(19) **OFICIUL DE STAT PENTRU INVENŢII ŞI MĂRCI**
Bucureşti

ROMÂNIA

(11) **RO 134860 A2**
(51) **Int.Cl.**
G06F 21/70 (2013.01)

(12) # CERERE DE BREVET DE INVENŢIE

(21) Nr. cerere: **a 2019 00609**

(22) Data de depozit: **30/09/2019**

(41) Data publicării cererii:
30/03/2021 BOPI nr. **3/2021**

(71) Solicitant:
• **UNIVERSITATEA POLITEHNICA DIN BUCUREŞTI**, *SPLAIUL INDEPENDENŢEI NR.313, SECTOR 6, BUCUREŞTI, B, RO*

(72) Inventatori:
• **SVASTA PAUL**,
STR.CETATEA DE BALTĂ, NR.131, BL.1, SC.B, ET.3, AP.18, SECTOR 6, BUCUREŞTI, B, RO;
• **VASILE DANIEL-CIPRIAN**,
STR. NERVA TRAIAN NR.10, BL.M38, SC.3, AP.78, SECTOR 3, BUCUREŞTI, B, RO

(54) # REŢEA CONDUCTIVĂ DE PROTECŢIE A CIRCUITELOR ELECTRONICE DE SECURITATE ÎMPOTRIVA INTRUZIUNILOR FIZICE

(57) **Rezumat:**

Invenţia se referă la o reţea conductivă de protecţie a circuitelor electronice de securitate împotriva intruziunilor fizice care funcţionează împreună cu un circuit activ de detecţie a intruziunilor, pentru a proteja datele de securitate procesate şi stocate de circuitele electronice de securitate, precum: module criptografice, dispozitive de plată securizată şi alte circuite electronice care implementează funcţii de securitate. Reţeaua conductivă, conform invenţiei, conţine trei straturi cu trasee conductive imprimate pe substraturi flexibile sau rigide, acoperind în totalitate circuitele electronice protejate, separate prin straturi dielectrice, în care: primul strat, situat spre circuitele protejate, este format dintr-o suprafaţă (**1**) conductivă care acoperă întreaga suprafaţă a reţelei conductive, al doilea strat este realizat din trasee (**2**) conductive foarte subţiri, cu spaţii foarte mici între trasee, ce formează un circuit conductiv prevăzut cu un port (**5**) de intrare şi un port (**6**) de ieşire, iar cel de-al treilea strat, situat deasupra celui de-al doilea strat şi expus la exterior, conţine trasee (**3**, **4**) conductive cu acelaşi model ca cel al traseelor (**2**) stratului al doilea şi suprapuse cu acestea, asigurând cuplaje inductive şi capacitive între ele, traseele (**3**, **4**) conductive ale stratului al treilea formând circuite închise, astfel încât efectuarea unei intruziuni asupra traseelor (**3**, **4**) conductive ale stratului al treilea determină modificarea caracteristicilor de circuit ale traseului conductiv (**2**) de pe stratul al doilea, iar circuitul (**8**) activ de detecţie a intruziunilor, care sondează traseul (**2**) conductiv de pe stratul al doilea cu semnale corespunzătoare în vederea detectării caracteristicilor acestuia, poate detecta o intruziune fizică, situaţie în care şterge datele de securitate.

Revendicări: 11
Figuri: 2

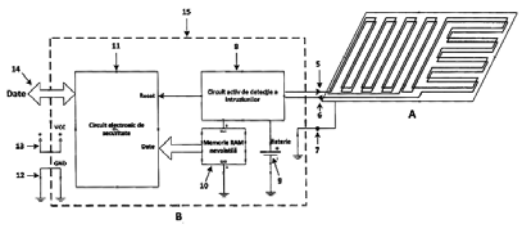

Fig. 1

RO 134860 A2

Contextul invenției

Invenția se referă la o rețea conductivă și la modul de utilizare a acesteia în scopul protecției circuitelor electronice de securitate împotriva intruziunilor fizice. Aceasta funcționează împreună cu un circuit activ de detecție a intruziunilor pentru protejarea datelor de securitate procesate și stocate de circuitele electronice de securitate, precum: module criptografice, dispozitive de plată securizată și alte circuite electronice care implementează funcții de securitate.

Invenția face parte din domeniul tehnic al electronicii, fiind o combinație de elemente de electonică analogică și elemente de electronică digitală.

Protecția împotriva intruziunilor fizice (cunoscută în literatura de specialitate sub denumirea, în limba engleză, "*anti-tamper protection*") are ca scop blocarea accesului persoanelor neîndreptățite să cunoască datele conținute de circuitele electronice de securitate. O astfel de persoană este numită persoană neautorizată.

Intruziunile fizice reprezintă totalitatea acțiunilor ce duc la obținerea accesului la circuitele integrate și la traseele conductoare ce formează circuitul electronic de securitate. Prin efectuarea unei intruziuni fizice, o persoană neautorizată poate obține informații despre datele de securitate procesate sau stocate de circuitul electronic de securitate.

Datele de securitate sunt considerate a fi orice date confidențiale în format electronic, precum: chei criptografice, date secrete, programe informatice proprietare ("*firmware*"), etc.

Circuitele electronice de securitate (CES) sunt formate din circuite integrate logice (procesoare, circuite programabile tip FPGA și CPLD, porți logice, etc.), interconectate, care execută funcții funcții criptografice și stochează date de securitate. Circuitele electronice de securitate pot funcționa în cadrul unui echipament sau independent. În cazul în care funcționează independent, circuitul electronic de securitate poate implementa și alte funcții, complementare celor de securitate, precum: comunicații de date, asigurarea alimentării cu energie electrică, interfață pentru senzori și acționări, etc.

Protecția împotriva intruziunilor fizice asupra CES se realizează cu ajutorul unui ansamblu format dintr-o rețea conductivă și un circuit de detecție a intruziunilor.

Rețeaua conductivă este realizată din trasee conductive, foarte subțiri și apropiate, pe un substrat izolator rigid (cablaj imprimat) sau flexibil (folie imprimată). Rețeaua conductivă acoperă în totalitate circuitul electronic protejat, orice intervenție asupra ei fiind detectată de circuitul de detecție a intruziunilor. Utilizarea unor modele

complexe de realizare a rețelei conductive asigură o rezistență crescută la tentativele de intruziune fizică.

Circuitul de detecție a intruziunilor monitorizează starea rețelei conductive și în cazul în care determină neconcordanțe față de starea de referință, acționează în sensul păstrării caracterului confidențial al datelor de securitate (sau nedestinate persoanelor neîndreptățite să le cunoască): zeroizarea datelor (suprascrierea datelor), ștergerea datelor sau distrugerea fizică a unui element critic de circuit.

O metodă uzuală de stocare a datelor de securitate este utilizarea unei memorii RAM (*Random Access Memory*) a cărei tensiune de alimentare este asigurată (controlată) de circuitul de detecție a intruziunilor, iar în cazul detecției unei intruziuni, întrerupe alimentarea acestei memorii, cunoscută sub denumirea de "memorie RAM nevolatilă". Caracterul "nevolatil" este dat de faptul că tensiunea de alimentare a memoriei RAM este asigurată de o baterie de rezervă, sau acumulator, pe duratele când echipamentul nu este alimentat de la rețea. Această metodă este cea mai rapidă din punct de vedere al duratei de ștergere a datelor stocate față de alte metode de stocare (de ex. memorii EEPROM, FLASH, etc.).

Analiza rețelei conductive se poate realiza în mod pasiv, prin injectarea unui curent constant prin aceasta, sau în mod activ prin sondarea cu semnale corespunzătoare. Circuitele active de detecție a intruziunilor (CADI) prezintă o sensibilitate crescută în detecția tentativelor de intruziune, față de circuitele pasive de detecție a intruziunilor, oferind un răpuns eficient și rapid.

O structură de protecție împotriva intruziunilor este prezentată în brevetul US9298956B2 ("*Tamper Protection Mesh in an Electronic Device*", Jeremy Wade, Thomas Templeton, Trent Weber, Michael Lamfalusi) formată dintr-o rețea conductivă, creată pe partea interioară a carcasei ce protejează circuitele electronice, și un circuit ce detectează apariția stărilor de circuit închis sau circuit deschis. În cazul acestei invenții, limitarea detecției la aceste stări, nu permite determinarea cazului în care un traseu conductiv este modificat prin efectuarea unui scurt circuit între două puncte ale aceluiași traseu în scopul dezafectării detecției intruziunilor pentru o zonă acoperită de acest traseu.

O metodă eficientă de detecție a intruziunilor este propusă în brevetul US8689357B2 ("*Tamper Detector for Secure Module*", Mohit Arora, Rakesh Pandey, Pushkar Sareen, Prashant Bhargava). Circuitul de detecție generează impulsuri cu ajutorul unor generatoare de impulsuri tip LFSR (*Linear Feedback Shift Registers*) cu care sondează traseele rețelei conductive. Semnalele rezultate sunt transformate în impulsuri și sunt verificate cu semnalele originale întârziate cu o durată bine

determinată. Intruziunea este detectată în cazul în care aceste semnale nu sunt corelate. Această metodă, bazându-se pe verificarea întârzierii impulsurilor prin rețeaua conductivă, nu analizează caracteristicile de circuit care afectează propagarea impulsurilor prin rețeaua conductivă. Astfel, în condiții tehnologice corespunzătoare, se poate dezafecta o zonă acoperită de circuitul conductiv prin realizarea unui circuit extern de întârziere a impulsurilor care să conecteze două puncte ale rețelei conductive.

Problema tehnică pe care o rezolvă prezenta invenție constă în obținerea unui sistem format dintr-o rețea conductivă și un circuit activ de detecție a intruziunilor care să să detecteze intruziunile fizice și tentativele de intruziuni, cum ar fi: efectuarea de scurt-circuite ale traseelor conductive fără modificarea curenților de sondare, realizarea de circuite externe care să simuleze întârzierea semnalelor de sondare sau simularea semnalelor de sondare. Aceste acțiuni, funcție de metoda utilizată în detecție a intruziunilor, au rolul de a dezactiva zone ale rețelei conductive în scopul facilitării accesului la circuitele electronice protejate.

Avantajele invenției sunt:

- performanțe superioare în detecția intruziunilor fizice prin analiza caracteristicii de transfer a rețelei conductive;
- traseele conductive expuse spre exterior sunt izolate galvanic de traseele conductive sondate cu semnale de circuitul activ de detecție a intruziunilor, fapt ce împiedică o eventuală măsurare a caracteristicilor semnalelor utilizate în sondare;
- accesul la traseele conductive sondate cu semnale de circuitul activ de detecție a intruziunilor se poate face numai după îndepărtarea traseelor de pe stratul exterior, fapt ce determină detecția intruziunii;
- stratul pe care se află traseul conductiv sondat cu semnale de circuitul activ de detecție a intruziunilor este ecranat electromagnetic față de circuitele electronice protejate, eliminând influența acestora în detecția intruziunilor;

În continuare, este prezentată invenția în legătură cu figurile 1 și 2, în care:

- figura 1 prezintă structura rețelei conductive, formată din trei straturi cu trasee conductive, izolate cu straturi dielectrice;
- figura 2 prezintă schema de principiu a sistemului de protecție împotriva intruziunilor fizice a circuitelor electronice de securitate, ce conține rețeaua conductivă, circuitul activ de detecție a intruziunilor, circuitul electronic de

securitate și alte elemente necesare asigurării funcției de protecție împotriva intruziunilor.

Descrierea invenţiei

Invenția se referă la o rețea conductivă de protecţie a circuitelor electronice de securitate (CES) și la modul de utilizare a acesteia, în scopul realizării funcției de protecție a CES.

Rețeaua conductivă (RC) este o structură formată din trei straturi ce conțin trasee conductive, izolate cu straturi dielectrice. RC poate fi realizată din cablaj imprimat rigid tip FR4 (sticlotextolit), sau folie flexibilă imprimată. RC este prezentată în figura 1, ansamblul A.

Primul strat al RC, notat cu 1, este format dintr-o suprafață conductivă ce acoperă întreaga suprafață a RC. Este conectat la semnalul de masă al CADI și CES prin intermediul conexiunii 7. Acest strat este situat între CES și CADI și restul straturilor conductive.

Cel de-al doilea strat, format din traseul notat cu 2, este realizat din trasee conductive foarte subțiri, cu spații foarte mici între trasee, ce formează un circuit conductiv prevăzut cu un port de intrare 5 și un port de ieșire 6. Portul 5 este utilizat pentru aplicarea unui semnal de sondare a RC iar portul 6 este utilzat pentru achiziția semnalului reultat în urma sondării RC. Aceste semnale au ca referință planul de masă disponibil la conexiunea 7. Aplicarea semnalului de sondare prin portul 5 și achiziția semnalului de răspuns al RC la portul 6 este efectuată de CADI. Traseul 2 are un model sub formă de meandre. Dimensiunile foarte mici ale traseelor, împreună cu spațiile foarte mici între trasee și modelul sub formă de meandre, au rolul de a îngreuna eventualele tentative de intruziune sau de dezafectare a unor zone ale RC prin realizarea de șunturi. Traseul 2 este organizat sub forma unor zone, astfel încât acesta este compus din conectarea în serie a tuturor zonelor care compun RC, pe acest strat.

Cel de-al treilea strat, situat deasupra stratului format de traseul 2, conține trasee conductive cu aceleași dimensiuni și model ca cele ale traseului 2, însă fiecare zonă este conectată în scurt circuit. Spre exemplificare, în figura 1 au fost reprezentate doar două zone, formate din traseele notate cu 3 și 4. Aceste trasee se suprapun exact peste traseul 2, excepție făcând traseele care realizează scurt-circuitul fiecărei zone. Traseele 3 și 4 sunt cuplate capacitiv și inductiv cu traseul 2, determinând modificarea caracteristicii de propagare a traseului 2. De asemenea, în cazul în care cel puțin unul dintre traseele conductive de pe cel de-al treilea strat (circuite închise) este afectat de o intruziune (deschiderea circuitului sau producerea

unui scurt circuit între trasee), caracteristica de transfer a traseului 2 va suferi modificări. Aceste modificări sunt detectate de CADI care acționează în sensul protejării datelor de securitate ale CES. Stratul al treilea, ce conține zone cu trasee închise (în scurt circuit), este expus la exterior. Ansamblul RC împreună cu CADI va detecta rapid și eficient intruziunile fizice deoarece primul strat afectat va fi cel de-al treilea strat. Totodată, o determinare exhaustivă a parametrilor semnalelor utilizate în sondarea RC, efectuată de un potențial atacator, nu se poate realiza prin analiza celui de al treilea strat deoarece acesta nu este conectat galvanic la traseul 2, prin care se propagă semnalele de sondare.

Modul de utilizare al RC, în scopul asigurării securității CES, este prezentat în figura 2. Circuitele CES (11), CADI (8), memoria RAM (*Random Access Memory*) nevolatilă (10) și bateria (9) formează ansamblul B, prezentat în figura 2. Acest ansamblu este acoperit în totalitate de RC (ansamblul A), așa cum este reprezentat în figura 2 prin linia segmentată 15, fără a lăsa fante sau orificii care să permită observarea acestor circuite din exterior.

Porturile de intrare 5 și ieșire 6, împreună cu conexiunea de masă 7 sunt conectate la CADI, respectiv la semnalul de masă comun elementelor componente ale ansamblului B. Astfel, CADI generează periodic semnale de sondare și le aplică la portul 5 al RC. Răspunsul RC la aceste semnale este achiziționat de CADI de la portul 6 și este analizat pentru a detecta eventualele diferențe față de valorile de referință. Valorile de referință se stabilesc prin măsurători la momentul fabricării unui modul format din ansamblurile A și B. Modul de proiectare a RC determină o anumită caracteristică de transfer (amplitudine și fază funcție de frecvență) a acesteia. Efectuarea unei intruziuni modifică această caracteristică de transfer. CADI are rolul de a detecta aceste modificări. Semnalele de sondare pot fi semnale sinusoidale, pot fi impulsuri, trenuri de impulsuri sau semnale cu caracteristici specifice în amplitudine, timp și frecvență. Parametrii semnalelor de sondare sunt determinați punctual în etapa de proiectare a ansamblurilor A și B, funcție de dimensiunile și geometria RC, pentru asigurarea unei sensibilități corespunzătoare de măsurare a CADI. Tipul de semnal utilizat trebuie să pună în evidență modificările caracteristicii de transfer a RC.

Un modul format din ansamblurile A și B poate funcționa în cadrul unui echipament sau independent, caz în care poate avea funcții suplimentare (așa cum este prezentat în capitolul anterior).

Pentru a asigura protecția permanentă a CES, CADI trebuie să funcționeze și pe duratele când echipamentul, în care este instalat CES, nu este alimentat de la o

sursă de energie. În acest scop, modulul format din CES și CADI dispune de o sursă de energie de rezervă, internă sau externă, sub forma unei baterii sau acumulator. În figura 2 este reprezentată această sursă de energie sub forma bateriei 9, instalată în interiorul ansamblului B.

În mod uzual, datele de securitate sunt stocate într-o memorie RAM nevolatilă, componenta 10 a ansamblului B. Alimentarea acestei memorii este asigurată de CADI, având ca sursă de energie bateria 9. În cazul în care CADI detectează o intruziune, întrerupe alimentarea memoriei nevolatile 10, determinând astfel pierderea informației stocate în aceasta. Memoria RAM nevolatilă poate fi parte componentă a CES sau CADI, sau poate fi un circuit dedicat, așa cum este prezentat în figura 2.

CES comunică cu echipamentul în care este instalat (sau cu alte dispozitive în cazul în care funcționează independent) prin intermediul unei magistrale de date 14 (figura 2).

Alimentarea cu energie se realizează prin intermediul portului de alimentare, reprezentat în figura 2 prin conexiunile 12 (GND - masă) și 13 (VCC – tensiune de alimentare). Funcție de natura aplicației, acest port poate avea mai multe tensiuni de alimentare, de curent continuu sau alternativ, sau poate utiliza orice metodă de transfer de energie electrică.

Rețeaua conductivă împreună cu modul de utilizare a acesteia, prezentate în această invenție, pot fi utilizate în protejarea împotriva intruziunilor fizice a circuitelor electronice de securitate, precum: module criptografice, dispozitive de plată electronică și alte circuite electronice care implementează funcții de securitate. De asemenea, această invenție poate fi utilizată pentru protejarea dreptului de proprietate asupra aplicațiilor informatice implementate în echipamente electronice.

REVENDICĂRI

1. Rețea conductivă, destinată protecției împotriva intruziunilor fizice asupra circuitelor electronice de securitate, alcătuită din trei trei straturi cu trasee conductive, izolate cu straturi dielectrice, caracterizată prin aceea că primul strat, situat spre circuitele protejate, este format dintr-o suprafață conductivă (1) ce acoperă întreaga suprafață a rețelei conductive, cel de-al doilea strat, situat deasupra primului strat, este realizat din trasee conductive (2) foarte subțiri, cu spații foarte mici între trasee, ce formează un circuit conductiv prevăzut cu un port de intrare (5) și un port de ieșire (6), cel de-al treilea strat situat deasupra stratului format de traseul (2) și expus la exterior, conține multiple trasee conductive (precum 3 și 4).
2. Rețea conductivă conform revendicării 1, caracterizată prin aceea că traseele conductive de pe stratul al treilea au aceleași dimensiuni și același model ca cele ale traseului (2) și, de asemenea, se suprapun exact peste traseul (2).
3. Rețea conductivă conform revendicărilor 1 și 2, caracterizată prin aceea că traseele conductive de pe stratul al treilea (precum 3 și 4) sunt organizate pe zone , traseele corespunzătoare acestor zone formează circuite închise.
4. Circuit activ de detecție a intruziunilor (8) conectat prin porturile (5) și (6) la rețeaua conductivă conform revendicării 1, caracterizat prin aceea că asigură, împreună cu rețeaua conductivă, funcția de protecție a circuitelor electronice de securitate.
5. Rețea conductivă conform revendicării 1, caracterizată prin aceea că acoperă în totalitate circuitele protejate, circuitul electronic de securitate (11) și circuitul activ de detecție a intruziunilor (8), fără a lăsa fante sau orificii care să permită observarea acestor circuite din exterior.
6. Circuit activ de detecție a intruziunilor (8) conform revendicării 4, caracterizat prin aceea că verifică periodic integritatea rețelei conductive prin aplicarea unor semnale la portul de intrare (5) și analizează răspunsul rețelei conductive la portul de ieșire (6), corespunzătoare traseului conductiv (2) de pe stratul al doilea.
7. Circuit activ de detecție a intruziunilor conform revendicărilor 4 și 6, caracterizat prin aceea că în cazul în care răspunsul rețelei conductive la

semnalele de sondare este diferit de valoarile de referință, acesta stabilește evenimentul de intruziune.

8. Circuit activ de detecție a intruziunilor conform revendicării 7, caracterizat prin aceea că în cazul unei intruziuni, acesta acționează în sensul protejării datelor de securitate prin ștergerea sau suprascrierea lor (zeroizare), iar în situația în care datele de securitate sunt stocate într-o memorie RAM nevolatilă, atunci circuitul activ de detecție a intruziunilor întrerupe alimentarea acesteia.
9. Circuit activ de detecție a intruziunilor conform revendicărilor 4 și 6, caracterizat prin aceea că semnalele utilizate de acesta la sondarea rețelei conductive pune în evidență modificările caracteristicii de transfer a rețelei conductive în caz de intruziune fizică.
10. Circuit activ de detecție a intruziunilor conform revendicărilor 4 și 6, caracterizat prin aceea că valorile de referință utilizate în sondarea rețelei conductive se stabilesc prin măsurători la momentul fabricării modulului format din rețeaua conductivă și circuitul activ de detecție a intruziunilor.
11. Circuit activ de detecție a intruziunilor conform revendicărilor 4 și 6, caracterizat prin aceea că pentru asigurarea neîntreruptă a funcției de protecție împotriva intruziunilor fizice asupra circuitului electronic de securitate, acesta este prevăzut cu o sursă de energie de rezervă sub forma unei baterii sau acumulator.

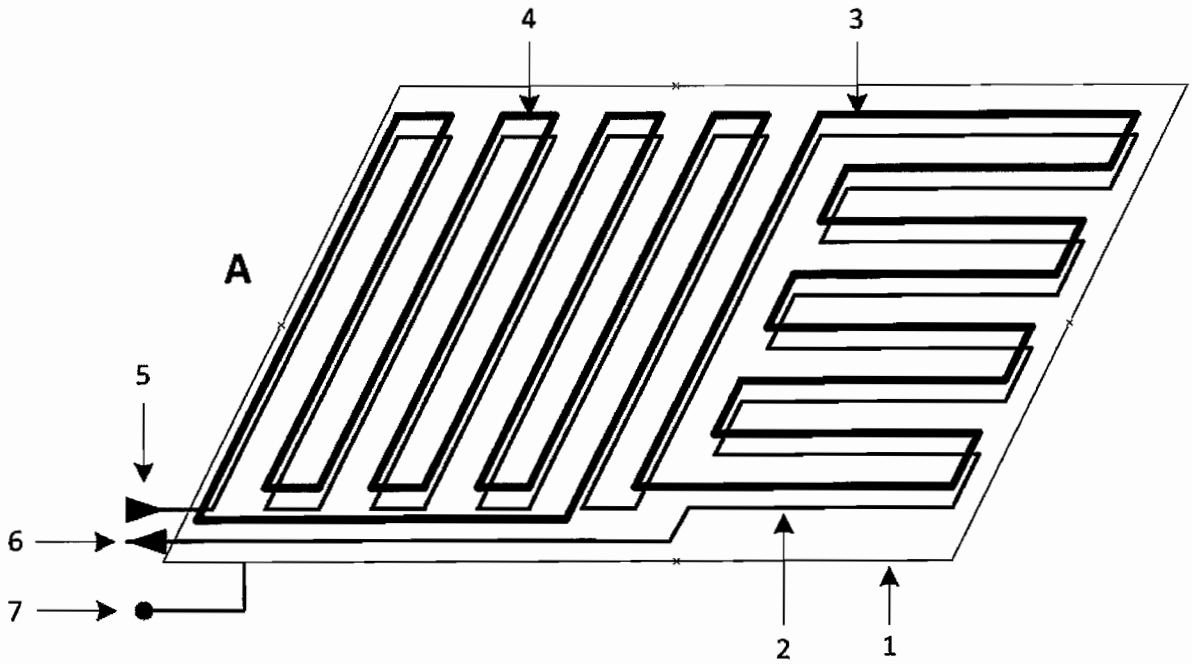

Fig. 1

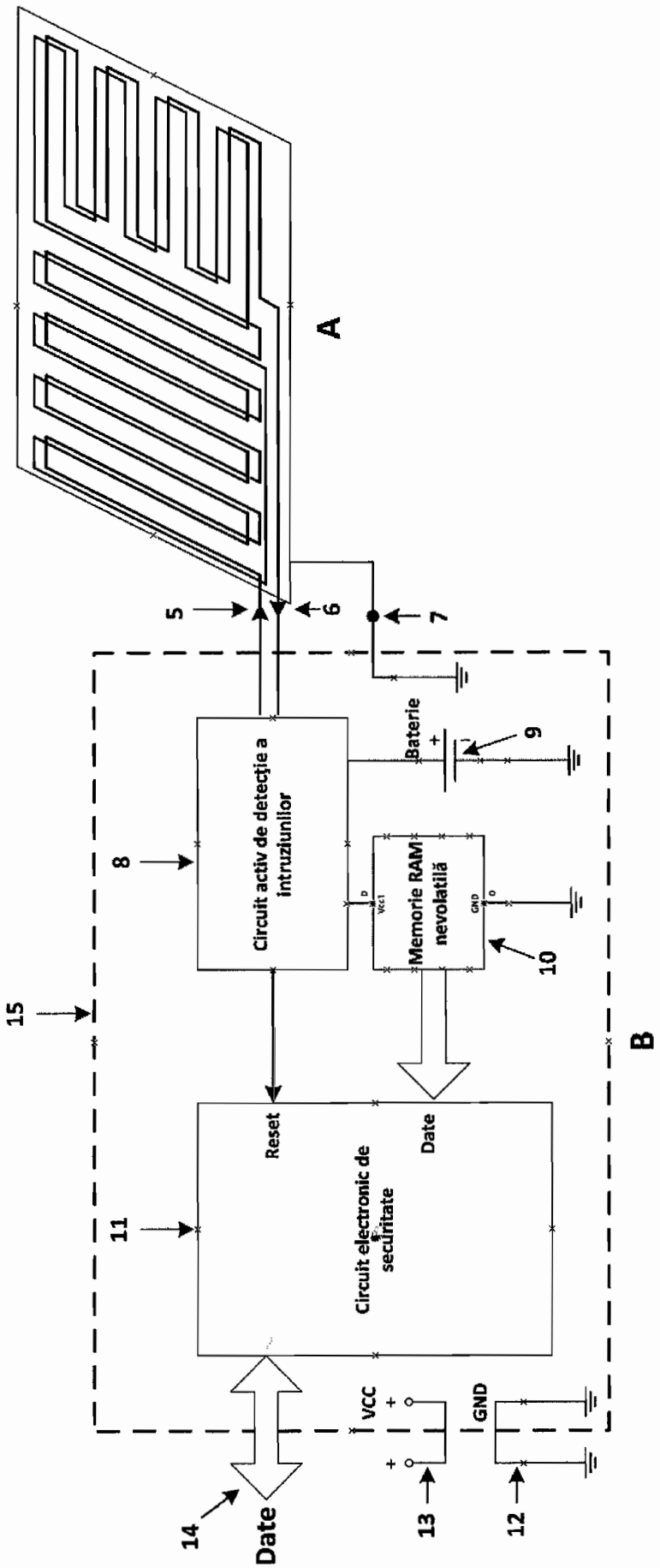
A
5
6
7
Baterie
9
8
Circuit activ de detecţie a intruziunilor
Memorie RAM nevolatilă
10
15
B
Reset
Date
Circuit electronic de securitate
11
VCC
GND
14
Date
13
12

Fig. 2