

numărul 3/2011

Alarma

Arta de a trăi în siguranță



SISTEMELE DE SECURITATE - O NECESITATE PENTRU PROTECȚIA VIEȚII ȘI A PROPRIETĂȚII

INSTALAȚIILE DE DETECTARE A INCENDIULUI NU MAI SEMNALEAZĂ DOAR INCENDIILE

CALENDARUL EXPOZIȚIONAL 2012



ARTS

Revistă editată de Asociația Română pentru Tehnică de Securitate

EDIȚIE ELECTRONICĂ

SISTEMELE DE SECURITATE – O NECESITATE PENTRU
PROTECȚIA VIEȚII ȘI A PROPRIETĂȚII 4

INSTALAȚIILE DE DETECTARE A INCENDIULUI
NU MAI SEMNALEAZĂ DOAR INCENDIILE © 8

COMUNICAREA ÎN DOMENIUL SECURITĂȚII 12

LISTA SOCIETĂȚILOR MEMBRE ALE A.R.T.S 21

NE-AM INFORMAT PENTRU DUMNEAVOASTRĂ...
CALENDARUL EXPOZIȚIONAL 2012 23

ISSN 1582-4152

Revistă editată
de Asociația Română
pentru Tehnica de Securitate



REDAȚIA:
Asociația Română pentru
Tehnica de Securitate
Splaiul Independenței 319, O.B. 152
Scara A, Etaj 2, Sector 6
(incinta SEMA Parc)
București, România
www.arts.org.ro
e-mail: office@arts.org.ro

Coordonator științific:
Cristian Soricuț
Coordonator marketing:
Adina Cioclei

Tehnoredactare:
A.R.T.S.

Articolele publicate nu angajează
decât răspunderea autorilor.

Reproducerea materialelor din
acest buletin se poate face
numai cu indicarea sursei.

Se primesc la redacție pentru publicare:
rezultatele unor studii și cercetări în
domeniul apărării vieții oamenilor la
acțiunile factorilor de risc; analize ale
unor evenimente produse în țară sau
străinătate, cu concluzii și învățăminte
pentru activitatea de prevenire, precum
și pentru pregătirea și desfășurarea
intervenției; note documentare pentru
promovarea măsurilor preventive
pentru apărarea vieții oamenilor la
acțiunile factorilor de risc.

Conform uzanțelor editoriale,
manuscrisele - publicate sau nepublicate -
nu se restituie autorilor.

SE DISTRIBUIE GRATUIT



Imagini video impecabile Supraveghere Video HD

IP8332 Cameră IP de tip bullet
pentru supraveghere de exterior
1MP • H.264 • Zi&Noapte • Iluminator IR



▲ IP8332

- Sensor CMOS 1/4"
- Rezoluție 1280x800
- Iluminator IR eficient până la 15 m
- Triplă codare H.264, MPEG-4, MJPEG
- Streaming Multiplu Simultan
- Streaming adaptabil în funcție de activitate
- Funcție detecție tentative de vandalizare
- Carcasă cu factor de protecție IP66
- Alimentare PoE standard 802.3af integrată
- Slot card SD/SDHC integrat pentru înregistrare locală
- Suportă standard ONVIF pentru integrare facilă și interoperabilitate avansată

Distribuit în România de ELTEK Distribution

SISTEMELE DE SECURITATE – O NECESITATE PENTRU PROTECȚIA VIEȚII ȘI A PROPRIETĂȚII

Gabriela DEGERATU - Specialist PR AVITECH



Sistemele de securitate se numără printre elementele care au devenit parte integrantă a realității individuale și sociale. Fie că ne aflăm acasă, pe stradă, la serviciu, suntem înconjurați de dispozitive și echipamente care ne conferă sentimentul de siguranță sau ne inhibă pornirile infracționale. La fel ca telefonul mobil sau internetul, utilizarea sistemelor de securitate face parte din activitatea cotidiană.

Prevenirea infracționalității este unul dintre obiectivele majore ale utilizării sistemelor electronice de securitate atât în zonele urbane aglomerate, cât și în cele industriale și rezidențiale. Spectrul larg al actelor combătute sau evitate prin intermediul noilor tehnologii joacă un rol important în aplicabilitatea acestora în toate ramurile de activitate.



Multitudinea de situații care necesită ajutorul tehnologiilor performante pentru asigurarea securității a generat apariția a numeroase soluții cu funcții specifice. Cele mai uzuale soluții de acest gen sunt: supraveghere video, monitorizare, detecție efracție, securitate perimetrală, control acces, interfonie. Sistemele integrate de securitate sunt o altă opțiune deosebit de competitivă la momentul actual.

Supravegherea video este cea mai răspândită dintre toate soluțiile dedicate securității și siguranței indivizilor și proprietăților. Captarea imaginilor video în toate mediile, indiferent de condiții, reprezintă unul dintre atuurile pentru care supravegherea video este prima alegere a majorității celor ce întrebuițesc sisteme de securitate.



Camere video de înaltă definiție, echipamente bazate pe IP, iluminatoare IR care permit obținerea de imagini clare chiar și atunci când nu există nicio sursă de iluminare - toate sunt echipamente de ultimă generație, cu o utilitate practică dovedită.

Aplicațiile Video Analytics sunt o altă modalitate de a crește eficiența sistemului de supraveghere, deoarece permit scanarea zonelor acoperite pe baza scenariilor predefinite și alertarea utilizatorului. Un intrus, un obiect sustras sau abandonat sunt doar câteva exemple de evenimente care pot alerta operatorul.

Monitorizarea este o soluție complexă, bazată de cele mai multe ori pe cele mai noi descoperiri tehnologice.

Procesul se realizează dintr-un dispecerat de monitorizare, spațiu care reunește echipamente și aplicații ce înlătură mare parte din erorile umane.

Un dispecerat de monitorizare asigură captarea și analiza imaginilor în timp real, monitorizarea de la distanță a sistemelor de detecție efracție, luarea deciziilor și soluționarea problemelor rapid.

Pentru că un dispecerat este locul în care se transmit evenimentele de la unul sau mai multe puncte de supraveghere, informația afișată este extrem de importantă. De aceea este esențial ca echipamentele de vizualizare să fie caracterizate de fiabilitate și capacitate de funcționare în condiții critice, 24/7.

Centrele de comandă și control pentru securitate și supraveghere trebuie să ofere imagini video de înaltă calitate și fluxuri de informație sigure, astfel ca operatorii să poată detecta și interveni asupra diverselor situații înainte ca acestea să devină amenințări.

Detecția efracției este o altă soluție de încredere pentru mediul de afaceri și pentru obiectivele strategice. Principalul rol constă în semnalizarea sigură și rapidă, 24/7, a oricărei tentative de intruziune în zonele de securitate.

Integrarea facilă cu sistemele de supraveghere video, acces control și adresare publică garantează eficiență maximă în reducerea tentativelor de efracție. Astfel, la declanșarea alarmelor se pot transmite mesaje preînregistrate la numerele de telefon stabilite în prealabil sau se poate alarma sistemul de supraveghere pentru a comuta pe monitoare camerele video care urmăresc zona în care are loc tentativa de efracție.

Soluțiile de securitate perimetrală sunt extrem de eficiente în protejarea obiectivelor care acoperă o suprafață mare sau a celor care necesită o protecție suplimentară împotriva tentativelor de efracție.

Configurarea unei soluții de securitate perimetrală trebuie să țină cont de parametri precum mărimea perimetrului, forma acestuia, tipul de obiectiv care trebuie protejat, relieful și condițiile de mediu.

În structura unui sistem de securitate perimetrală pot fi integrate echipamente precum bariere cu infraroșu, garduri inteligente, cabluri cu senzori magnetici sau telefonici, senzori de alarmă etc. Nu lipsesc nici software-urile pentru dispecerizare și management, infrastructura pe fibră optică, sisteme de transmisie GPRS, PSTN, IP și GSM.

Controlul accesului este o soluție apreciată, cu o largă întrebuintare în spații publice strategice (aeroportului, gări, stadioane, arene sportive etc.), dar și în clădirile de birouri, ansamblurile rezidențiale etc.





Soluția asigură în primul rând, o triere corespunzătoare a persoanelor care au dreptul de a intra în diverse arii ale unui perimetru, prevenind actele de vandalism, utilizarea neautorizată a unor documente sau echipamente, furtul de bunuri sau informații etc.

Totodată, existența unui sistem de control al accesului garantează creșterea gradului de organizare a personalului și posibilitatea de a monitoriza traficul de persoane, indiferent dacă vorbim despre angajați, vizitatori sau chiar de spectatorii de pe un stadion.

Soluțiile de interfonie sunt deosebit de utile pentru securitatea clădirilor. Funcțiile principale sunt trierea persoanelor care au acces în anumite zone și managementul evacuărilor inițiale în caz de urgență.



Sistemele de interfonie moderne permit controlarea, dintr-un singur punct, a tuturor intrărilor, precum și integrarea facilă cu alte sisteme de securitate dintr-o clădire.

Printre componentele unui astfel de sistem se numără posturi de exterior și de interior, puncte de ajutor și informații, stații de evacuare în situații de urgență, mecanisme de blocare, interfață videointerfonie IP etc.

Pentru companiile de mari dimensiuni și mai ales pentru cele care își desfășoară activitatea în mai multe locații (mai multe sedii, sucursale, centre de producție, depozite, puncte de desfacere etc.), soluția ideală este implementarea unui **sistem integrat de securitate**.



Ținând cont de evoluția tehnologică, integrarea soluțiilor de supraveghere video, control acces și pontaj, detecție efracție și detecție incendiu într-un singur sistem poate fi considerată o nouă tendință în domeniul securității pentru a acoperi astfel nevoia de control centralizat. Solicitățile de a răspunde unor provocări din ce în ce mai mari cu soluții performante și sisteme integrate de securitate, care încorporează tehnologii de ultimă generație sunt tot mai numeroase.

Printre avantajele unui astfel de sistem se numără monitorizarea și gestionarea în timp real și de la distanță a tuturor funcțiilor sale. Acest fapt îi conferă flexibilitate maximă, cu posibilitatea de extindere ulterioară și adaptabilitate în funcție de arhitectura fiecărei clădiri.



Un singur sistem de securitate integrată se traduce prin reducerea semnificativă a resurselor implicate în procesele de instalare, supraveghere, service, întreținere, administrare și instruire. În condițiile în care securitatea este periclitată tot mai frecvent, iar bugetele se micșorează, sistemele de acest tip sunt cele mai indicate pentru a obține cel mai bun control al securității.

Oricare ar fi mixul de soluții pentru care se optează, utilizarea acestora ne conferă încredere și un sentiment de protecție atât a bunurilor, cât și al persoanelor.

Soluții complete de securitate



La AVITECH ne-am luat angajamentul să vă oferim mai mult decât echipamente performante, sisteme integrate sau tehnologii de ultimă generație.

Noi vă propunem **soluții complete de securitate**, ce acoperă un spectru larg de domenii, de la sisteme pentru magazine și sedii de birouri cu o suprafață redusă, până la proiecte complexe, de mari dimensiuni, cum ar fi sisteme de management trafic urban, sisteme de supraveghere zone metropolitane, soluții pentru clădiri înalte și platforme industriale.

Pentru a asigura fiabilitatea soluțiilor noastre, oferta este completată de **servicii de înaltă calitate**, cum ar fi: analiză cerințe, consultanță, întocmire studii de fezabilitate, proiectare, management de proiect, logistică, instalare și punere în funcțiune, instruire, service, mentenanță.

Gama noastră de **echipamente** de securitate este cuprinzătoare, fiind îmbogățită permanent cu cele mai noi modele și tehnologii de la renumiți producători mondiali din domeniile:

- Supraveghere video
- Monitorizare
- Detecție efracție
- Interfonie
- Control acces
- Pontaj
- Securitate perimetrală
- Sisteme integrate



INSTALAȚIILE DE DETECTARE A INCENDIULUI NU MAI SEMNALEAZĂ DOAR INCENDIILE

Noi posibilități de utilizare a sistemelor de detectare și semnalizare a incendiilor

La alegerea unui sistem de detectare și semnalizare a incendiilor conform reglementărilor naționale privind aceste produse, beneficiarii clădirilor se așteaptă să li se livreze o instalație montată corect, care să poată îndeplini cu succes cerințele unei recepții exigente, scopul fiind în final primirea unei autorizații de funcționare a clădirii. Există însă în prezent o tendință evidentă ca proiectanții, instalatorii și antreprenorii să utilizeze tot mai frecvent instalația de detectare și semnalizare a incendiilor și pentru alte funcții necesare clădirii, reducând astfel în mod eficient costurile aferente echipării noii construcții.

Datorită standardelor ridicate aplicabile în prezent în Europa (seria EN 54, dar și standarde naționale specifice precum VdS sau seria TRVB), beneficiarul clădirii poate primi nu doar o instalație care transmite semnale de alarmă în caz de incendiu, ci un sistem care permite și executarea unui număr considerabil de funcții de management al clădirii, ca de ex. supravegherea și comanda clapetelor de protecție la incendiu, a trapelor sistemului de evacuare a fumului, a porților și barierelor, a echipamentelor și instalațiilor de stingere.

În plus, instalațiile de detectare și semnalizare a incendiilor pot fi conectate și cu sistemele electroacustice de avertizare în caz de urgență, sisteme mult mai eficiente decât mijloacele tradiționale de alarmare – sirenele cu avertizare tonală.

Utilizarea multivalentă sistemelor de detectare și semnalizare a incendiilor aduce avantaje semnificative beneficiarului clădirii. Iată câteva aspecte care susțin această afirmație:

- Instalațiile de detectare și de alarmă la incendiu din Europa se află sub incidența unor norme stricte referitoare la siguranța electrică, compatibilitatea electromagnetică și păstrarea funcționalității în caz de defect. Chiar dacă – probabil – nu sunt impuse cerințe atât de stricte și pentru alte sisteme, beneficiarii, proiectanții și instalatorii pot profita de aceste standarde ridicate și în alte aplicații – chiar dacă aceste aplicații sunt exploatate prin intermediul magistralei sistemului de semnalizare a incendiilor
- Îndeplinirea cerințelor impuse de standarde se asigură atât de către producător, cât și de organisme de certificare independente și notificate la nivel european. Caracteristicile tehnice ale produselor și asigurarea calității producției nu se verifică doar o singură dată la realizarea produsului, ci se auditează și anual. Se realizează astfel asigurarea continuă a calității produsului.

- Proiectanții, personalul care realizează punerea în funcțiune și cel însărcinat cu întreținerea sistemelor de detectare și de alarmă la incendiu sunt specialiști de vârf. Persoanele care proiectează sau realizează lucrări de întreținere ale unorsemena instalații trebuie să fie certificate. Premise în acest sens constituie și școlarizările continue ale angajaților (efectuate chiar și de către producători), astfel încât aceștia să fie familiarizați cu cele mai noi standarde și cu realizările tehnologice de ultimă oră. Suplimentar, aceste societăți trebuie să dispună și de un sistem de management al calității. De asemenea, firmele care se ocupă cu lucrări de întreținere trebuie să păstreze în stoc cele mai importante componente ale instalației ca piese de schimb, pentru a înlocui cât mai rapid eventualele componente defecte. Aceste aspecte subliniază încă odată faptul că principalul scop al instalației de detectare și semnalizare a incendiilor este cel de satisfacere a cerințelor de siguranță la cel mai înalt nivel.
- Este posibilă și o reducere semnificativă a costurilor. Detectoarele de incendiu pot fi găsite în aproape toate zonele clădirilor. De aceea, centrala de detectare și semnalizare a incendiului, „creierul” instalației, este conectată printr-o magistrală de comunicație cu aproape fiecare parte a clădirii. Această structură de transmisie a datelor este realizată în majoritatea cazurilor în topologie inelară, așadar redundantă. Magistrala bus poate fi utilizată nu doar pentru sistemul de detecție a incendiului, ci poate fi utilizată ca suport și pentru transmiterea altor informații și comenzi necesare clădirii.

Ce este posibil încă din ziua de azi

Centralele moderne de detectare și semnalizare a incendiului, ca de ex. de la ESSER by Honeywell, sunt minicalculatoare specializate, capabile să afișeze rapid și sigur diferite mesaje de stare ale elementelor magistralei inelare și să inițieze comenzile programate în legătură cu aceste evenimente. În cel mai simplu caz se recunoaște o mărime specifică incendiului, se activează sirenele pentru alarmarea acustică, se inițiază comenzile programate pentru situația de incendiu și se apelează pompierii. În cele de mai jos sunt descrise și alte opțiuni utile și posibile.

Conectarea în rețea cu sisteme de alarmare vocală

Beneficiarii își doresc frecvent sisteme adresare publică în numeroase clădiri, ca de ex. hoteluri, centre comerciale etc. Acestea trebuie să transmită o gamă largă de semnale, de la muzica de fond și până la mesaje publicitare. Sistemele alarmare vocală moderne prevăzute de către autorități în numeroase tipuri de

clădiri în scopul conducerii unor proceduri rapide de evacuare a utilizatorilor clădirii pot prelua foarte ușor aceste sarcini.

Realizarea unor asemenea sisteme de alarmare vocală implică un nivel ridicat de inteligibilitate a mesajelor

transmise în oricare parte a clădirii și imunitate ridicată împotriva defectelor. Aceste caracteristici sunt perfect aplicabile și în cazul sistemelor de adresare publică. De aceea este aproape naturală unificarea acestor două instalații, deoarece sistemul de alarmare vocală este capabil să preia foarte ușor ambele funcții.

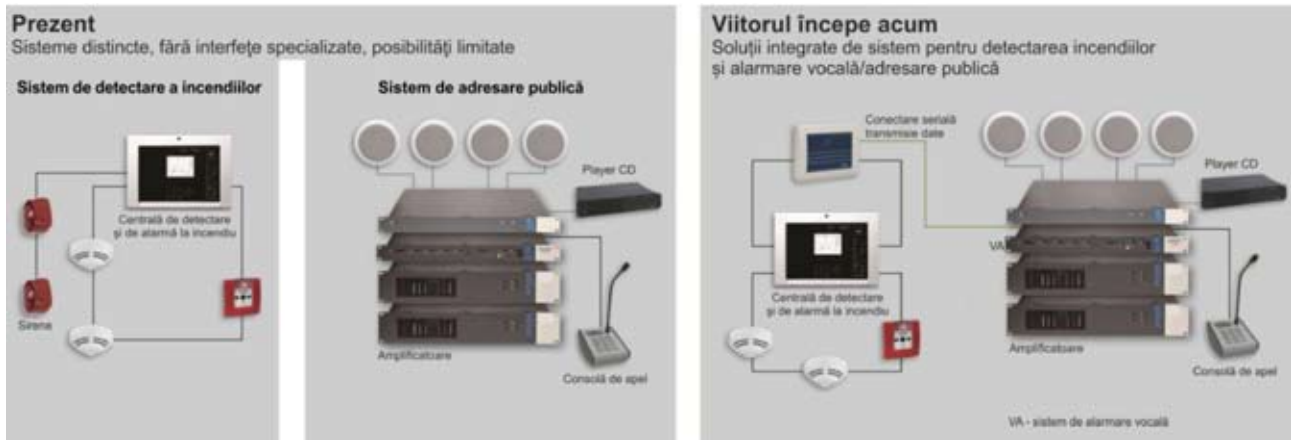


Fig. 1: Prezent și viitor: integrarea sistemelor de alarmare vocală și de adresare publică

Comanda și supravegherea clapetelor de protecție la incendiu

Clădirile dispun de clapete de protecție la incendiu montate în tubulatura de ventilație. În caz de incendiu, acestea împiedică deplasarea fumului dinspre focarul de incendiu către alte părți ale clădirii. Clapetele de protecție la incendiu sunt instalate în zona de trecere a tubulaturii de ventilație dintr-un compartiment de incendiu în altul, fiind distribuite astfel în întreaga clădire.

În ciuda faptului că în general comanda clapetelor de protecție la incendiu intră în categoria sistemelor de protecție împotriva incendiului, deseori în acest scop se utilizează un subsistem dedicat. Ca urmare, în clădire se pozează două cabluri bus distincte și se instalează două centrale (centrala sistemului de detectare și de alarmă la incendiu și cea de comandă a clapetelor de protecție la incendiu).

Instalația de ventilație și climatizare este destinată utilizării zilnice a clădirii, fiind controlată de un sistem de management dedicat. Clapetele de protecție la incendiu constituie o parte mecanică a acestor instalații, fiind însă incluse și în conceptul unitar de protecție la incendiu a obiectivului și trebuie controlate și de instalația de avertizare pentru incendii.

În caz de incendiu este foarte important să se afle care dintre clapetele de protecție la incendiu sunt închise corect și care au rămas deschise, de ex. din cauza unor defecte. Astfel, forțele de intervenție pot determina zonele clădirii în care s-a răspândit fumul. Forțele de intervenție pot primi aceste informații prin intermediul centralei sistemului de detectare și de alarmare la incendiu.

Comanda și supravegherea clapetelor de protecție la incendiu sunt sarcini complexe care nu pot fi realizate satisfăcător de instalațiile simple, tradiționale de detectare și semnalizare a incendiilor. Aceste sarcini pot fi îndeplinite însă de sisteme moderne, care includ cele mai noi elemente de intrare/ieșire cum ar fi transponderele FCT de la ESSER by Honeywell, care au fost concepute special pentru acest tip de aplicație.

Ca urmare, atât din punct de vedere al tehnologiei de protecție împotriva incendiilor, cât și din considerente legate de costuri, pentru comanda și supravegherea clapetelor de protecție la incendiu devine mai avantajoasă utilizarea unui singur sistem – cel de detectare și de alarmare la incendiu.

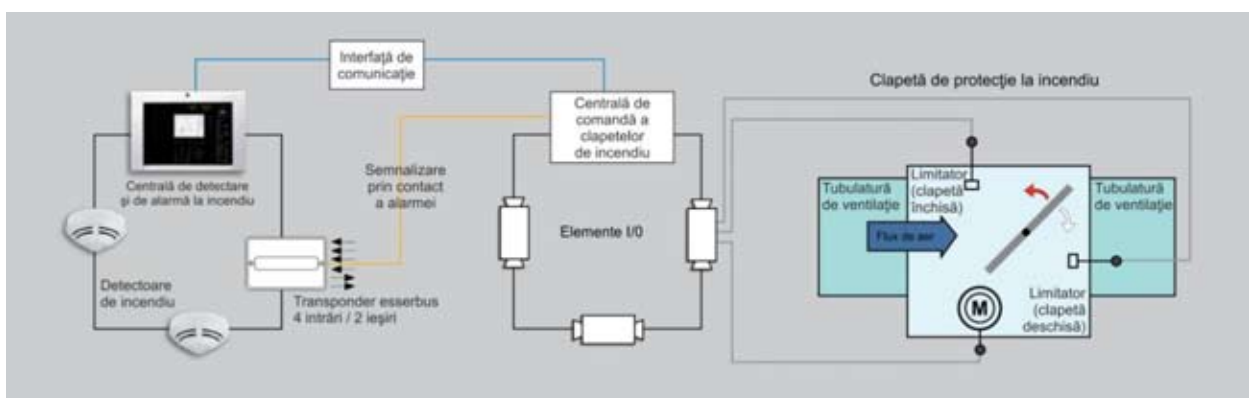


Fig. 2: Situația actuală: sisteme separate, cheltuieli duble cu cablul, posibilități limitate



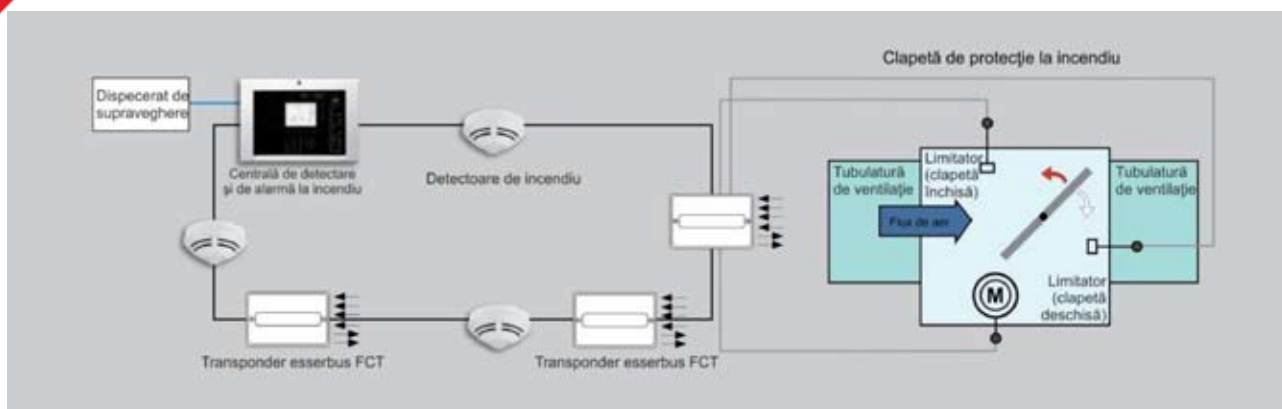


Fig. 3: Soluție de viitor: un singur sistem pentru semnalizarea incendiului și controlul / supravegherea clapetelor de protecție la incendiu

Instalațiile de semnalizare a incendiului sunt folosite tot mai des

Datorită faptului că instalațiile de semnalizare a incendiului trebuie să corespundă celor mai înalte exigențe, fiind certificate în acest sens de organisme notificate, devine evident faptul că funcțiile acestora nu pot fi preluate de alte echipamente tehnice ale clădirii. Invers însă, anumite funcții ale căderii vor putea fi preluate de sistemele de detectare și de semnalizare

a incendiilor, beneficiind în plus și de caracteristicile de siguranță specifice acestor sisteme.

O viziune pentru care Honeywell Life Safety își continuă munca inovatoare în folosul siguranței oamenilor.

Marca ESSER este parte a grupului Honeywell, fiind inclusă în divizia „Life Safety”. În România suntem prezenți cu centre de vânzări și pregătire tehnică în București și Lugoj, precum și cu un centru logistic și o unitate de producție în Lugoj.

Honeywell Life Safety Romania Str. Salcănilor nr. 2 bis RO-305500 Lugoj Tel. +40 (0)256 350 000 Fax +40 (0)256 307 564	Honeywell Life Safety Romania Calea Floreasca nr. 169A, Clădirea A, Etaj 2 RO-014459 București Tel. +40 (0)31 224 36 10 Fax +40 (0)21 204 81 85
---	--

hls-romania@honeywell.com • www.hls-romania.com

ESSER
by Honeywell



**ANALOG
CAMERA**



IP CAMERA



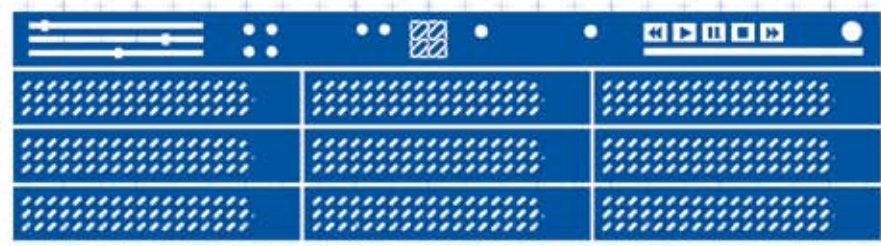
**FIRE
ALARM
INTEGRATION**

FIRE SUPPRESSION SYSTEM

OPEN PLATFORM
SECURITY MANAGEMENT SYSTEM
BUILDING MANAGEMENT SYSTEM
LOGICAL ACCES/IT SECURITY SYSTEMS



**OUTDOOR
DETECTION**



HIGH CAPACITY IP VIDEO STORAGE SERVER



**NETWORK AUDIO & VIDEO
RECORDER/TRANSMITTER**



**INTELLIGENT VIDEO
VIDEO | TRAFFIC
ANALYTICS | MANAGEMENT**



**VIRTUAL VIDEO
MATRIX UNIT**



INTEGRATED SECURITY SYSTEMS
**INTRUSION SMS
ACCES CONTROL BMS**



Siguranță prin tehnologie

COMUNICAREA ÎN DOMENIUL SECURITĂȚII

Gheorghe ILIE - Conf. univ. dr. ing.
Adrian ROȘCA - Lector formator ing.

În această lucrare dorim să sintetizăm, întâi, câteva repere ale comunicării care au relevanță implicită în comunicarea din domeniul securității și, apoi, să aducem în discuție câteva elemente ale acesteia, din dorința de a deschide o aplicație de comunicare specifică de domeniu, absolut necesară înțelegerii și eficientizării activității din domeniul securității.

Complexitatea domeniului securității reclamă, printre altele, o comunicare eficientă între toți participanții la securitate: beneficiari, proiectanți, producători, vânzători, implementatori, operatori și evaluatori.

Direcțiile eficientizării comunicării în domeniul securității sunt dificil de precizat, dar credem că cel puțin patru dintre acestea trebuie luate în considerare:

- adecvarea limbajului;
- egalitatea de șanse a interlocutorilor și libera exprimare, inclusiv, prin feed-back-uri;
- oportunitatea și completitudinea comunicării;
- neînchiderea sesiunii de comunicare (respectarea principiului continuității comunicării), chiar și când s-au stabilit și acceptat concluziile sesiunii, ținând seama de caracterul deschis al securității.

1. Repere ale comunicării

1.1 Structuralitatea comunicării

Comunicarea reprezintă forma suverană de devenire a societății, este liantul și garantul comunității, al vieții sociale, în care ansamblul de acțiuni sociale constituie o succesiune de acțiuni în care percepția și reprezentarea individuală au loc în termeni de așteptări și anticipări, previziuni și strategii.

În contextul acestei importanțe majore acordată, pe bună dreptate, comunicării, s-a fundamentat și s-a construit o remarcabilă structură științifică menită să reglementeze, eficientizeze, fluidizeze și să dezvolte

gradul de comunicare și, pe această bază, existența social. În același timp însă, plecând de la filozofii antici și până la specialiștii de marcă ai zilelor noastre în comunicare, s-a structurat o bogată și remarcabilă literatură, produsă individual sau în școli consolidate și recunoscute, despre comunicare, astfel încât te și întrebi dacă mai este ceva de spus, dacă cineva mai poate veni cu ceva nou despre acest fenomen social.

Și totuși, pentru că devenirea socială este infinită ca forme, pentru că domeniile ei se restructurează și se rafinează în permanență, comunicarea, la rândul său, se perfecționează atât ca teorie, cât și ca modele și aplicații.

Potrivit **modelului empiric**¹ al comunicării, aceasta reprezintă un proces de schimb de mesaje între o sursă de informații și un destinatar, prin intermediul unui emițător cuplat la un receptor printr-un canal de comunicație. Ca acțiune, comunicarea se esențializează în răspunsul la cele cinci întrebări fundamentale: *Cine transmite?, Ce transmite?, Prin ce canal?, Către cine? și Cu ce efect?*

Răspunsurile la aceste cinci întrebări nu sunt facile deoarece, prin similitudine cu modelul, cine transmite nu este un simplu emițător, ci este un inovator, are inițiativă și se angajează, are stil și personalitate și cântărește cu grijă ce transmite, când, cât și cui.

Considerând retorica drept **știința a comunicării**, Platon stabilește cele cinci etape ale comunicării (fig.1)²:

1 DINU, M.: *Comunicarea*, Editura Algos, București, 2000, pag. 94.

2 DUNCA, P. și colectivul: *Negocierea și medierea conflictelor*, Editura Universității de Nord din Baia Mare, Editura Detectiv, București, 2010, pag. 27.

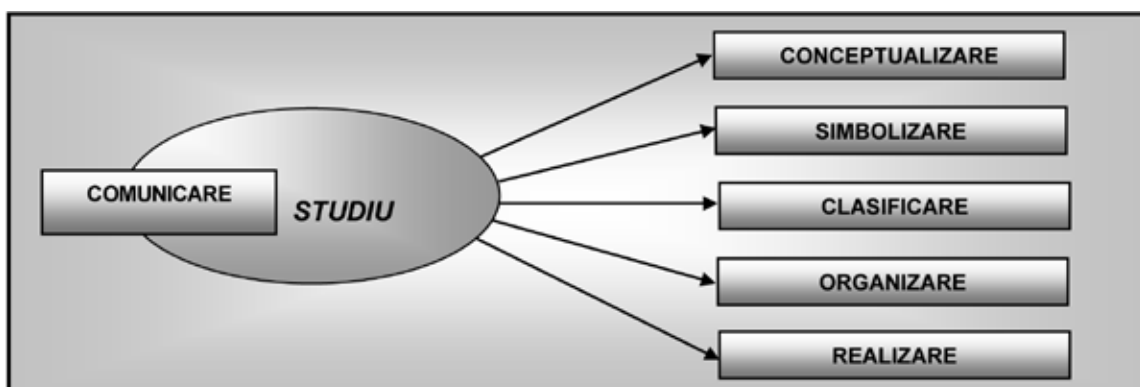


Fig. 1– Etapele comunicării

- studiul cunoașterii (conceptualizarea);
- studiul sensului cuvintelor (simbolizarea);
- studiul comportamentului uman și al modurilor de abordare a vieții (clasificarea);
- studiul aplicării practice (organizarea);
- studiul instrumentelor de influențare a oamenilor (realizarea).

Din punct de vedere structural, comunicarea reprezintă un proces³ (fig.2) prin care două entități,

3 DUNCA, P. și colectivul: Op. cit., pag. 29.

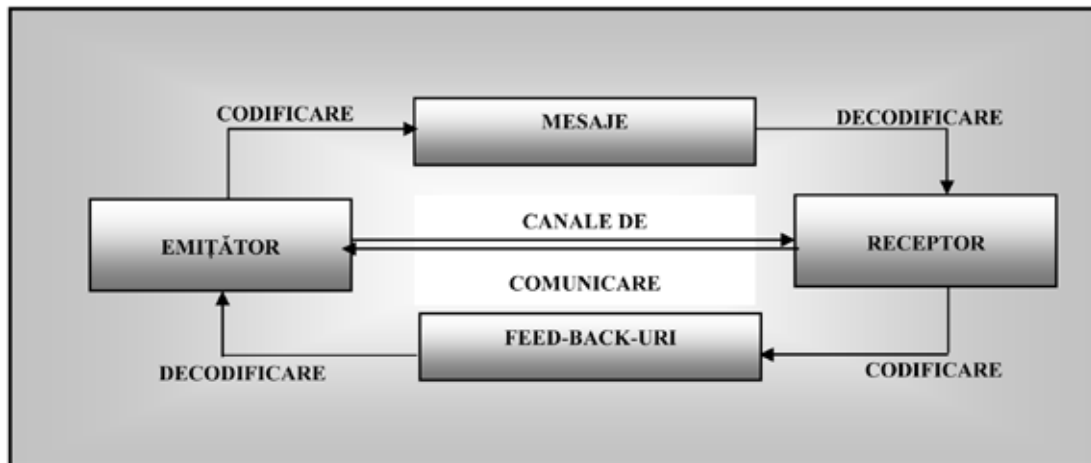


Fig. 2 – Modelul comunicării

Prin toate acțiunile și inacțiunile noastre, reușim să ne modificăm permanent relația cu lumea înconjurătoare și reușim să transmitem permanent, explicit sau implicit, mesajul nostru către lume. Nu poate exista non-comunicare. Toate acțiunile, mișcările, gesturile noastre poartă în ele semnificații perceptibile de către ceilalți, care au un impact asupra relațiilor noastre cu aceștia.

În același timp însă, comunicarea interumană este mult mai complexă, informațiile transmise și receptate pot fi gânduri, trăiri, intenții, formulate în cuvinte sau în gesturi. Pozițiile celor doi, cea a emițătorului și cea a receptorului, fiind într-o permanentă schimbare de roluri. Fluxul de informații se transmite în ambele sensuri, folosindu-se atât comunicarea verbală, cât și cea nonverbală.

Comunicarea interumană este un proces de tip tranzacțional, prin care oamenii transferă energii, emoții, sentimente și schimbă semnificații, din perspectiva educației, comunicarea având rolul de premisă, sursă, mijloc și efect. John Dewey a spus că: *"Oamenii trăiesc în comunitate în virtutea lucrurilor pe care le au în comun, iar comunicarea este modalitatea prin care ei ajung să dețină în comun aceste lucruri. Comunicarea este un mod de a exista al comunității."*

1.2 Nevoia de a comunica

Nevoia de a comunica eficient într-o organizație este imperativă pentru toți cei implicați în funcționarea sigură a acesteia. Apariția unei întreruperi în comunicare sau a unei comunicări defectuoase poate

o entitate **emițător** și alta **receptor**, schimbă între ele mesaje, folosind canale de transmitere a informațiilor, funcționând, concomitent, în ambele sensuri, fiecare dintre participanți jucând alternativ rolul de emițător și receptor.

Comunicarea înseamnă nu numai atunci când vorbim, ci mult mai mult, comunicăm și atunci când nu rostim nici un cuvânt, prin gesturi, prin comportament, comunicăm și atunci când întoarcem spatele celui alt, când zâmbim, când plângem.

fi serioasă și costisitoare. Urmările comunicării deficitare sunt importante, putând merge de la neîndeplinirea sarcinilor de serviciu, demiteri, falimente și până la pagube materiale.

Scopul comunicării poate fi pentru: **a atenționa sau a informa pe alții, a explica a distra, a descrie, a negocia, a convinge** etc.

Școala de la Palo Alto⁴ subliniază faptul că pentru a cunoaște mecanismele comunicării, trebuie studiate situațiile în care aceasta suferă dereglări sau blocaje. În această idee, definiția structural-axiomatică elaborată de școală scoate în evidență șapte principii (legi) de bază ale comunicării:

- **imposibilitatea de a nu comunica**, deci nu există non-comunicare, non-comportament comunicațional; pe primul plan situându-se intenționalitatea comunicării;
- **orice comunicare se analizează** „în conținut și relație; paralel cu transmiterea de informații, se produce și inducerea unui anumit comportament.”;
- **comunicarea este „un proces continuu**, în care feedback-ul devine factorul principal al comunicării.”;
- **comunicarea îmbracă două forme**: analogică sau digitală; omul este singura entitate care poate folosi simultan sau separat cele două forme de comunicare;
- **comunicarea este ireversibilă**, în sensul că odată receptat mesajul, acesta produce cert un efect;

4 DINU, M.: Op. cit., pag. 85.

- comunicarea presupune raporturi de forță; de regulă, emițătorul deschide sesiunea, iar receptorul o susține; eficientizarea comunicării impune egalarea șanselor celor doi competitori; de aici, importanța deosebită a feed-back-urilor;
- comunicarea presupune procese de ajustare și acomodare, precum și similaritate de înțelegere și reacție între cei doi interlocutori.

1.3 Limbajul și comunicarea

Pentru înțelegerea comunicării este esențial să avem imaginea asupra atât a cuprinderii procesului de comunicare, cât și a contextului acesteia, astfel încât să putem aprecia modul și nivelul de atingere ale celor patru scopuri ale comunicării: **receptarea, înțelegerea, acceptarea și provocarea unei reacții** (o schimbare de comportament sau de atitudine).

Foarte important este ca în procesul de comunicare, emițătorul și receptorul să atribuie aceleași semnificații mesajului transmis. Atât în ceea ce privește relevanța, cât și în forma de reprezentare.

Similaritatea interpretării, acceptată, dar numai în condițiile în care desprinderea de realitate este mai ales o problemă de reprezentare, devine inacceptabilă în momentul în care între emițător și receptor apar incompatibilități de receptare și înțelegere. Pentru a preîntâmpina apariția incompatibilităților atât emițătorul, cât și receptorul trebuie să-și pregătească transmiterea, respectiv recepția, astfel încât construcția mesajului să corespundă funcțiilor limbajului și să ajute la apropierea înțelegerii.

După Roman Jakobson⁵, limbajul este constituit conform celor șase funcții structurale și de relevanță și trebuie:

- să exprime atitudinea emițătorului față de conținutul mesajului (**funcția expresivă - emotivă**);
- să prezinte un caracter neutru-informativ și, cel mai adesea, să aducă în comunicare o a treia persoană sau obiectul de referință (**funcția referențială**, numită și denotativă, cognitivă sau informațională, care reflectă sensul mesajului). Referința suportă două niveluri: unul intern și unul extern. Primul vizează referințele operate în interiorul textului, intratextuale, cel de-al doilea este specific contextului situațional, extralingvistic;
- să apeleze la forme de imperativ, vocativ și la persoana a doua, ca instrumente pentru a determina o reacție, un efect, un rezultat (**funcția conativă - persuasivă**);
- să joace rolul de intermediar între emițător și receptor, să verifice funcționarea canalului, să realizeze și să mențină contactul între interlocutori, prin forme de atenționare sau de confirmare a continuității contactului (**funcția fatică**);
- să transmită informații despre codul utilizat, care devine el însuși obiect al enunțului (**funcția metalingvistică**). Codul trebuie să fie comun utilizatorilor, altfel comunicarea nu se poate desfășura. La nivel lingvistic, se manifestă prin

formule ca *adică, cu alte cuvinte, altfel spus*. Distincția care stă la baza identificării acestei funcții se operează între limbajul obiectual (referitor la obiect) și metalimbaj (referitor la limbaj).

- să utilizeze în descrierea unei situații, figurile de stil la nivel fonologic, morfologic, sintactic și semantic (**funcția poetică - estetică**).

1.4 Recunoaștere semnificației

Procesul de comunicare, ca fundament al relațiilor interumane, reprezintă un ansamblu de procese fizice și psihice cu ajutorul cărora sunt puse în coactivitate două sau mai multe persoane, în baza unei semnificații.

Recunoașterea semnificației este semnul activității comune și al apartenenței la scop sau la grup, fundamentul înțelegerii între interlocutori, dar și al înțelegerii de sine.

Ferdinand de Saussure face distincție între semnificant (forma acustică, de exemplu) și semnificat (relevanța mesajului).

Drept urmare, comunicarea interpersonală reprezintă o tranzacție de mesaje (directă sau sub formă de feed-back-uri), păstrându-se relațiile de rol (emițător sau receptor), de regulă, alternativ, pornită, fără dubiu, de la un anumit interes, motiv sau scop.

Relația dintre semnificant și semnificat poate fi mai strânsă sau mai largă, în funcție de completarea limbajului cu imaginea emițătorului (gesturi, atitudine, comportament); de aceea, ritualurile în comunicare sunt riguros analizate în ceea ce privește atât cutumele, interdicțiile, atitudinile, comportamentele, gestică, privirea, inflexiunile vocale, cât și improvizațiile, sublinierile sau atacurile ori retragerile.

Stilul în comunicare reprezintă personalitatea interlocutorului și definește maniera de utilizare a elementelor comunicării: gândirea, inovația, argumentarea, atitudinea, talentul, implicarea, nivelul de cultură etc.

Stilul în comunicare are o topică impresionantă, dar reducând acest lucru la elementul strict pragmatic al evaluării eficienței în comunicare, remarcăm următoarele tipuri de stiluri: *neutru, solemn, familiar, colegial, didactic, managerial* etc., referitoare la poziția și atitudinea interlocutorilor, dar și *reflexiv, emotiv, sau autoritar*, referitoare la structura interioară a interlocutorilor.

În afara stilului, comunicarea interpersonală presupune și situații de acțiune și reacție pentru interlocutori, caracterizate prin relații de tip *direct, didactic sau progresiv-formal, impersonal sau personal*.

Actul comunicațional rezidă din calitatea demersului și din gradul de angajare a participanților la comunicare, manifestări ce depind clar de personalitatea angajaților.

Dacă informația este materia primă a comunicării și aceasta asigură relevanța schimbului, nonverbalismul, kinetica, cronemica, cronostica și chiar paraverbalismul pot întregii relevanța cuvintelor, o pot înlocui temporal sau chiar definitiv în anumite contexte, ca manifestări psihologice de personalitate.

5 DINU, M.: Op. cit., pag. 95.

1.5 Caracteristicile psihologice ale comunicării

Caracteristicile psihologice ale comunicării sunt analizate pe baza mai multor modele (fig. 3)⁶,

6 Ilie T-S, *Rolul personalității în binomul comunicare - securitate a informațiilor*, Securitatea privată nr. 1/2010 (32), pag. 14.

care au în vedere stări interne și reprezentări mentale, ca proprietăți ale subiecților comunicării (emițător și receptor), precum și a lumii predefinite și obiective. În acest fel, analiza comunicării devine o reconstrucție a intențiilor și reprezentărilor fiecăruia, cu accesibilitate directă atât din partea subiecților, cât și din partea observatorilor.

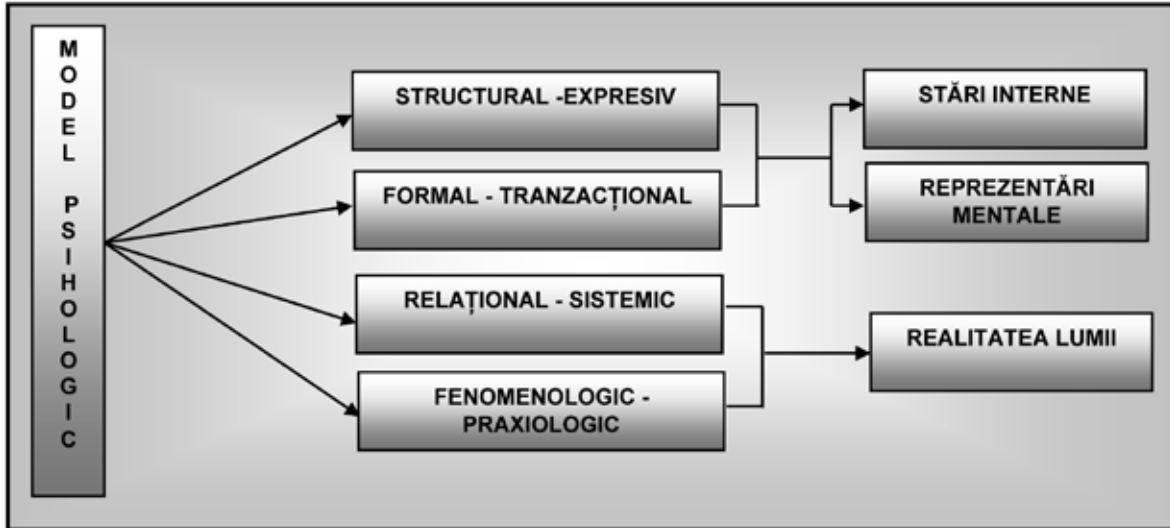


Fig. 3 – Stări interne și reprezentări mentale

Conform **modelului structural – expresiv** originea exprimării verbale a subiecților se află în structura psihică a fiecăruia. Comunicările, ca proces, sunt direct marcate de motivațiile și nevoile interne și de constituția psihicului subiecților, ca un rezervor de pulsuni primare sau refulare.

Modelul formal – tranzacțional structurează comunicarea în baza unei analize tranzacționale bazate pe trei tipuri de atitudini corporale și mesaje paraverbale:

- atitudini și paralimbaje rigidizate și neutre care derivă din ceea ce s-a transmis de la părinți către copii;
- atitudini și paralimbaje care țin de stăpânirea sentimentelor, însoțind comunicări logice și raționale;
- atitudini și paralimbaje care permit să transpună sentimentele și stările de tip: furie, plăcere, bucurie, iubire, mândrie.

Modelul relațional-sistemic scoate în evidență supremația relațiilor dintre indivizi, potrivit căreia perceperea înseamnă perceperea relațiilor de interacțiune de tipul: *digitală analogică, simetrică și complementară, confirmare și invalidare, tangențializare, descalificare, mistificare* etc.

Modelul fenomenologic-praxiologic se bazează pe intenționalitatea conștiinței care permite unui individ să existe prin intermediul său cultural și să fie caracterizat prin analize fenomenologică, comprehensivă și etnometodologică.

Indiferent de modelul utilizat pentru analiza comunicării, eficiența acesteia se bazează pe reușita unui subiect, angajat cu bună intenție, să ajungă la starea

internă a altui subiect, precum și pe capacitatea acestora de a participa la elaborarea realității transmise.

1.6 Protecția informațiilor în comunicare

Comunicarea presupune cognoscibilitate, raționament, relaționalități, bijectivitate și reacție, în timp ce nivelul de cunoaștere depinde decisiv de calitatea surselor de informare și de angajamentul participanților la cunoaștere⁷.

Dacă comunicarea eficientă presupune un schimb continuu de informații, activ constructiv, disponibil și eficient, astfel încât modelul inovării, stilului, angajării, memorării și livrării să se manifeste operațional, securitatea trebuie să asigure siguranța și stabilitatea de proces, protecția angajării participanților la comunicare, protecția valorilor informaționale și disponibilitatea, integritatea, confidențialitatea și nonrepudierea informațiilor care fac obiectul comunicării (fig. 4).

Comunicarea în calitate de proces, pentru a fi eficientă trebuie să i se asigure sigure calitate, adică siguranță și stabilitate (principalele caracteristici ale calității).

Calitatea procesului depinde însă și de modelul folosit, capabil să asigure atingerea obiectivelor de transfer și înțelegere de informații. De aceea, modelul des, nu neapărat cel al filosofilor romani, trebuie să asigure, pentru a fi operațional, informații, forme de structurare și transmitere, reflecții și reacții, într-o dinamică adecvată. Din această cauză, modelul trebuie protejat la imixțiuni, la deformări, la denaturări și mai ales față de blocări de toate tipurile.

7 Ilie T-S, *Op. cit.*, pag. 16.

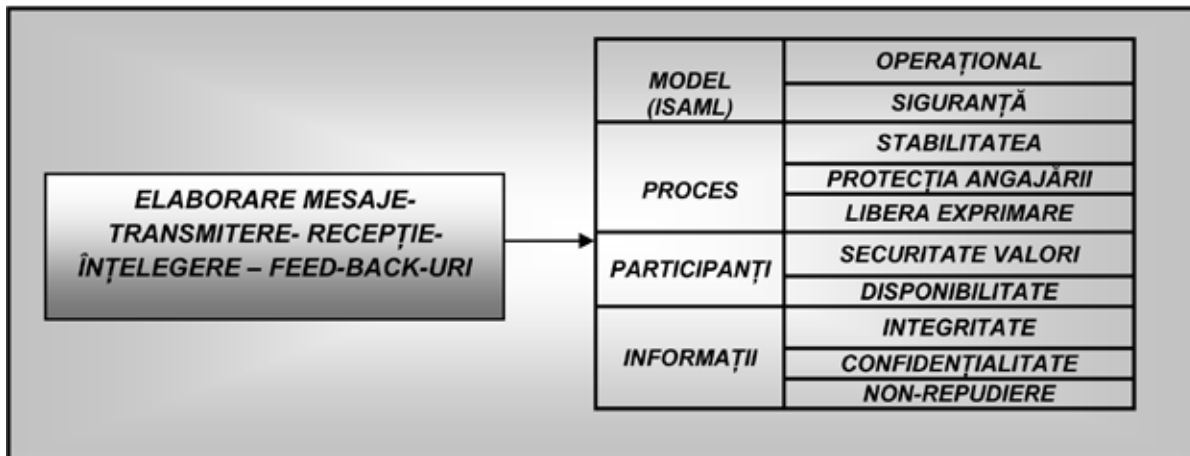


Fig. 4 – Securitatea comunicării

Indiferent de presiuni, de zgomot, de amestec limitat sau de acte de insecuritate, pentru o comunicare eficientă, modelul trebuie să rămână operațional.

Securitatea procesului este cel puțin necesară eficienței și ea trebuie să se manifeste în toate cele patru componente ale sale: funcțională, fizică, informațională și de personal.

Dacă despre componentele funcțională și fizică, fiind vorba de un proces, se pot evidenția, în principal elemente așa numite clasice (protecția infrastructurii, rezistența resurselor, continuitatea procesuală, apărarea împotriva atacurilor fizice etc.), față de componentele informațională și de personal, în securitatea comunicării sunt elemente specifice care merită o atenție deosebită.

Dintre acestea, vom evidenția doar două, acolo unde se manifestă și personalitatea comunicatorilor:

(1) **Protecția mesajelor** care presupune asigurarea tuturor funcțiilor de comunicare:

- **expresivitatea** prin asigurarea raționalității emițătorului, controlul emotivității sale, a labilității sentimentale și subiective; disponibilitatea informațiilor;
- **referențialitatea** prin asigurarea veridicității obiectivelor de referință; veridicitatea informațiilor;

- **faticul** expresiv al contactului cu cuprinderea atenționărilor interlocutorilor, convenționalizarea și ritualizarea formală, confidențialitatea schimbul de informații;
- **metalingvistica** prin unitatea de expresie, înțelegere și reacție, precum și prin convenția nenegării a ceea ce ai transmis; **non-repudiarea** mesajelor;
- **poetica** expresiei prin convenții de cod și sensuri, de semne sau structurări; **non-conflictualitatea** sau **convenționalitatea** informațiilor;
- (2) **Protecția emoțională** a interlocutorilor care presupune:
 - susținerea managementului proceselor;
 - asigurarea conexiunii echipelor participante la proces;
 - fundamentarea deciziilor și susținerea participării la acțiunile de implementare a acestora;
 - armonizarea intereselor procesuale;
 - asigurarea legăturilor între procesului, precum și între sistemele integrate în același mediu personal sau de existență (cu influență reciprocă);
 - întreținerea stărilor de emulație, de participare asumată din perspectiva guvernării riscurilor.

- VA URMA-

2. Comunicarea în domeniul securității

LISTA SOCIETĂȚILOR MEMBRE ALE A.R.T.S.

1	3 I AUTOMATIZĂRI ȘI TELECOMUNICAȚII	CRAIOVA
2	A&I INDUSTRY	LUGOJ
3	A-TECH ELECTRONICA	BUCUREȘTI
4	AL.SE.RO. IMPEX	ORADEA
5	ALARM SECURITY CONSULTING CS	BUCUREȘTI
6	ALFRED NET	VOLUNTARI
7	AMBER SECURITY	BUCUREȘTI
8	AMPRO SYSTEM	BACĂU
9	ANTONESCU MIHAIL BOGDAN, PF	BUCUREȘTI
10	ATECNO SERV	BRAȘOV
11	AVITECH CO.	BUCUREȘTI
12	BALASFI ADRIANA	BAIA-MARE
13	BĂDESCU SORIN MARIAN	BUCUREȘTI
14	BĂNULEASA MIHAI , PF	BUCUREȘTI
15	BELAI DAN PAUL, PF	GHEORGHIEI
16	BENTEL DISTRIBUTION	BUCUREȘTI
17	BENTEL SISTEM	CLUJ-NAPOCA
18	BIDEPA EXPERT	BUCUREȘTI
19	BIT SERVICII	BUCUREȘTI
20	BORCEA NICOLAE	PLOIEȘTI
21	BRATAN GABRIEL	BUCUREȘTI
22	CAPABIL	TIMIȘOARA
23	CASIDO	GALAȚI
24	CBRN EXPERTS CONSULTING	BUCUREȘTI
25	CENTRUL RIVERGATE	BUCUREȘTI
26	CIVITAS SYSTEMS	CRAIOVA
27	COMANDOR	TIMIȘOARA
28	COMANDOR INTERNATIONAL	TIMIȘOARA
29	COMTEH	CONSTANȚA
30	CONSAL SECURITY	BUCUREȘTI
31	CONTACT PLUS	ARAD
32	D&S SYSTEMS ELECTRONIC	BUZĂU
33	DACHE VALENTIN	BUCUREȘTI
34	DARIA TELECOM	PITEȘTI
35	DEPISTO STAR	GHEORGHIEI
36	DIACOM PRESTCOM	LUPENI
37	DOLEX PRO GROUP	BUCUREȘTI
38	DOTEL ALARMS	BUCUREȘTI
39	EGMS-ELECTROMONTAJ ȘI SERVICE	BUCUREȘTI
40	ELECTRA	IAȘI
41	ELECTRO BBSZ	MIERCUREA-CIUC
42	ELECTRONIC ADVANCED SYSTEMS	BUCUREȘTI
43	ELPROF	BUCUREȘTI
44	ELTREX	TIMIȘOARA
45	EMPORIUM	BUCUREȘTI
46	ESMART GROUP CO	BUCUREȘTI
47	EUROGUARD.	TÂRGOVIȘTE
48	FIBER NET	BUCUREȘTI

49	FIRERO ROMANIA	TÂRGU-MUREȘ
50	FORȚA ZERO-PAZĂ ȘI SECURITATE	BISTRIȚA
51	G.I.S. SYSTEM SECURITY	BUCUREȘTI
52	G.U. FERROM COM	BUCUREȘTI
53	GENDIS SYSTEMS	BUCUREȘTI
54	GENERAL SECURITY	CLUJ-NAPOCA
55	GEOSEI DYNAMICS	BUCUREȘTI
56	GEROM INTERNATIONAL PRODIMEX	BUCUREȘTI
57	GLOBAL SECURITY SISTEM	BUCUREȘTI
58	GTS TELECOM	BUCUREȘTI
59	HELINICK	BUCUREȘTI
60	HELIOS SECURITY	GALAȚI
61	HOLDIMAG	BAIA-MARE
62	HONEYWELL LIFE SAFETY ROMÂNIA	LUGOJ
63	I. & C.	TULCEA
64	ICCO SYSTEMS	BRAȘOV
65	IDEAL INSTAL	BRAȘOV
66	IDS SECURITY SYSTEM PROVIDERS	BUCUREȘTI
67	IMSAT CUADRIPOLO	BRAȘOV
68	IMSAT SERVICE	BUCUREȘTI
69	INTERNATIONAL CONSULTING SECURITY GRUP	BUCUREȘTI
70	KEYSTONE TEXTEL	TIMIȘOARA
71	KMW SYSTEMS	IAȘI
72	KT ELECTRONICS & AUTOMATICS	BRAȘOV
73	LAN SERVICE	BUZĂU
74	L.E.N.Co. ELECTRONIC	BRĂILA
75	LOCKSYS EXPERT	BUCUREȘTI
76	LOGIMAETICS SECURITY	TIMIȘOARA
77	MAC DOUGLAS GRUP	BUCUREȘTI
78	ML SYSTEMS CONSULTING	BUCUREȘTI
79	NAPA IMPEX	DANGEORGIU DE MUREȘ
80	NEI GUARD	VOLUNTARI
81	NEOTRONIX GROUP	BUCUREȘTI
82	NEW MOBITEL SECURITY	SATU-MARE
83	NORD EST CONECTIONS	BOTOȘANI
84	NOSTER IMPORT EXPORT	BUCUREȘTI
85	NOVATEHNIC	BRĂILA
86	NTT ELECTRONIC SERVICE	BUCUREȘTI
88	OPTIMUM PROD IMPORT	BUCUREȘTI
89	PARADOX SERVICE	PIATRA-NEAMȚ
90	PRACTIC INSTAL	BUCUREȘTI
91	PRIMATECH	BAIA-MARE
92	PROSECURITY DISTRIBUTION	BUCUREȘTI
93	PROTECTOR SYSTEM	BUCUREȘTI
95	QUADRA ACCES SYSTEM	REȘITA
95	QUARTZ MATRIX	IAȘI
96	QUICK SERVICE - future IT	CONSTANȚA
97	RASIROM R.A	BUCUREȘTI
98	RDD TRUST SECURITY	CRAIOVA
99	ROMANO ELECTRO	BUCUREȘTI
100	ROMTEST ELCTRONIC	BUCUREȘTI

101	ROVIS CO	BUCUREȘTI
102	SAG SERVICES PROVIDER	BUCUREȘTI
103	SASU DAN , PF	BUCUREȘTI
104	SCHRACK SECONET AG REPREZENTANTA	BUCUREȘTI
105	SEBE CRISTINEL, PF	BUCUREȘTI
106	SECANT SECURITY	BUCUREȘTI
107	SECPRAL COM	CLUJ-NAPOCA
108	SECURITY GLOBAL CONSULTING	BUCUREȘTI
109	SECURO TECH	ARAD
110	SECURYTAS SYSTEMS	PLOIEȘTI
111	SEMCO	BALȘ
112	SET ALARM INTERNATIONAL	BUCUREȘTI
113	SIEL INVEST	BUCUREȘTI
114	SIEMENS	BUCUREȘTI
115	SINVEX MULTISERVICE	PLOIEȘTI
116	SION SECURITY	BUCUREȘTI
117	SMART SECURITY TECH	BUCUREȘTI
118	SSI IMPORT-EXPORT	BUCUREȘTI
119	STIMPEX SYSTEMS	BUCUREȘTI
120	TECH SAFES	BUCUREȘTI
121	TECHNOSEC	BUCUREȘTI
122	TECHNOSYS	PLOIEȘTI
123	TEHNO ALROM	IAȘI
124	TEHNO EXPRES	BUZĂU
125	TERMOPROT	BRAȘOV
126	THE FACILITY MAINTENANCE COMPANY	BUCUREȘTI
127	TORNADO CREATIVE	BUCUREȘTI
128	TOTAL SECURITY	CLUJ-NAPOCA
129	UNION PROTECTION	CLUJ-NAPOCA
130	UNIVERSAL SERVICE 95	BUCUREȘTI
131	URMET & GERBER COMMUNICATIONS	BUCUREȘTI
132	UTI CONSTRUCTION & FACILITY MANAGEMENT	BUCUREȘTI
133	UTC SECURITY & FIRE SOLUTIONS	BUCUREȘTI
134	UTI SYSTEMS	BUCUREȘTI
135	VEGA	ONEȘTI
136	VH ELECTRONIC	CRAIOVA
137	VHI	BRAȘOV
138	VIDEOVOX SECURITY	BUCUREȘTI
139	VOICU MARIN IOAN - PFA	BUCUREȘTI
140	VONREP	TÂRGU JIU
141	ZAMFIR DUMITRU, PF	MOARA VLĂSIEI, ILFOV
142	ZECO ELECTRONICS AND IMPORT EXPORT	CLUJ-NAPOCA
143	ZODD TECK	BUCUREȘTI

**CENTRUL DE
FORMARE PROFESIONALĂ
A.R.T.S.**

**A.R.T.S. este acreditată pentru organizarea
cursurilor pentru ocupațiile:**

**TEHNICIAN PENTRU SISTEME DE
EDETECȚIE, SUPRAVEGHERE VIDEO,
CONTROL ACCES
- cod COR 313210 -**

**INGINER SISTEME DE SECURITATE
- cod COR 214438 -**

PROIECTANT SISTEME DE SECURITATE

**Modul pentru sisteme tehnice de efracție,
control acces, CCTV, monitorizare și
pentru sisteme tehnice de detectare, sem-
nalizare și alarmare la incendiu
- cod COR 214319 -**

PROIECTANT SISTEME DE SECURITATE

**Modul pentru instalații pentru stingerea
incendiului și sisteme de ventilare pentru
evacuarea fumului și gazelor fierbinți
- cod COR 214319 -**

Înființată în anul 2003, Asociația Română pentru Tehnica de Securitate, este o organizație profesională apolitică, non-guvernamentală și non-profit, ce reunește societățile implicate pe piața serviciilor de securitate și care militează pentru profesionalizarea firmelor membre și creșterea nivelului de securitate în România.

A.R.T.S. - membră



A.R.T.S. - membră



**ROMANIAN
SECURITY FAIR**

2012

În calitate de organizator, A.R.T.S. anunță organizarea celei de a doua ediții a evenimentului expozițional **Romanian Security Fair 2012.**

ASOCIAȚIA ROMÂNĂ PENTRU TEHNICA DE SECURITATE
București, Splaiul Independenței 319
O.B. 152 Scara A Etaj 2
Telefon: +4031-405.64.02
Fax: +4031-405.64.01
E-mail: office@arts.org.ro
www.arts.org.ro

ARTS
Arta de a trai în siguranță

EVALUAREA PRELIMINARĂ A OBIECTIVELOR DE SECURITATE. NECESITATE, UTILITATE, EFICIENȚĂ

Gheorghe ILIE - Conf. univ. dr. ing.
Adrian ROȘCA - Lector formator ing.

I. Consideratii generale

În articolul din nr. 2/2011 al revistei "Alarma" am menționat etapele ce compun evaluarea preliminară a obiectivelor de securitate:

- a) etapa I - analiza și definitivarea cerințelor de securitate;
- b) etapa a II-a - revizuirea metodologiilor de evaluare;
- c) etapa a III-a - nivelul îndeplinirii cerințelor prestabilite prin proiect și estimarea prețului de cost;
- d) etapa a IV-a - analiza documentelor de evaluare în vederea stabilirii *acceptanței*, utilizând metode diverse, printre care și metoda costurilor necesare, și, de asemenea, am precizat că, în faza finală se va redacta "raportul de evaluare", care conține concluziile privind structura, integrabilitatea și modelul ciclului de viață al produsului, precum și aspecte economico-funcționale: componența, fezabilitatea/utilitatea, costuri, performanțe, grade de operaționalitate.

În urma unor discuții cu câțiva din cei care au citit articolul sus-menționat, nu este suficient a aplica metode convergente și recunoscute pentru a obține soluții de securitate performante, deoarece problema costurilor și, în general, a eficienței activității de asigurare a securității unui obiectiv, reprezintă o chestiune omniprezentă, la fiecare pas și, în cele mai multe cazuri, determinantă. În orice categorie de obiectiv, de interes privat sau public, problema costurilor este o problemă de decizie a top-managementului și, de aceea, nu se poate aborda chestiunea securității fără o analiză atentă a costurilor aferente implementării și menținerii soluțiilor de securitate.

II. Abordarea specifică a aspectelor economice

În domeniul investițiilor, în faza de evaluare a necesității și utilității unor sisteme sau instalații complexe se folosește conceptul de evaluare și analiză a raportului **cost/beneficiu**, sau a raportului **beneficiu/cost**, care se calculează anual.

Referindu-ne la domeniul asigurării protecției obiectivelor, este cunoscut faptul că investițiile în securitate nu aduc profit (beneficiu) direct. În această situație este necesar să se particularizeze definirea și calcularea factorilor care conduc la evaluarea raportului sus-menționat. În cele ce urmează vom analiza raportul cost/beneficiu.

1. Elemente specifice

Sintagma unanim acceptată, care definește specificitatea domeniului, este **Return Of Security Investment – ROSI**: în traducere liberă "*întoarcerea investițiilor în securitate*" sau, "*ce câștigăm de pe urma implementării sistemelor de securitate*".

În contextul descris de acest articol, **costul** conține toate cheltuielile cu concepția, proiectarea și implementarea sistemului complex de securitate, precum și cele necesare pentru consultanță, training, mentenanță, hardware și software, managementul riscului și exploatare, pe toată durata ciclului de viață a sistemului.

Beneficiul, pentru această categorie de produse, este definit ca fiind totalitatea economiilor provenind din evitarea pierderilor fizice, de proces, de imagine, alterarea informațiilor proprietare și altele, drept consecință a existenței și funcționării sistemului de securitate ca pavază principală în fața acțiunii divelor amenințări din mediu.

De regulă, argumentele în favoarea cheltuielilor pentru securitate sunt, majoritar, calitative, în sensul că, fără "securitate" entitatea publică sau privată va înregistra "pierderi"; în aceste situații, beneficiul rămânând același, balanța inițială cost-beneficiu se va înclina spre costuri. Se mai vehiculează și alte sintagme recunoscute și acceptate, pentru a orienta afacerile în raport de necesitatea asigurării securității lor, precum:

- a te bucura de "securitate", înseamnă a derula afaceri convenabile;
- a avea "securitate", este echivalent cu a cheltui pentru asigurări;
- reticența la a cheltui pe "securitate" va scădea pe măsura creșterii activelor unei entități (bunuri, valori, informații etc.).

Evident că, din punctul de vedere al profesioniștilor, atât din domeniul asigurării securității, cât și din sectorul economico-financiar, aceste puncte de vedere, deși recunoscute, nu sunt suficiente și mai ales, nu sunt determinante.

Ideea de bază în utilizarea raportului cost/beneficiu, în domeniul asigurării securității obiectivelor, este de a calcula pierderile cauzate de neasigurarea protecției, pe care organizația se așteaptă să le aibă și să se compare acestea cu investițiile în securitate, necesare pentru a reduce impactul amenințărilor netratate. Se folosește conceptul **ALE** (Annualised Loss Expectancy - evaluarea pierderilor așteptate/estimate, anual), care se referă la:

- afectarea componenței fizice și procesuale (construcții, amenajări, servicii, instalații etc.) datorită neasigurării protecției complexe (sistem de securitate corespunzător și caracteristici constructiv-funcționale aferente valorilor și importanței procesului predominant în organizație);
- pierderi de informații (din punctul de vedere al integrității, confidențialității, disponibilității) privitoare la baze de date, clienți, informații de piață, licențe, informații proprietare, informații clasificate, datorită vulnerabilităților din sistemele

informatice proprii, a caracteristicilor fizice ale obiectivului, pază umană necorespunzătoare s.a.

Pentru a reduce, apriori, aceste viitoare posibile pierderi, organizațiile trebuie să investească, cel puțin, în următoarele direcții:

- asigurarea securității fizice și procesuale;
- asigurarea securității informaționale;
- calificarea și asigurarea securității personalului implicat.

În scopul evaluării cât mai aproape de realitate se vor detalia costurile curente, anuale (CA), care se referă la:

- licențele produselor de securitate achiziționate;
 - echipamentele specifice de securitate;
 - consultanța și analiza pe probleme de specialitate.
- Nu trebuie scăpate din vedere nici costurile referitoare la:
- asigurarea logistică a echipamentelor și susținerea utilităților;
 - susținerea mentenanței;
 - achiziția de software, firmware și actualizarea acestora pe durata ciclului de viață;
 - achiziția de componente hardware specifice sectorului IT (firewall, switch-uri, hub-uri, routere s.a.);
 - instruirea personalului;
 - restabilirea funcțională după incidente de securitate;
 - asigurarea salariilor pentru personalul implicat în domeniul securității;
 - rezolvarea problemelor privind impactul noilor amenințări din mediu, apărute în timp, precum și evaluarea periodică a noutăților tehnice și tehnologice specific etc.

Deoarece pierderile estimate, anuale, reprezintă o valoare, evident, aproximativă, influențată de o categorie largă de factori externi sau interni, se utilizează indicele EFS (Eficiența Sistemului), care exprimă gradul în care funcționarea unui sistem de securitate, împreună cu procedurile corespunzătoare, asigură reducerea pierderilor în cadrul organizației unde este instalat.

Din datele menționate în literatura de specialitate, acesta se încadrează între 75-85%, ca eficiență, în condițiile implementării unei soluții de securitate, corecte și adaptate mediului și obiectivului protejat și asigurării mentenanței corespunzătoare.

În final, economiile anuale (EA) se pot exprima astfel:

$$EA = ALE * EFS - CA$$

Analiza eficienței costurilor (investițiilor) are dificila misiune de a «măsura» performanțe nefinanciare; în securitate, ar trebui evaluat modul cum ripostează la atacuri, reducerea pierderilor fizice și procesuale, protecția informațiilor reprezintă rezultatul investițiilor în sisteme de securitate. După cum se vede, calculul economiilor anuale este o expresie care integrează efectele tuturor măsurilor de securitate din obiectiv.

Întrucât, pe durata ciclului de viață a produsului-sistem de securitate, se înregistrează numeroase schimbări, up-grade-uri, ar fi foarte util să avem un «feed-back», să se evidențieze consecințele unor măsuri concrete, punctuale, de protecție fizică, procesuală sau informațională. În plus, am avea avantajul acționării pe «direcția principală» de manifestare a amenințărilor și, implicit, de reducere a costurilor globale cu securitatea.

Ideea de bază a unei abordări în acest sens constă în faptul că o «contramăsură» are două consecințe:

- a) reduce probabilitatea manifestării acesteia, având efect «preventiv» și/ sau,
- b) reduce impactul determinat de acțiunea atacurilor, având efect «reparator».

În acest sens, se menționează, câteva exemple:

- implementarea unui sistem de protecție perimetrală, instalarea de firewall-uri, software antivirus, aplicații de criptare, au efecte «preventive»;
- aplicarea de proceduri de «back-up» are efect «reparator» și «preventiv»;
- aplicarea, în proiectare și implementare, a principiului redundanței are efect «preventiv» și «reparator».

Impactul și frecvența manifestărilor amenințărilor (incidentelor de securitate), sunt, evident, dificil de cunoscut apriori, ele reprezentând o variabilitate statistică, insuficient studiată. Din acest motiv ponderile alocate, atât probabilităților, cât și impactului, nu pot fi suficient de precise și, mai ales, nu se pot evidenția acele situații de «vasi-simultaneitate» care pot determina consecințe extrem de nefavorabile.

Ca urmare, estimarea ROSI este necesar să fie amendată prin introducerea unuia sau mai multor parametri și studierea rezultatelor obținute din variația acestora; acest lucru se obține aplicând metode de generare a unor valori aleatoare pentru parametri și efectuând simularea diverselor situații, pe aceasta cale. O metodă frecvent folosită în acest scop, este metoda Monte Carlo.

2. Concluzii

Concepția și implementarea de soluții de securitate reprezintă o necesitate, atât timp cât există amenințări, care se încadrează într-o plajă largă de manifestări.

Incidentele de securitate nu sunt, în mod necesar, independente. De cele mai multe ori, consecințele defavorabile asupra activelor sunt determinate de o succesiune de evenimente, unele cu aspect inițial «pașnic», aflate în configurații și intercondiționări diverse.

Pentru a susține fundamentarea deciziei de către top-management este necesar să cunoaștem, atât consecințele investiției în securitate, cât și influența punctuală, a diverselor acțiuni concrete de asigurare a securității unui obiectiv. Impactul total al incidentelor de securitate poate conduce la o depășire a impactului rezultat ca sumă a impacturilor incidentelor independente; de exemplu, scăderea dramatică a încrederii într-un sistem informatic cu bug-uri sau ușor atacabil, poate avea ca efect final abandonarea întregului sistem.

Cunoașterea mediului, a caracteristicilor obiectivului, precum și evaluarea cât mai realistă a eficienței măsurilor de securitate, sunt premise serioase în asigurarea protecției dorite.

3. Bibliografie

1. Risk Management Standards AS/NZS 4360-2004
2. Security Metrics Guide for Information Technology Systems (NIST 800-55)

NE-AM INFORMAT PENTRU DUMNEAVOASTRĂ... CALENDARUL EXPOZIȚIONAL 2012

Nr crt.	Data	Eveniment expozițional	Locația
1	14-16 februarie	IFEST - Trade Fair for Environment, Energy and Safety at Work	Ghent (Belgia)
2	14-17 februarie	SST - Security and Safety Technologies - Fachmesse für Sicherheitstechnologie	Moscova (Rusia)
3	19-23 februarie	Firehouse World - Exhibition and Conference	San Diego (SUA)
4	20-22 februarie	ISS World - Intelligence Support Systems for Lawful Interception, Criminal Investigations and Intelligence Gathering	Dubai (Emiratele Arabe Unite)
5	22-23 februarie	FeuerTRUTZ - Trade Fair with Congress for Preventive Fire Protection	Nuremberg (Germania)
6	27 februarie – 03 martie	RSA Conference	San Francisco (SUA)
7	28 februarie – 03 martie	SICUR - International Security, Safety and Fire Protection Exhibition	Madrid (Spania)
8	28 februarie - 02 martie	Safety & SECURITY - International Specialized Exhibition for Security, Safety and Protection	Sofia (Bulgaria)
9	29 februarie – 02 martie	KIPS - Kiev Int. Protection, Security & Fire Safety Exhibition	Kiev (Ukraine)
10	01 – 03 martie	Secutech India - India's Professional Exhibition and Conference for Electronic Security, Homeland Security and Fire Security	Mumbai (Bombay) (India)
11	05 – 08 martie	Defense & Security - A Tri-Service Asian Defense & Internal Security Event for Land, Sea and Air	Bangkok (Thailanda)
12	06 – 07 martie	IFSEC West Africa - West African Security Industry Event	Lagos (Nigeria)
13	06 – 07 martie	Border Security Expo	Phoenix (SUA)
14	06 – 09 martie	Security Show	Tokyo (Japonia)
15	19 – 21 martie	ISNR - International Security National Resilience Exhibition & Conference	Abu Dhabi (Emiratele Arabe Unite)
16	28 – 30 martie	ISC EXPO/West - International Security Conference and Exposition	Las Vegas (SUA)
17	martie	Fire Tech - Fire Safety Technologies	Kiev (Ukraine)
18	04 – 06 aprilie	Beijing International Building Technology - Electrical Engineering, Building and Home Automation	Beijing (China (PR))
19	16 – 21 aprilie	FDIC - Fire Department Instructors Conference	Indianapolis (USA)
20	18 – 20 aprilie	Secutech - International Exhibition and Conference for Electronic Security, Info Security, Fire and Safety	Taipei (Taiwan)
21	23 – 26 aprilie	SECUREX - International Security Exhibition	Poznan (Polonia)
22	24 – 26 aprilie	SAWO - International Fair of Work Protection, Rescue and Fire Fighting	Poznan (Polonia)

23	24 – 26 aprilie	SPIE Defense, Security + Sensing - Annual International Conference and Exhibition on Infrared Imaging, Optics and Sensor Equipment	Baltimore (SUA)
24	24 – 26 aprilie	Mexico Fire Expo	Mexico City (Mexic)
25	24 – 26 aprilie	INFOSECURITY Europe - Information Security Event	Londra (Marea Britanie)
26	24 – 27 aprilie	MIPS - International Protection, Security & Fire-Fighting Exhibition	Moscova (Rusia)
27	25 – 26 aprilie	Counter Terror Expo	Londra (Marea Britanie)
28	01 – 02 mai	Health & Safety Canada - IAPA Conference & Trade Show (Industrial Accident Prevention Assn.)	Toronto (Canada)
29	07 – 09 mai	IDREE - International Disaster Reduction and Emergency Technology & Equipment Expo	Beijing (China (PR))
30	08 – 10 mai	ExpoSec - Specialized Exhibition on Electrical Security Systems	Sao Paulo (Brazil)
31	14 – 17 mai	IFSEC - Security Solutions & Network Advantage	Birmingham (Marea Britanie)
32	15 – 17 mai	Safety and Health Expo	Birmingham (Marea Britanie)
33	15 – 18 mai	SECURITY KOREA (formerly SecurityWorld Expo)	Seoul Republica Korea)
34	22 – 24 mai	ITEC - Defence - Training - Simulation - Education	Londra (Marea Britanie)
35	22 – 25 mai	SAME JETC - The Joint Engineer Education & Training Conference and Expo	St. Louis (SUA)
36	22 – 25 mai	CIEPE - China Police - Asia Pacific Police Logistics & Equipment Trading Platform	Beijing (China (PR))
37	22 – 25 mai	ISSE - Integrated Safety and Security Exhibition	Moscova (Rusia)
38	mai	ProfStyle (formerly TELOGREYKA) - International Exhibition of Uniforms, Special Footwear, individual Protection Facilities, Labor Protection, Caution Systems, Sewing Machinery, Technic	Moscova (Rusia)
39	04 – 06 iunie	Asian Securitex - Asian International Security, Safety and Fire Protection Show & Conference	Hongkong/SAR (China (PR))
40	05 – 07 iunie	PRAGOALARM/PRAGOSEC - International Fair of Security Equipment, Systems and Services, Fire Protection and Rescue Equipment	Praga (Republica Cehă)
41	06 – 08 iunie	ArbeitsSicherheit Schweiz - Exhibition for Occupational Safety, Health and Prevention	Berne (Elveția)
42	11 – 14 iunie	NFPA Conference & Expo - Conference & Expo of National Fire Protection Association	Las Vegas (SUA)
43	12 – 14 iunie	ISF - Malaysia's Security & Safety Exhibition & Forum	Kuala Lumpur (Malaezia)
44	12 – 14 iunie	FIREC - Malaysia's Fire Protection and Rescue Expo & Conference	Kuala Lumpur (Malaezia)
45	13 – 16 iunie	F.I.R.E. - Annual Conference & Exposition New York State Association of Fire Chiefs	New York (SUA)
46	19 – 21 iunie	IFSEC South Africa SECUREX - International Security Exhibition and Conference	Midrand (Africa de Sud)

47	28 – 30 iunie	Secutech Thailand - International Trade Fair for Security and Safety	Bangkok (Thailanda)
48	iunie	ISS World Europe - Intelligence Support Systems for Lawful Interception, Criminal Investigations and Intelligence Gathering	Praga (Republica Cehă)
49	iulie	KISS - Korea International Safety and Security Exhibition	Seoul (Republica Korea)
50	03 – 04 august	FRI - Fire-Rescue International	Denver (SUA)
51	15 – 17 august	Intersec Buenos Aires - South American Integral Security Fair	Buenos Aires (Argentina)
52	22 – 24 august	Secutech Vietnam - International Security, Fire & Safety Exhibition & Conference	Ho Chi Minh City (Viet Nam)
53	03 – 06 septembrie	LOGISTYKA - Exhibition for Police and Military Equipment and Fire Protection	Kielce (Polonia)
54	04 – 07 septembrie	SMM - Shipbuilding, Machinery & Marine Technology - International Trade Fair Hamburg	Hamburg (Germania)
55	05 – 07 septembrie	TURVALLISUUS - Safety and Security Exhibition	Tampere (Finlanda)
56	10 – 12 septembrie	ASIS - American Society for Industrial Security International Annual Seminar & Exhibits	Philadelphia (SUA)
57	10 -14 septembrie	INTERPROTEC - International Fair of Personal Protective Equipment, Health and Safety at Work	Brno (Republica Cehă)
58	12 – 14 septembrie	OS+H Asia - Occupational Safety + Health Exhibition & Conference for Asia	Singapore (Singapore)
59	18 – 20 septembrie	COS+H - China International Occupational Safety & Health Exhibition	Beijing (China (PR))
60	18 – 21 septembrie	SKYDD - PROTECTION & SECURITY EXPO - International Security, Safety & Fire Exhibition	Stockholm (Suedia)
61	19 – 21 septembrie	ELENEX VIETNAM - Int. Exhibition for Electrical, Buildings & Urban Infrastructure, Installation & Automation	Ho Chi Minh City (Viet Nam)
62	19 – 21 septembrie	CIHS - China International Hardware Show - Trade Fair for Tools, DIY and Building Hardware, Security Systems, Locks and Fittings	Shanghai (China (PR))
63	20 – 23 septembrie	ISAF Istanbul - Istanbul Fair for Security, Fire, Emergency and Search-Rescue	Istanbul (Turcia)
64	25 – 27 septembrie	Protection Technologies - International Exhibition Forum	Kiev (Ukraina)
65	25 – 28 septembrie	SECURITY - The World Forum for Security & Fire Prevention	Essen (Germania)
66	25 – 28 septembrie	Fire Safety of XXI Century - International Exhibition for Fire Prevention and Liquidation	Moscova (Rusia)
67	27 – 29 septembrie	Nationaler Kongress der französischen Feuerwehr	Amiens (Franța)
68	septembrie	Disaster Management Exhibition & Conference	New Delhi (India)
69	septembrie	African Aid Relief & Disaster Management Expo & Conference	Midrand (South Africa)
70	septembrie	Security & Fire Automatics (Complex Security Systems)	Moscova (Rusia)
71	03 – 05 octombrie	IFSEC India - Indian Security Exhibition	New Delhi (India)
72	03 – 05 octombrie	FISP - International Safety and Protection Fair	Sao Paulo (Brazilia)
73	04 – 07 octombrie	Retter - Fachmesse für Sicherheit & Einsatzorganisation	Wels (Austria)
74	05 – 07 octombrie	R.E.A.S. - Emergency Exhibition	Montichiari (Italia)

75	09 – 11 octombrie	RSA Conference Europe - The World's leading Information Security Conference and Exhibition	Londra (Marea Britanie)
76	16 – 18 octombrie	Arbeitsschutz Aktuell - Safety and Health - The Prevention Forum - Congress & Trade Fair	Augsburg (Germania)
77	16 – 18 octombrie	it-sa - The IT Security Expo	Nuremberg (Germania)
78	18 – 20 octombrie	China Fire - International Fire Protection Equipment Technology Conference and Exposition	Beijing (China (PR))
79	22 – 24 octombrie	NSC - National Safety Council Congress & Exposition	Orlando (USA)
80	22 – 25 octombrie	Sfitex - St. Petersburg International Security & Fire Exhibition	St. Petersburg (Rusia)
81	23 – 26 octombrie	BEZPEKA - SECURITY - International trade show of security systems and equipment	Kiev (Ukraina)
82	23 – 26 octombrie	Interpolitex - International Forum for Means of State Security	Moscova (Rusia)
83	25 – 27 octombrie	Romanian Security Fair	București (România)
84	27 – 30 octombrie	DEFENSYS - Thessaloniki International Defense & Security Fair	Thessaloniki (Grecia)
85	31 octombrie – 01 noiembrie	Infosecurity.nl - IT Security trade show	Utrecht (Olanda)
86	octombrie	Ambiente Lavoro Convention - Exhibition of Hygiene and Safety at Working Places	Modena (Italia)
87	octombrie	International HSE Expo	Kish (Iran)
88	03 – 04 noiembrie	ISC Solutions (ISC Expo East) - National Summit on Security - An ISC Expo Event	New York (USA)
89	06 – 08 noiembrie	Dubai Air Medical & Rescue Show	Dubai (Emiratele Arabe Unite)
90	07 – 09 noiembrie	SICUREZZA - International Exhibition for Surveillance and Alarm Electronics Equipment and Safety and Security Devices	Milano (Italia)
91	14 – 16 noiembrie	Geoprotecta - Swiss specialised exhibition for integral risk management of natural disasters and climate change	St. Gallen (Elveția)
92	26 – 28 noiembrie	MILIPOL QATAR - International Exhibition of internal State Security, Police Equipment, Industrial Security, Civil Defence	Doha (Qatar)
93	noiembrie	Central Asia Secure Expo - International Exhibition for Security, Safety, Fire, Building Automation and Police Equipment	Almaty (Kazakhstan)
94	noiembrie	IFSEC Arabia - Security Exhibition	Riyadh (Arabia Saudită)
95	01 – 04 decembrie	MEFSEC - Middle East & Africa Fire, Safety & Security Exhibition	Cairo (Egipt)
96	03 – 05 decembrie	INDESEC EXPO - India's integrated Homeland Security and Defence Exhibition	New Delhi (India)
97	03 – 06 decembrie	I/ITSEC - Interservice/Industry Training, Simulation and Education Conference	Orlando (SUA)
98	04 – 07 decembrie	EXPOPROTECTION/FEU - The Exhibition for Risk Management	Paris (Franța)
99	06 – 09 decembrie	Mamtek Istanbul - Shops, Shopping Centers, Market systems, Equipment and Logistics Fair	Istanbul (Turcia)

ARTS

Arta de a trăi în siguranță



ASOCIAȚIA ROMÂNĂ PENTRU TEHNICA DE SECURITATE

BUCUREȘTI Sector 6
Splaiul Independenței 319
O.B. 152 Scara A Etaj 2

www.arts.org.ro
office@arts.org.ro

Tel: +4031.405.64.02
Fax: +4031.405.64.01