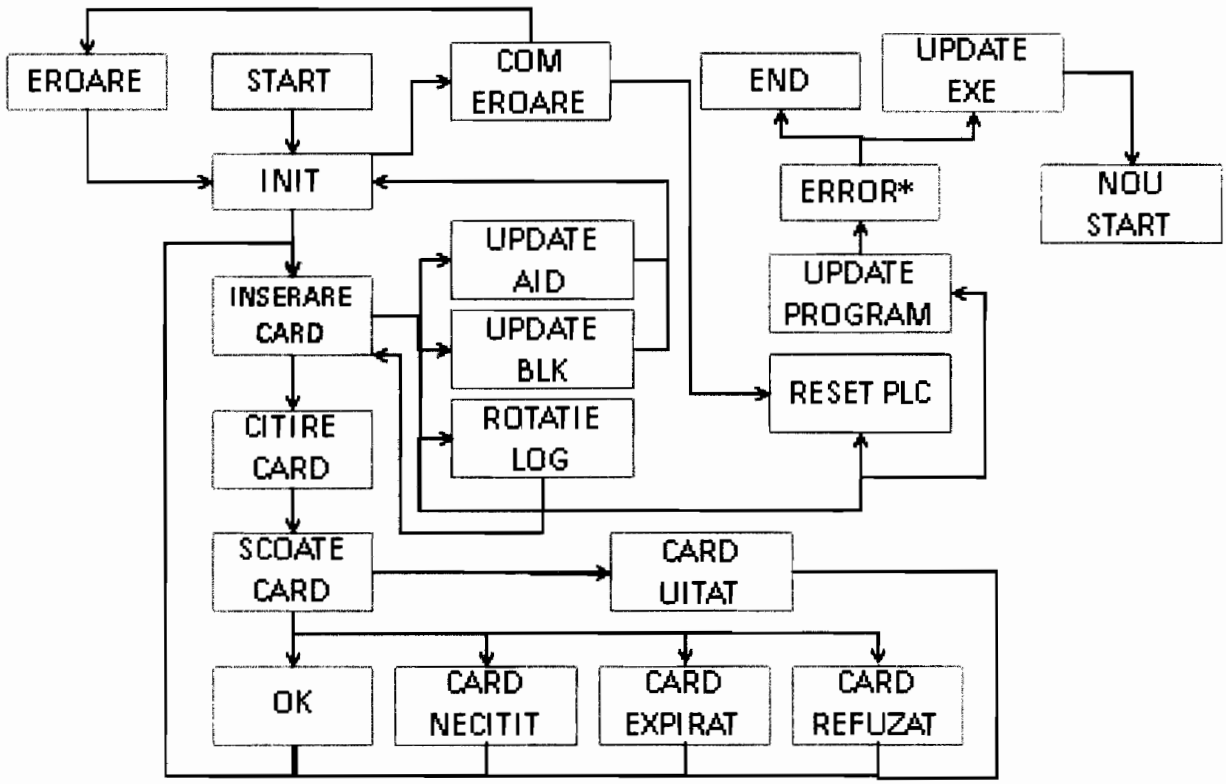


Fig. 3

0-2013-00379--
20-05-2013

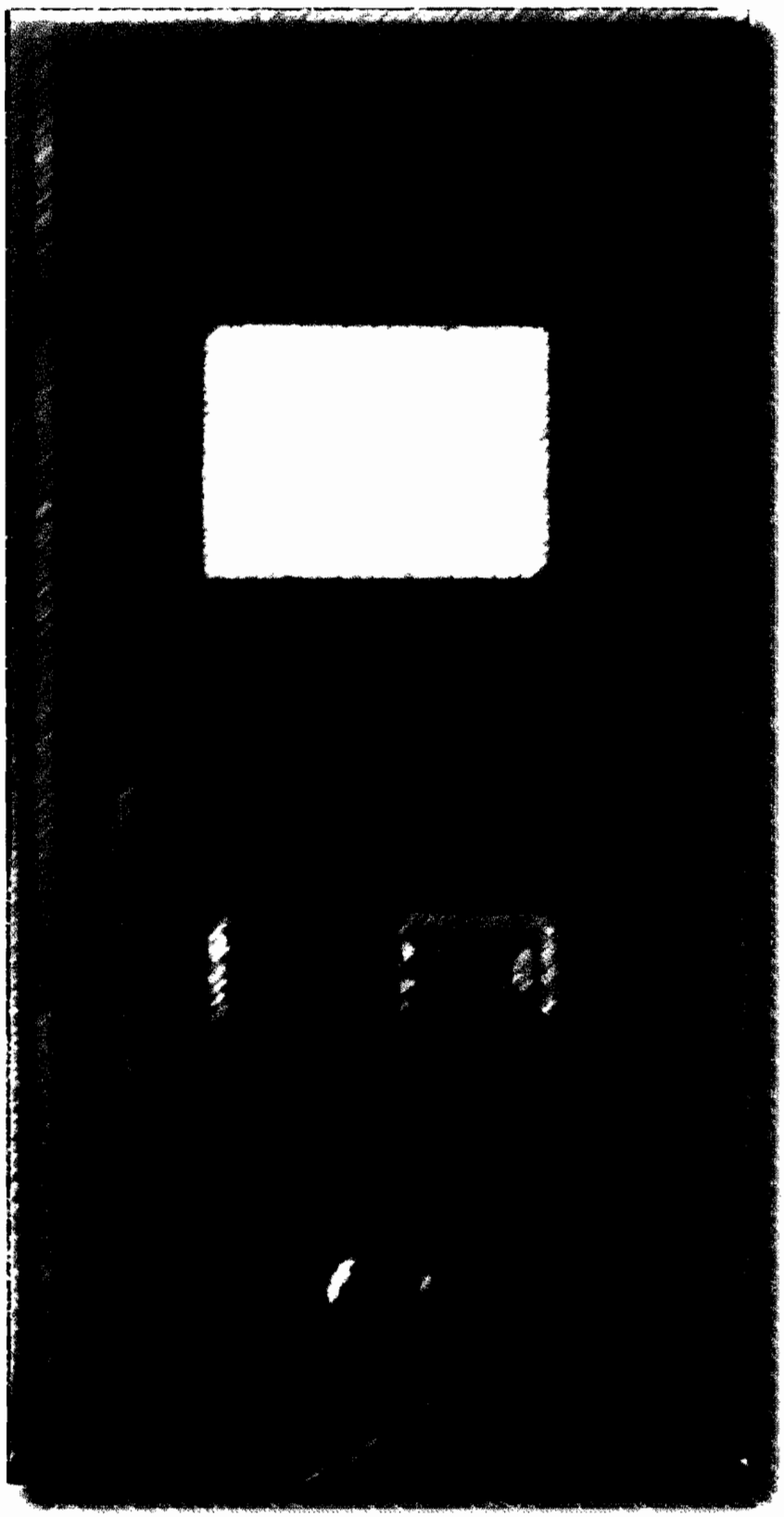


Fig. 4