CONCEPTUL ŞI MODELUL TEORETIC AL SISTEMULUI INTEGRAT DE PROTECȚIE A INFRASTRUCTURILOR CRITICE

THE CONCEPT AND THEORETICAL MODEL OF INTEGRATED SYSTEM FOR THE PROTECTION OF CRITICAL INFRASTRUCTURE

Colonel (r) prof. univ. dr. Benone ANDRONIC*
Doctorand Cristian ILIE

Conceptul de protecție, la fel ca cel de securitate, constituie o problemă ştiințifică, dar şi practică şi de aceea acesta ar trebui să fie realizat într-o strânsă colaborare cu beneficiarul, cu analize şi testări complexe, pe etape şi apoi în stadiul final.

De fapt, datorită complexității securității şi protecției infrastructurilor critice se impune elaborarea unui nou concept de protecție care să integreze problemele de calitate şi de securitate a acestora, şi care să fie capabil să contracareze producerea evenimentelor nefericite şi să asigure restabilirea cât mai rapidă a integralității lor.

***Cuvinte cheie**: infrastructură critică; culegere de informații; matrice de risc; risc asumat; strategii de protecție; sistem de protecție integrat.*

Te concept of protection, as the security, is a scientific and practical matter and therefor it should be done in close collaboration with beneficiary, whith complex analysis on stages an testing in final phases.

In fact the complexity of security and critical infrastructure protection us necessary to develop a new concept of protection that which integrates the securiy an quality issues and to be able to counterct the unfortunate event production and ensure swift restoration of their completeness.

***Keywords:** critical infrastructure; intelligence; risk matrix; risk assumed; protection strategies; integrated protection system.*

* Profesor universitar asociat la Universitatea Națională de Apărare „Carol I”,email:benoneandronic@yahoo.com

În accepţiunea noastră sistemele integrate de protecţie a infrastructurilor critice ar putea fi cele de comandă şi control (C4I2SR)* care au ca funcţii de bază culegerea de informaţii, transmiterea şi procesarea acestora, asistarea actului de decizie şi asigurarea de mijloace pentru protecţie, securitate şi apărare.

Cele două axiome în analiza acestui domeniu ar putea fi următoarele: imposibilitatea asigurării în proporţie de 100% a protecţiei infrastructurii critice (PIC) oricare ar fi aceasta; inexistenţa[1] unei soluţii unice, a unui sistem universal pentru asigurarea PIC.

Punerea în practică a conceptului de protecţie a infrastructurilor critice ar trebui să impună implementarea sistemului de PIC în conformitate cu prevederile de securitate, precum şi evaluarea, proiectarea şi punerea în aplicare a mecanismelor integrate de protecţie (măsuri constructive şi de dotări; măsuri organizatorice şi procedurale; măsuri de resurse umane şi personal).

Sistemul de protecţie a infrastructurilor critice ar putea cuprinde următoarele mecanisme: protecţia perimetrului şi bariere fizice a acestora; controlul viabil al accesului; detecţia oricărei tentative de efracţie; supravegherea prin televiziune cu circuit închis; sistem informaţional; centre de control principale şi secundare; electroalimentare.[2]

În opinia noastră orice sistem de protecţie integrat este un ansamblu de măsuri umane, tehnice şi procedurale, pentru realizarea descurajării, întârzierii, detecţiei, evaluării şi intervenţiei împotriva încercărilor de pătrundere neautorizată în perimetrul infrastructurii critice. S-a constatat că măsurile de protecţie exclusiv umane sunt neeficace şi ineficiente şi nu pot asigura păstrarea integrităţii împrejmuirilor perimetrului infrastructurii.[3]

S-au elaborat liste care s-au analizat şi actualizat periodic referitoare la problemele ce apar în proiectarea şi realizarea sistemelor integrate de protecţie a infrastructurilor critice. Unele dificultăţi care sunt de actualitate şi care au o influenţă majoră asupra performanţelor sistemului de protecţie sunt: necunoaşterea exactă a tuturor datelor ce caracterizează ameninţarea (disponibilitate, „amprente" specifice, parametrii evolutivi, potenţial distructiv etc.), ceea ce are implicaţii directe asupra modului de stabilire a unor caracteristici tehnice şi operaţionale: (dimensiunile ariei de supraveghere, tipul senzorilor utilizaţi, rezoluţii unghiulare şi în distanţă etc.), estimarea cu dificultate a caracteristicilor resurselor utilizate pentru combaterea ameninţării: (tip de contraacţiune, efective, timp de reacţie în funcţie de dispunere, mijloace de deplasare etc.), mijloace de lovire (non-letale sau letale); necesitatea aprecierii cât mai exacte a condiţiilor de mediu generale şi specifice unei anumite locaţii în

---

* Comandă, control, comunicaţii, computere, informaţii, intelligence, supraveghere, recunoaştere.

[1] Georgică Slămnoiu, *Model teoretic funcţional de sistem integrat de protecţie a infrastructurilor critice,* Sesiunea anuală de comunicări ştiinţifice cu participare internaţională „Perspective ale securităţii şi apărării în Europa", 19-20 noiembrie 2009, Bucureşti, Volumul V, Editura Universităţii de Apărare „Carol I", p. 69.

[2] Ibidem.

[3] Georgică Slămnoiu, *Aspecte generale ale conceptului de sistem integrat de protecţie a infrastructurilor critice,* Sesiunea anuală de comunicări ştiinţifice cu participare internaţională „Perspective ale securităţii şi apărării în Europa", 19-20 noiembrie 2009, Bucureşti, Volumul V, Editura Universităţii de Apărare „Carol I", p. 58.

vederea stabilirii tipului de senzori utilizaţi, performanţelor de detecţie, necesitatea folosirii unor sisteme redundante etc.; necesitatea automatizării proceselor de supraveghere, detecţie, urmărire şi identificare în funcţie de caracterul permanent al activităţii şi de importanţa ei.

Definirea conceptului de sistem integrat de protecţie a infrastructurilor critice

Ca o caracteristică de calitate a infrastructurilor critice protecţia acestora se poate defini ca o capacitate a sistemului de conservare a caracteristicilor sale funcţionale sub presiunea unor acţiuni distructive care l-ar putea transforma în pericol pentru mediul înconjurător, ar afecta viaţa oamenilor aflaţi în zona de risc sau ar provoca pagube materiale, informaţionale etc.

Considerăm că se poate adopta conceptul de protecţie deplină deoarece reuneşte atributele de complexitate şi responsabilitate, aduce rezolvări echilibrate la atacuri şi accidente, şi îndeplineşte condiţiile impuse de legi, norme sau standarde. Protecţia deplină reprezintă calitatea definitorie de înmănunchiere conceptuală a tuturor aspectelor juridice, organizatorice, informaţionale, fizice şi umane, în medii calitative diverse, cu mecanisme viabile, adaptive şi perfecţionabile, apte să reziste şi/sau să riposteze la o gamă largă de atacuri, accidente etc., abordate previzionar înainte, în timpul desfăşurării şi după încetarea acestora, pe baza asumării conştiente a riscului operaţional şi unor costuri suportabile.[4]

Managementul protecţiei

Managementul riscului conţine o serie de activităţi, bine definite, organizate şi executate, care în funcţie de condiţiile de existenţă şi obiectivele fundamentale ale organizaţiei analizează, pe baza concepţiei de protecţie, toţi factorii de risc în scopul minimizării riscului asumat şi costurilor aferente.

În literatura de specialitate sunt consemnate unele metode precum: metoda interdependenţelor funcţionale şi metoda matricelor de risc.

Pentru aplicarea primei metode se începe cu analiza factorilor controlabili (structura organizatorică, personalul angajat, strategia de protecţie adoptată, sistemele de protecţie utilizate şi procedurile aplicate), dar şi a celor necontrolabili (erori de sistem, acţiuni teroriste, catastrofe naturale şi altele). Această metodă foloseşte interdependenţa ierarhică de evenimente pozitive ce sunt în relaţii fie de tip „sau logic" fie „şi logic", ceea ce permite clarificarea ameninţărilor, măsurilor şi contramăsurilor.[5]

Componentele principale ale metodei matricelor de risc sunt: aria protejată, ameninţările probabile şi nivelul de risc.

În vederea construirii matricei de risc se stabilesc ariile protejate şi zonele vitale; se estimează consecinţele în cazul atacurilor reuşite şi se calculează valoarea riscului asumat prin însumare ponderată a valorilor estimate. Pentru definirea zonelor vitale de protecţie se

---

[4] Eugen Siteanu, Ilie Gheorghe, *Fiabilitatea produselor tehnice,* Editura AISTEDA, Bucureşti, 2001, p. 27.
[5] Georgică Slămnoiu, *Op.cit.*, p. 59.

foloseşte metoda „arborilor de defectări" care constă în analiza preliminară a ameninţărilor, stabilirea obiectivelor ameninţate şi definirea zonei vitale.

Metoda matricei de risc, prin aplicarea la obiectivul propus, permite obţinerea unor valori pentru „riscul asumat" care se compară cu conceptul atitudinii faţă de risc (acceptabil, atitudine selectivă, inacceptabil) şi determină toleranţa selectivă (măsurile de prevenire şi atenuare a efectelor) şi neacceptabilitatea (măsurile de asigurare pentru cazurile de materializare a riscurilor maxime).[6]

Prin analiza caracteristicilor obiectivului se pun în evidenţă: caracteristici fizice (zona amplasării; zona extinderii imediate; perimetrul amplasamentului; zona interioară imediată; zona spaţiului funcţional; zona spaţiului interior); caracteristici funcţionale (caracteristicile activităţii obiectivului; categoria şi caracteristicile echipamentului; vectori de transport); caracteristici informaţionale (cadrul informaţional; nivel informatizare; flux informaţional; reţele de calculatoare suport; securitatea fizică a informaţiei); caracteristici de personal (tipuri de potenţial infractor estimat; tipul relaţiilor cu instituţii similare; caracteristicile personalului propriu).

Managementul riscului reprezintă în esenţă „teoria", iar căile de reducere a riscurilor identificate aparţin managementului protecţiei, adică „practicii". Din punct de vedere structural, acesta presupune un complex de măsuri organizatorice, fizicotehnologice şi informaţionale capabile să preîntâmpine acţiunea factorilor distructivi pentru a le diminua sau anihila consecinţele.[7]

Conform prevederilor legale, în raport de riscul şi costurile asumate de organizaţie, strategiile de protecţie a infrastructurilor critice au următoarele niveluri: minimală, risc asumat de circa (12-15)%; suficienţă, risc asumat de circa (8-12)%; acoperitoare, risc asumat de circa (5-8)%; sigură, risc asumat de circa (3-5)%.[8]

După gradul de acoperire a domeniului de activitate a organizaţiei (firmei) responsabile de PIC. strategiile pot fi de două categorii: globale (omogene sau ierarhice) sau parţiale.

Dar costurile strategiilor globale sunt foarte mari, iar modul de realizare depinde de importanţa funcţională a componentei protejate în sistem şi de nivelurile de risc acceptate.

Conceptul de sistem integrat de protecţie

Din cauza implicaţiilor sociale ale obiectivelor industriale tehnologiei şi proceselor de timp real, colectivelor umane integrate, realizărilor arhitectonice precum şi elementelor de mare influenţă ecologică, protecţia acestora, ca element principal de calitate tehnologică şi socială, reprezintă o condiţie fundamentală de eficienţă economică. Dar despre eficienţă economică se poate vorbi numai în condiţiile în care procesele industriale se desfăşoară în siguranţă şi securitate, fără dezastre ecologice, având în vedere că în vizorul terorismului

[6] Ilie Gheorghe, *De la managementul riscului la guvernarea prin risc,* Editura UTIPress, Bucureşti, 2009, p.25.
[7] Georgică Slămnoiu, *Op.cit.*, p. 60.
[8] Ibidem, p. 61.

internaţional sunt şi aceste capacităţi (coroborate cu aspectele concurenţei neloiale). De aceea e necesar un concept de protecţie ştiinţific şi implementarea mecanismelor ce se impun pentru asigurarea calităţii şi contracararea unor evenimente nedorite, periculoase (acte de terorism, sabotaje, furturi, cutremure, inundaţii, explozii, emisii de noxe sau poluări etc.).

În figura 1 sunt prezentate schematic elementele principale şi conexiunile lor cu protecţia şi eficienţa economică a organizaţiilor şi firmelor (întreprinderilor), respectiv a PIC.

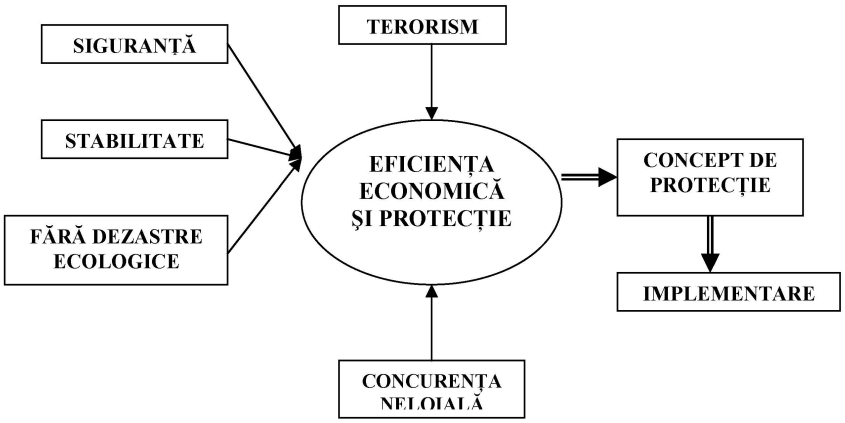

Figura nr.1. *Necesitatea conceptului de protecţie pentru infrastructurile critice*

Analizând ansamblul ameninţărilor generale (acte de terorism, sabotaj, disimulări informaţionale, accidente tehnologice şi de producţie etc.), şi ţinând seama de caracteristicile capacităţilor industriale, din punctul de vedere al protecţiei, acestea se pot clasifica conform tabelului nr. 1.

După procesul de producţie utilizat, capacităţile industriale se clasifică în următoarele clase: monoproces; multiproces; multiproces cu consecinţe de insecuritate cumulative.

Capacităţile industriale din clasele multiproces şi multiproces cu consecinţe de insecuritate cumulative sunt deosebit de sensibile şi se încadrează în clasele superioare de protecţie G, F şi E.

Din această clasificare reiese că problema protecţiei este complexă, cu măsuri fundamentale comune, dar şi cu altele diferenţiate pentru clase de capacităţi şi pentru capacităţi în sine.

Problemele de protecţie (securitate) ale acestor capacităţi sunt supuse întregii game de ameninţări (fizice, informaţionale, funcţional-tehnologice, organizatorice şi de personal),

cu menţiunea că raportul dintre ameninţările fizice şi cele funcţional-informaţionale îşi mută ponderea, tot mai mult, spre cele din urmă, ceea ce complică şi mai mult problema protecţiei.

Tipul capacităţii industriale	Nivelul de risc	Clasa de protecţie	Exemple de capacităţi industriale
Impact social major	3,2-5	E, F, G	Capacităţi termo şi hidroelectrice, reţele de distribuţie electricitate, gaze şi produse petroliere, cu densitate tehnologică şi suprafaţă geografică mare
Consecinţe catastrofice			Capacităţi nucleare, chimice, armament şi materiale explozibile şi rafinării
Deosebit de sensibile	3,2-4,5	E, F	Capacităţi strategice, din punct de vedere tehnologic şi al produselor realizate
Supuse unor mari presiuni	3,2-4	E	Capacităţi de mare eficienţă economică şi în puternică concurenţă pe piaţă
Nivel de risc mediu	1,1-3,2	B, C, D	De mărime şi producţie mică sau medie

Tabelul nr. 1. *Clasificarea principalelor capacităţi industriale din punctul de vedere al protecţiei şi securităţii acestora*

Din lecţiile învăţate a reieşit dezvoltarea şi diversificarea mijloacelor şi procedeelor de atac asupra acestor capacităţi şi timpul practic suficient de lung la dispoziţia atacatorilor pentru a-şi pregăti acţiunile.

Datorită complexităţii securităţii şi protecţiei industriale şi noilor orientări teroriste, se impune elaborarea unui nou concept de protecţie care să integreze problemele de calitate şi de securitate a firmelor (aprovizionare, producţie, piaţă, relaţii de cercetare, bancare tec.), sociale, tehnologice, ecologice şi de protecţie fizică, informaţională, de personal, împotriva incendiilor şi catastrofelor naturale, şi care să fie capabil să contracareze producerea evenimentelor nefericite şi să asigure restabilirea cât mai rapidă a capacităţii de producţie.

Acest nou concept trebuie să asigure următoarele cerinţe: analiza ameninţărilor; estimarea vulnerabilităţilor şi riscurilor producerii evenimentelor nedorite şi a consecinţelor acestora; stabilirea clasei de protecţie a capacităţii şi a strategiei de protecţie, în funcţie de riscurile şi costurile probabile; definirea mediului de protecţie necesar păstrării capacităţii de producţie; definirea mediului de protecţie; realizarea, implementarea şi integrarea mecanismelor de protecţie într-un sistem eficace; constituirea structurii de protecţie pentru asigurarea stabilităţii dinamice a sistemului; evaluarea, testarea şi autorizarea sistemului de protecţie; stabilirea limitelor de deschidere şi de perfecţionare; alegerea ştiinţifică a

măsurilor de mentenanţă; definirea şi realizarea asigurării complexe (pagube, riscuri etc.) a capacităţii de producţie protejate.

Conceptul de protecţie, la fel ca cel de securitate, este o problemă ştiinţifică, dar şi practică şi de aceea el trebuie realizat într-o strânsă colaborare cu beneficiarul, cu analize şi testări complexe, pe etape şi apoi în stadiul final.

Mediul de protecţie a infrastructurilor critice ar trebui să asigure: protecţia mediului infrastructurilor critice; protecţia proceselor de producţie; protecţia calităţii; protecţia ecologică; confidenţialitatea tehnologică; protecţia fizică (perimetre, clădiri, linii tehnologice, capacităţi de conducere şi informaţionale, personal, bunuri); protecţia informaţiilor (inclusiv licenţe, mărci, reţete de fabricaţie); un cadru moral de educaţie şi comportament pentru protecţia şi securitatea întregului personal angajat (norme, angajamente de confidenţialitate, coduri deontologice); prevenirea şi stingerea incendiilor; protecţia împotriva catastrofelor naturale; cadrul juridic al desfăşurării activităţii structurii de protecţie; cadrul, resursele şi procedeele de înlăturare a consecinţelor producerii evenimentelor nedorite şi de restabilire a capacităţii de producţie.[9]

Orice sistem de protecţie a infrastructurilor critice trebuie să asigure: prevenirea şi descurajarea acţiunilor răuvoitoare; detecţia, cât mai devreme posibil, a acţiunilor răuvoitoare; întârzierea desfăşurării acţiunii răuvoitoare; stoparea acţiunii (prinderea şi neutralizarea răuvoitorilor înainte de a-şi finaliza acţiunea); micşorarea la minimum posibil a urmărilor unei acţiuni răuvoitoare reuşite; evidenţierea unui număr cât mai mare de indicii în vederea urmăririi şi prevenirii răufăcătorilor; siguranţa şi stabilitatea proceselor şi afacerilor; confidenţialitatea informaţiilor şi a proceselor de conducere; protecţia împotriva incendiilor şi a catastrofelor naturale; eliminarea sau atenuarea, cât mai mult posibil, a accidentelor tehnologice şi de muncă, precum şi a celor cu consecinţe ecologice.[10]

Pentru realizarea funcţionării optime a sistemelor de protecţie a infrastructurilor critice sunt necesare următoarele măsuri: proiectarea optimă a construcţiilor şi instalaţiilor; utilizarea celor mai performante tehnologii de supraveghere şi alarmare; măsuri organizatorice adecvate; realizarea unui sistem informatic eficace şi cu suport sigur.

Sistemul de protecţie trebuie să aibă la baza structurii sale datele provenite din analizele efectuate şi conceptul adoptat: strategia de protecţie; ameninţările, vulnerabilităţile, tratarea riscurilor de insecuritate; scopul acţiunilor teroriste sau inamice; atacurile credibile; zonele critice.

La proiectarea sistemelor de protecţie a infrastructurilor critice este necesar să se ţină cont şi de următoarele principii: sistemul de securitate se bazează pe o concepţie, pe o strategie aleasă şi pe o atentă analiză a costurilor şi eficienţei; el are un comportament adaptabil şi este deschis, dar este specific obiectivului pe care îl protejează; el are o structură mixtă (om - maşină) şi caracter cibernetic (cu autoreglare), cu învăţare în funcţie

[9] Ibidem, p. 63.
[10] Ibidem, p. 64.

de politicile de protecţie aplicate; „înghețarea" sistemului de protecţie şi neadaptarea lui înseamnă insecuritate; costurile mari ale protecţiei pot fi diminuate prin analize şi mecanisme adecvate şi compensate în oarecare măsură de siguranţa (protecţie) producţiei, satisfacţia beneficiarilor, siguranţa şi comportamentul personalului.

Mecanismul de protecţie e partea practică (pragmatică) a strategiei de protecţie având una din cele trei forme: 1) ansamblul de măsuri cu soluţii tehnice şi organizatorice parţiale; 2) mecanism de protecţie cu măsuri, echipamente şi personal organizatoric profesional; 3) sistemul de protecţie bazat pe teoria sistemelor şi pe funcţii de previziune şi adaptabilitate.

Spaţiul multidimensional în care se manifestă protecţia infrastructurilor critice faţă de condiţiile externe şi faţă de atacurile şi ameninţările posibile reprezintă mediul de protecţie. Dimensiunile mediului de protecţie sunt date de relaţia biunivocă dintre acesta şi riscul asumat, dar şi de costurile suportate.

Mecanismul de protecţie fizică (parte componentă a mecanismului de protecţie) are ca scop detecţia, întârzierea şi contracararea acţiunilor ostile sau situaţiilor periculoase şi cuprinde mecanisme cu rol de barieră fizică, detecţie la efracţie şi incendiu, de control acces, de supraveghere cu camere TV şi de alarmare, intervenţie şi stingere a incendiilor.

Concluzii

Legislaţia română nu stabileşte reguli complete pentru protecţia infrastructurilor critice, referitoare la prevenirea şi minimalizarea atacurilor teroriste, pregătirea resursei umane pentru a fi gata de a reacţiona în faţa atacurilor, o capabilitate de răspuns imediat la faţa locului şi organizarea refacerii în urma unui atac. De aceea este necesară definirea conceptului de sistem integrat de protecţie, concept bazat pe analiza complexă a riscurilor şi ameninţărilor la adresa infrastructurilor critice.

Pe baza acestui concept se proiectează modelul teoretic funcţional al sistemului integrat de protecţie a infrastructurilor critice, care asigură diminuarea riscurilor la adresa acestora.

Întrucât sunt necesare soluţii de siguranţă ce pot garanta protecţia infrastructurilor critice trebuie implementate o serie de măsuri care să contribuie la diminuarea riscurilor.

Având la bază conceptul de sistem integrat de protecţie se poate adopta modelul teoretic funcţional al sistemului şi proiecta o arhitectură specifică a acestui sistem ce include: un sistem radar de supraveghere a zonelor de detecţie şi alertă; un sistem video; un sistem pentru identificare automată; arme no-letale şi sistemul de comandă şi control (C4I2SR).

Aceste subsisteme nu trebuie abordate individual pentru că nu s-ar ajunge altfel la o soluţie robustă şi completă.

În scopul conceperii şi realizării fizice a unui asemenea sistem, se impune îndeplinirea cumulativă a unor condiţii şi respectarea următoarelor etape: efectuarea unei analize de risc complete şi unui auit de protecţie care să releve riscurile şi vulnerabilităţile;

proiectarea sistemului de protecţie şi definirea procedurilor de utilizare/intervenţie; implementarea proiectului şi antrenarea personalului de intervenţie; analiza rezultatelor obţinute şi verificarea procedurilor; mentenanţa sistemului şi verificarea permanentă a respectării procedurilor.

Realizarea proiectului este o etapă multidisciplinară la care trebuie să colaboreze proiectanţi din toate domeniile sistemului de protecţie (protecţie electronică, mecanică, informatică şi umană).

BIBLIOGRAFIE

Kessel, R.T., *NATO Harbour Protection Trials 2006 analyst report: habour surveillance systems,* NATO Undersea Research Centre, La Spezia, Italy,2007.

Radu, O., Slămnoiu, G., Zărnescu, L., Coşereanu, L., *Harbor protection against terrorist threats: difficulties and possible solutions., NATO Systems Concepts and Integration Panel Symposium - SCI 180: Force protection in the Littorals,* Ottawa, Canada, September 25 - 27, 2006.

Siegfried, R., *Protection against New Asymmetric Underwater Threats,* Conference Proceedings - Underwater Defence Technology Europe 2006, Section 10A.2.

Şoricuţ, Cristian, *Sisteme de înaltă securitate,* în revista „ALARMA - Arta de a trăi în siguranţă!", septembrie 2008.