SISTEM DE ALARMĂ PENTRU AUTOMOBIL CU IMUNITATE LA FACTORII DESTABILATORI

Maxim BATÎR[1*]
Eugeniu MORARU[1]

[1]*Universitatea Tehnică a Moldovei, Facultatea Electronică și Telecomunicații, Departamentul TSE, gr. SSET-171*

[*]Autorul corespondent: Batîr Maxim, maxim.batir@sde.utm.md

Rezumat. *Aplicarea sistemelor de alarmă devine un imperativ la momentul actual şi se implementează pe larg în toate domeniile, inclusiv şi în automobile, unde ele devin un comonent standard de dotare. O problemă acută devine fiabilitatea şi imunitatea acestor sisteme la influienţa perturbaţiilor electromagnetice şi a intervenţiei vandalice de tipul „factor uman", unde ele trebuie să-şi îndeplinească funcţiile sale în cazurile defectării parţiale a componentelor sistemului şi să declanşeze alarma mod garantat în situaţiile critice. În lucrarea dată sunt analizate modurile de soluţionare ale acestor probleme la nivel de structură şi algoritmi de funcţionare a sistemelor de alarmă pentru automobil.*

Cuvinte cheie: *sistem de alarmă, senzor, rezervarea alimentării, canal de legătură, perturbaţie electromagnetică, dublarea liniilor de comandă.*

Introducere

Sistemele de alarmă pentru automobile existente conţin un service multifuncţional avansat ce permite de redus considerabil riscul de furt sau răpire al acestuia. Face de menţionat că o parte considerabilă a acestor sisteme sunt insificient protejate de acţinnea vandalilor cu experienţă, a perturbaţiilor electromagnetice naturale şi artificiale în canalele de comunicaţii [1]. Alt factor negativ este lipsa dublării liniilor de legătură şi canalelor de telecomunicare pentru situaţiile defectării liniilor canalelor de telecomunicare de bază, tot aici se atribuie şi rezervarea alimentării sistemului de alarmă. Funcţiile de comandă şi blocarea unor componente sistemului de bord al automobilului în majoritatea cazurilor sunt realizate în variantă de program cu algoritm fixat şi o parte din asemenea sisteme le permit de activat prin canal de telecomunicaţii.

O problemă importantă este, ca sistemul de alarmă şi pază să fi capabil să asigure o contraacţiune activă la tentativele de blocare artificială a senzorilor de alarmă pe care le întreprinde răufăcătorul în procesul de pătrunderii nesancţionate în salonul automobilului. E firesc că în procesul pătrnderii nesancţionate în interiorul automobilului o parte de componente al sistemului de alarmă sunt deteriorate, ce reduc probabilitatea activării alarmei şi blocarea unor componente sistemului de bord al automobilului.

Pentru diminuarea problemelor menţionate în această lucrare se propune o serie de soluţii ce ţin de structura (arhitectura) HARD-ului şi algoritmi de funcţionare, care tradiţional sunt realizate cu miloace SOFT, ce prevăd dublarea componentelor de comandă, a linilor şi canalelor de telecomunicaţii şi alimentării sistemului de alarmă. Tot aici sunt analizate măsurile de sporire a fiabilităţii şi procedeele de protecţie al sistemului de alarmă împotriva acţiunilor vandalice din partea răufăcătorilor. O trăsătură caracteristică acestei lucrări este ca structura sistemului de alarmă propus să fie autonomă faţă de sistemul de bord al automobilului, care să asigure o încoporare simplă şi rapidă în automobil de orice model cu intervenţie minimală în sistemul electric şi electronic al acestuia.

1. Problemele soluţionate

În afara realizării funcţiilor de bază a sistemelor de alarmă [2,3,4] este necesar de asigurat măsuri suplimentare de protejare fizică a HARD-ului de factorii climaterici, mecanici, electromagnetici de provenenţă naturală şi artificială care pot deregla funcţionarea

normală sistemului de alarmă sau defectarea lui. Factorii menţionaţi indică necesitatea de asigurare a următoarelor măsuri pentru protejarea echipamentului sistemului:

1) De asigurat măsuri pentru o fiabilitate mai înaltă.

2) Dublarea componentelor principale ale sistemului de alarmă ce sunt afectate în primul rând în procesul accesului nesancţionat în automobil.

3) Dublarea canalelor de comunicare pentru translarea alarmei şi legăturii bidirecţionare la distanţă.

4) Dublarea alimentării a componentelor sistemului pentru situaţiile de activare a alarmei şi diversie vandalică de tipul „factor uman".

5) Algoritmul de funcţionare al sistemului de alarmă trebuie să asigure o imunitate împotriva factorilor externi destabilizatori şi să excludă activarea alarmei false.

Măsurile de protejare menţionate duc la mărirea redundanţei sistemului de alarmă, unde e necesar de soluţionat în complex probleme contradictorii, pe de o parte de extins lista funcţiilor executate şi de perfecţionat fiabilitea sistemului în întregime, pe de altă parte de redus costul şi gabaritele fără afectarea funcţionalităţii sistemului de alarmă.

2. Modurile de soluţionare a problemei

Măsurile pemtru mărirea fiabilităţii prevăd utilizarea radiocomponentelor şi a materialelor elecrice de uz industrial, în sectoarele cele mai importante de aplicat componente de uz militar. Altă măsură de sporire a fiabilităţii este alegerea regimului de lucru optimal a componentelor electronice şi rezervarea a porţiunilor critice ale sistemului:

1) Utilizarea regimului electric mai puţin încărcat, de exemplu 10...30% din puterea maximă admisă;

2) Utilizarea rezervări reci, ce presupune prezenţa a unui bloc-componentă de rezervă în stare iniţială deconectată, unde el se conectează în sistem automat înlocuind blocul-componentă de lucru pentru situaţia depistării defectului în blocul de lucru. Decizia de recomutare a blocului defectat cu cel lucrător este luată de blocul principal al sistemului de alarmă;

3) Utilizarea rezervării fierbinţi, unde blocul-componentă de rezervă se află sub tensiunea de lucru şi se recomutează automat la depistarea defectului în blocul-componentă de lucru.

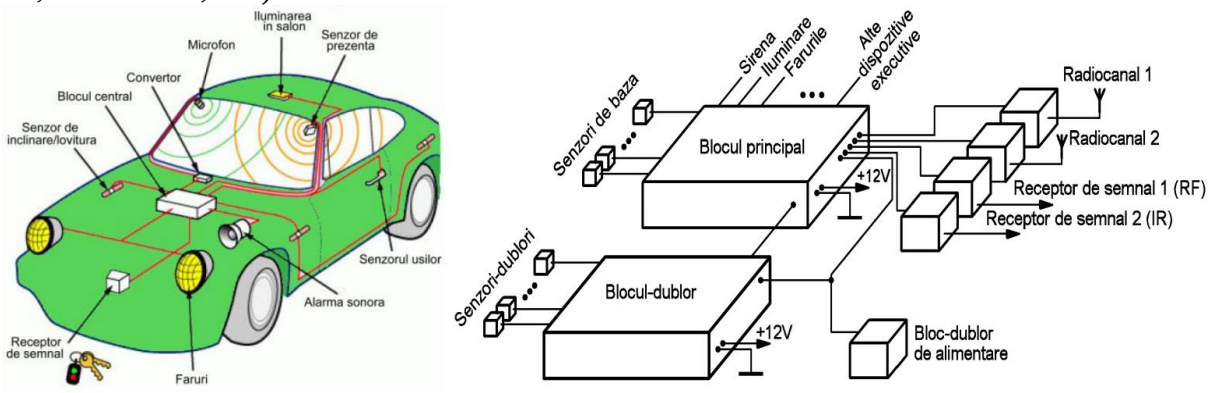
Dublarea componentelor în porţiunile vulnerabile al sistemului de alarmă permite de obţinut o eficienţă mai înaltă, însă duce la mărirea costului sistemului în întregime. Acestă complicare a HARD-ului este justificată pentru situaţia dată, deoarece defectul apare nu din cauza factorului natural spontan ci din cauza factorului uman intenţionat. Tot aici se referă şi dublarea canalelor de telecomunicaţie şi legăturii bidirecţionale la distanţă, ele de obicei sunt primele componente sistemului de alarmă ce sunt supuse atacului din exterior pentru înăbuşire. După atacul de înăbuşire a canalelor de telecomunicaţii urmează atacul asupra componentelor cu senzori de control al accesului şi dispozitivele de activarea alarmei, tradiţional e sirena acustică, farurile, semnalul de alarmă transmis prin canale de telecomunicaţii (GSM, GPS, prin satelit, etc.). Corespunzător ultimul atac al răufăcătorului este ocolirea sau spargerea componentelor blocării sistemului de bord al automobilului: sistemul de alimentare şi aprindere al motorului, sistemul hidraulic al volanului şi frânei, cutia de viteze, etc. [5,6]

În proces de acces nesancţionat în automobil pentru răufăcător este foarte important în primul rând fie deconectată alimentarea sistemului de alarmă sau deactivarea alarmei prin canalele standarde al sistemului de alarmă. Pentru asigurarea contraacţiunii împotriva deconectării alimentării se recurge la instalarea a unui acumulator de rezervă [7] şi bloc de monitoring, încărcare şi comutare în locurile greu accesibile ale automobilului, unde timpul accesului va dura nu mai puţin de 10-15 minute.

Implementarea măsurilor menţionate mai sus impune restricţii asupra algoritmului de funcţionare a părţii SOFT al acestui sistemde alarmă: excluderea alarmelor false; imunitate la perturbaţii (interferenţe) electomagnetice; imunitate criptografică împotriva acaparării codului de acces transmis şi recepţionat prin canale deschise de cumunicaţii.

3. Modurile de implementare

În configuraţia standardă al sistemului de alarmă se includ componentele pentru dublare necesare (Fig. 1a). Este preferabil de inclus şi senzori pentru funcţii suplimentare: controlul apropierii şi prezenţei, controlul spargerii sticlei (uşile, parbrizul şi sticla din spate), scanarea volumuli salonui cu unde de radiofrecvenţă (RF) şi raze infraroşii (IR), de extins componenţa dispozitivelor de acces şi control la panoul de comandă al sistemului de alarmă (pult cu raze IR, jeton RFID, tastatură secretă, dispozitiv de citire a ampentei degetului, etc.) ce pot interacţiona în complex (Fig. 1b). Ca funcţii suplimentare mai avansate poate fi inclusă fixarea şi transmiterea imaginii şi sunetului prin canale de telecomunicaţii, activarea semnalizatorului radio (prin satelit, GSM, GPS/GPRS, etc.).



a) **b)**

Figura 1. Structura şi componenţa sistemului de alarmă pentru automobil.

Protecţia împotriva accesului nesancţionat din exterior al automobilului este insuficientă, un pericol deosebit prezintă răpirea automobilului când sistemull de alarmă este deactivat şi proprietarul automobilului este ameninţat cu arma sau prin şiretlic să părăsească salonul automobilului în regimul motorului pornit. Pentru excluderea acestor situaţii în sistemul de alarmă este obligatoriu să fie încorporată funcţia Anti-HiJack, unde alarma este activată prin acţiuni ascunse pentru răpitor (formarea codului secret pe pult sau tastatură ascunsă, apasarea tastei secrete în loc ascuns al salonului, instrucţiune SMS specială expediată prin GSM, etc.). Pentru prevenirea furtului elementelor exterioare ale automobilului (ştergătoarele de parbriz, roţile, capacele decorative de protecţie a roţilor, etc.) este binevenit ca sistemul de alarmă să fie dotat cu senzori pe prezenţă şi înclinare/lovitură, cu ajutorul senzorilor suplimentari pot fi depistate şi alte acţiuni de intervenţie nesancţionată: instalarea obiectelor străine pe automobil, spargerea avinelopelor sau evacuarea nesancţionată cu transport special.

Concluzii

Ca rezultat a fost obţinut un concept a structurii sistemului de alarmă ce permite de realizat soluţionarea problemelor menţionate mai sus ce permite de obţinut următoarele performanţe funcţionale:

1) Utilizarea radiocomponentelor de uz industrial şi militar în sectoarele vulnerabile a sistemului de alarmă permite de asigurat fiabilitate suficientă pentru condiţiile mai dure de exploatare;

2) Rezervarea componentelor importante a sistemului permite de mărit fiabilitatea sistemului de alarmă şi imunitate la acţiunile vandalice de tipul „factor uman” şi activarea garantată a alamei pentru situaţii de acces nesancţionat în salonul automobilului;

3) Dublarea liniilor de legătură a componentelor sistemului şi a canalelor de telecomunicare permite de redus considerabil influenţa perturbaţiilor electromagnetice de provenenţă naturală şi în deosebit de cea artificială, scopul ultimei este neutralizarea transmiterii semnalului de alarmă;

4) Utilizarea rezervării alimentării sistemului de alarmă şi amplasarea lui în locurile greu accesibile ale automobilului permite de exclus neutralizarea rapidă a sistemului de alarmă, ce permite în mod garantat de activat regimul de alarmă şi de transmis semnalul şi mesajele de alarmă prin canalele de telecomunicaţie până la deactivarea, deconectarea şi deteriorarea sistemului în procesul pătrunderii nesancţionate în automobil;

5) Includerea funcţiilor asemănătoare intelectului artificial în algoritmul de funcţionare a părţii SOFT permite de analizat sitauţia curentă cu scopul de a exclude alarmă falsă, să asigure declaşare garantată a alarmei în situaţiile de acces nesancţionat real şi să fixeze tentativele de încercare a pătrunderii nesancţionate în salonul sau portbagajul automobilului. Tot aici se poate de menţionat că realizarea funcţiei Anti-HiJack este posibilă cu suport minimal HARD al sistemului de alarmă.

În afară de avantajele obţinute în soluţionarea problemei se conţin şi unele neajunsuri:

1) Se obţine o redundanţă suplimentară a părţii HARD ce duce la scăderea fiabilităţii, măririi gabaritelor sistemului şi complicarea tehnologiei de încorporare în sistemul de bord al automobilului;

2) Partea SOFT al sistemului de alarmă devine mai complicată şi voluminoasă care necesită anumite resurse ale microprocesorului sau microcontrolorului ce stă la baza sistemului de alarmă;

3) Necesită module şi algoritme speciale pentru protecţia criptografică a datelor transmise şi recepţionate prin canalele de telecomunicaţii.

Neajunsurile menţionate pot înlăturate prin utilizarea microcircuitelor specializate şi produselor SOFT mai performante.

Referinţe

1. АВРАМЧУК А.И. ПРИМЕНЕНИЕ GSM-КАНАЛА В СИСТЕМАХ ОХРАНЫ (БЕСПРОВОДНЫЕ СИГНАЛИЗАЦИИ GSM). [online]. [accesat 10.02.2021]. Disponibil: https://starsb.ru/primeneniye-gsm-kanala-v-sistemakh-okhrany-gsm-signalizatsii
2. Устройство и принцип работы автомобильной сигнализации. [online]. [accesat 10.02.2021]. Disponibil: https://techautoport.ru/elektrooborudovanie-i-elektronika/protivougonnaya-sistema/avtomobilnaya-signalizaciya.html
3. Автомобильная охранная система с 2-сторонней связью и дистанционным запуском двигателя Alligator C-3C. Инструкция по эксплуатации и установке. [online]. [accesat 10.02.2021]. Disponibil: https://www.fotosklad.ru/upload/iblock/e20/e20a06c9a5e586eebb1a22069270b61b.pdf
4. Бирюкова О.В. ЭЛЕКТРОННЫЕ СИСТЕМЫ СИГНАЛИЗАЦИИ. Электронный учебник. Рязань. Рязанский колледж электроники. 2015. [accesat 10.02.2021].
5. Борщенко Я.А., Васильев В.И. Электронные и микропроцессорные системы автомобилей: Учебное пособие. - Курган: Изд-во Курганского гос. ун-та, 2007.- 207 с.
6. Коваленко, О.Л. Электронные системы автомобилей: учебное пособие / О.Л. Коваленко; Сев. (Арктич.) федер. ун-т им. М.В. Ломоносова. - Архангельск: ИПЦ САФУ, 2013. - 80 с.: ил. ISBN 978-5-261-00762-3
7. Химические источники тока. Справочник / Под редакцией Н. В. Коровина, и А.М. Скундина. – М. Издательство МЭИ, 2003. – 740с., с ил.