SOLUȚIE DE IMPLEMENTARE A UNUI SISTEM DE SECURITATE CU TESTARE RIDICATĂ

Corneliu Popescu

Universitatea din Oradea
E-mail: corneliu_popescu@uoradea.ro

Rezumat: Un sistem de control al pericolelor este proiectat pentru a face față unor situații diferite de pericol la care este expusă, inevitabil, orice clădire, respectiv, orice activitate specifică, desfășurată în cadrul ei. Cu alte cuvinte, sistemele de control pericol, nu sunt productive, ele având sarcina de a crea precondițiile de funcționare fiabilă a obiectivului protejat. De calitatea unui astfel de sistem depinde, de multe ori, însăși existența clădirii respective, viața persoanelor, integritatea bunurilor din ea și desfășurarea activității.

În lucrarea de față, se prezintă o metodă eficientă cu aplicabilitate practică, putând fi utilizată cu succes în vederea creșterii calității acestor sisteme prin îmbunătățirea gradului posibilității de testare conform cerințelor justificate prin aplicația implementată.

Soluția propusă are în vedere creșterea calității sistemului, prin adoptarea unor măsuri specifice în direcția creșterii disponibilității, atribut primordial al calității unui sistem de securitate.

Plecând de la sarcinile specifice ale unui sistem de securitate și având în vedere implicațiile gradului de detectabilitate și mentenabilitate în disponibilitatea unui sistem, precum și tehnicile moderne de maximizare ale acestor atribute, în [3] și [4] am propus o soluție originală – în acord cu cerințele unui sistem de securitate – ce constă într-o structura redondanță globală cu autodiagnoză și reconfigurare la defect. Aplicarea soluției duce la o disponibilitate ridicată pentru sistem, cu implicații de majorare a costului sistemului cu aproximativ 20-23% - ceea ce o recomandă ca avantajoasă și din punct de vedere economic.

Cuvinte cheie: sistem de securitate, disponibilitate, „testare".

1. Noțiuni de bază legate de securitate

În literatura de specialitate, noțiunea de securitate este definită ca fiind un complex de măsuri procedurale, fizice, logice și juridice, destinate prevenirii, detectării și corectării diferitelor categorii de accidente fie că provin din cauze naturale, fie că ele apar ca urmare a unor acte de sabotaj. Prin categorii de accidente se înțeleg acele accidente care pun în pericol viața umană, informațiile, bunurile materiale, valorile și, nu în ultimul rând, mediul înconjurător.

Conceptul de securitate poate fi structurat pe trei niveluri, după cum urmează:

1. **Securitate fizică**: este nivelul „exterior" al securității și constă în prevenirea, detectarea și limitarea accesului direct asupra bunurilor, valorilor și informațiilor; de exemplu, într-un sistem distribuit, prima măsură de securitate care trebuie avută în vedere este cea de securitate fizică, prin prevenirea accesului fizic la echipamente: un anumit infractor care dorește să sustragă informații din sistem, trebuie, mai întâi, să intre în contact fizic cu echipamentul.

În afara aspectelor prezentate, securitatea fizică implică luarea măsurilor de protecție împotriva incendiilor, inundațiilor, scăpărilor de gaze și a calamităților naturale, toate aceste măsuri fiind legate de protecția, în ansamblu, a clădirilor împotriva pericolelor potențiale.

La ora actuală, se apreciază că distrugerile de informații, datorate vulnerabilității nivelului de securitate fizică, constituie cel mai mare procent de insecuritate.

2. **Securitate logică**: reprezintă totalitatea metodelor ce asigură controlul accesului la resursele și serviciile sistemului; securitatea logică poate fi împărțită în două mari niveluri:

- *niveluri de securitate a accesului*;
- *niveluri de securitate a serviciilor*.

Principalele *niveluri de securitate a accesului* sunt:

a. nivelul de acces la sistem: acest nivel este răspunzător de gradul de accesibilitate al utilizatorilor în sistem, de decuplarea sau de cuplare a unor stații;

b. nivelul de acces la cont: acest nivel verifică dacă utilizatorul are un profil valid pentru sistem;

c. nivelul drepturilor de acces: după ce un utilizator trece prin cele două niveluri anterioare, el va primi de la sistem anumite drepturi de conectare.

Principalele *niveluri de securitate a serviciilor* sunt:

a. nivelul de control al serviciilor: acest nivel este răspunzător de funcțiile de raportare a stării serviciilor și, respectiv, de avertizare;

b. nivelul de drepturi la serviciu: determină modul de utilizare a unui anumit cont de servicii.

3. **Securitate juridică**: este nivelul alcătuit dintr-o colecţie de legi naţionale care reglementează actul de violare a nivelurilor de securitate fizică şi logică şi stabileşte sancţiuni penale ale acestor acte; aici este important de subliniat că sistemul de securitate fizică trebuie astfel conceput, încât să permită în orice situaţii analiza posteveniment care să fie utilizată ca „martor" în procesul de realizare a obiectivului de securitate juridică.

Cele trei niveluri de securitate, anterior definite, determină, la un moment dat, securitatea în ansamblu a obiectivului protejat. Prin urmare, se poate constata că, între nivelurile de securitate fizică, logică şi juridică, există o interconectare puternică, ele influenţându-se reciproc, iar, în unele situaţii, determinându-şi existenţa ca nivel de securitate valid.

În orice caz, cele precizate mai sus, arată clar că soluţia cea mai eficientă pentru asigurarea securităţii la un moment dat, este analiza globală a gradului de securitate oferit de fiecare nivel în parte şi compensarea acelui nivel care, la un moment dat, oferă un grad mai scăzut de securitate, cu măsuri ferme de creştere a securităţii celorlalte două niveluri sau numai a unuia dintre ele de aşa manieră încât, securitatea obiectivului, în ansamblu, să fie mai mare sau egală cu un grad minim necesar.

În figura 1, sunt detaliate la nivel de bloc – conform [1] – elementele ce formează un sistem de securitate complex (*Danger Management System*):

Mediu de operare pentru securitate					
FIZIC	PERSONAL	REGLEMENT.	HARD	SOFT.	RETEA
Prevenire efracţie	Interviuri	Legi	Control acces	Control acces	Criptare
Detecţie efracţie	Vizualizare mediu	Politici	Fiabilitate	Securitate multinivel	Control Dialup
Protecţia mediului	Instruire	Proceduri	Protecţie electrică	Dezvoltare structurată	Controlere de reţea
Restaurare la dezastru	Monitori-zare	Acţiuni răspuns	Logica hardware	Verificări conturi	Fibre optice

Figura 1. Blocurile unui sistem de securitate

Întrucât nu există măsuri pentru asigurarea unui securităţi absolute, a fost dezvoltată strategia *Multiple-barrier* prin care o entitate de protejat este asigurată prin mai multe bariere de protecţie, aşa cum este ilustrat în figura 2:

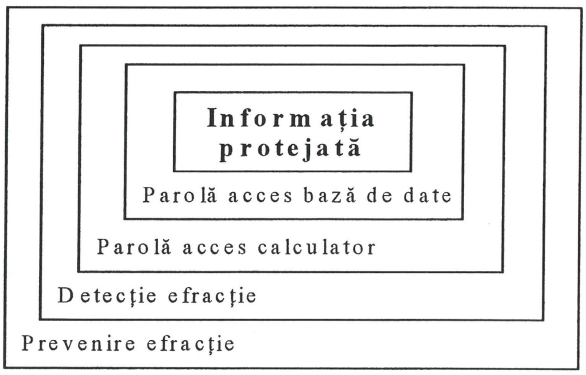

Figura 2. Strategia Multiple-barier

Tehnologia unui sistem de securitate este bazată pe conceptul inteligenţei distribuite [1], prin care mai multe subsisteme autonome (unităţi de control) sunt conectate, printr-o reţea, la sistemul terminal. Unităţile de control pot menţine autonomia totală şi capacitatea de funcţionare, independent de orice reţea terestră de comunicare deoarece au posibilitatea de transmisie prin satelit către sistemul terminal. Nu există ierarhie actuală de funcţionare, adică nu există relaţie *master-slave* între unitatea de control şi sistemul terminal. De fapt, unităţile de control sunt cele ce controlează reţeaua de securitate. Nu sistemul terminal este cel ce scanează unităţile de

control, ci unitățile de control emit spontan mesajele lor de alarmă, acest principiu fiind „piatra de temelie" a conceptului de securitate fizică.

Operația de alarmă locală și funcțiile de control ale unității de control previn eșecul total al sistemului, chiar și în timpul întreruperii liniilor de transmisie între subsisteme și terminalul de sistem.

2. Evaluarea sarcinilor unui sistem de securitate

Pentru ca la un moment dat, asupra unui sistem dat, să poată fi întreprinse măsuri menite a-i crește calitatea, trebuie analizate sarcinile ce revin sistemului la diferite momente de timp, astfel că, măsurile de creștere a calității rezultate în urma analizei, vor avea justificare clară chiar prin prisma funcțiilor de bază ale sistemului.

O condiție esențială pentru ca un sistem de securitate să-și poată îndeplini misiunea de protecție este ca el să fie „pregătit" tot timpul, adică, oricând s-ar produce condiții pentru un potențial pericol, sistemul să fie funcțional și să lanseze corect procedurile, conform scenariului prestabilit pentru fiecare eveniment în parte. Astfel, apare o diferență majoră între sistemele tehnice propriu-zise, care, la terminarea programului de lucru, sau de multe ori chiar în timpul programului de lucru, sunt oprite (excepție fac unitățile al căror proces tehnologic nu poate fi oprit) și un sistem de securitate, care, o dată instalat și pornit, nu mai este oprit niciodată, el funcționând non-stop zi-noapte. Alimentarea cu energie a sistemului de securitate se face prin conectare directă, înainte de întrerupătorul general al clădirii, unde este instalat sistemul (nu are comutator de pornit/oprit sau fișă de alimentare). Este de notat faptul că sistemul de securitate funcționează, de asemenea, chiar și în cazul întreruperii accidentale sau provocate a tensiunii rețelei de 220V, prin trecerea automată a tuturor componentelor sistemului de securitate pe baterii tampon de rezervă, special prevăzute în acest sens.

Principala funcție a unui sistem de securitate este să identifice evenimentele nedorite și să asigure utilizatorul cu instrucțiuni clare în situații critice fără a lăsa nici un dubiu asupra acțiunilor ce se impun.

Situațiile critice de alarmă sunt caracterizate, de obicei, de apariția mai multor alarme și mesaje de stres: în asemenea situații, utilizatorul trebuie să știe exact ce acțiuni să întreprindă la fiecare fază.

Sistemele de securitate moderne asigură utilizatorul cu un suport serios pentru asemenea situații. Ele îl informează clar asupra acțiunilor ce trebuie luate, iar, în anumite situații, este forțat un răspuns exclusiv.

Structura răspunsului este parte integrantă a funcțiilor unui sistem de securitate. În acest fel, utilizatorul sistemului are la orice moment informații asupra stărilor monitorizate și instrucțiuni clare asupra măsurilor ce se impun a fi luate.

Funcțiile sistemelor de securitate se extind de asemenea, și la alte aspecte de genul controlului priorității alarmelor și al mesajelor, al protecției sistemului, respectiv, a punctelor individuale de achiziție a datelor împotriva accesului neautorizat.

Interacțiunea acestor elemente este o precondiție decisivă pentru operarea eficientă a unui sistem de securitate. Un sistem de securitate permite monitorizarea centralizată de către utilizator precum și operarea centralizată a subsistemelor conectate. Acesta este motivul pentru care sistemul de securitate trebuie să integreze toate punctele de achiziție a datelor într-o organizare comună prin care utilizatorul să poată manevra toate alarmele și mesajele în aceeași manieră. Spre exemplificare, se prezintă cele mai importante funcții pe care o unitate de control le execută non-stop:

1. **Recepția alarmelor și a mesajelor**: Unitatea de control suportă recepționarea și recunoașterea alarmelor și a mesajelor de la toate subsistemele conectate:

a. elemente de detecție și control;

b. dispozitive periferice;

c. alimentare cu energie electrică.

2. **Transmiterea alarmelor și a mesajelor**: Unitatea de control poate transmite alarmele și mesajele către un dispecerat central de intervenție fie pe linie terestră, fie utilizând comunicația prin satelit sau radio.

3. **Operarea sistemelor detecție a pericolului**: Sistemele conectate, de detecție a pericolului, pot fi operate prin console sistem dedicate prin care se face recepționarea, recunoașterea și resetarea alarmelor, comutarea off /on a detectorilor, setarea detectorilor în modul test. De notat faptul că se face o parolare a accesului pe diferite niveluri de operare.

4. **Organizarea priorităților**: Toate alarmele și mesajele de la toate subsistemele conectate sunt clasificate în funcție de importanța lor, asigurându-le o prioritate: cea mai mare prioritate se acordă alarmelor ce

semnalizează pericol pentru viaţa omului (alarme de foc); prin contrast, alarmele de efracţie au de obicei o prioritate mai redusă. Tot prioritate scăzută se acordă mesajelor eronate sau alarmelor tehnice (nivel de lichid, depăşire de temperatură etc.), ce nu constituie un pericol major pentru viaţa umană şi pentru mediul înconjurător; această organizare a priorităţilor asigură că în situaţia apariţiei alarmelor multiple, se va afişa şi procesa alarma cu prioritatea cea mai mare.

5. **Acces la susbsisteme şi puncte de achiziţie a datelor**: Cerinţele de protecţie ale unui sistem de securitate sunt mai mari decât cele ce pot fi implementate prin utilizarea unui nume şi a unei parole. Este clar că nu toate persoanele conectate la sistem trebuie să aibă acces la toate subsistemele şi la toate punctele de achiziţie a datelor.

6. **Vizibilitatea stării informaţiei curente la toate nivelurile – observabilitatea**: Operarea unei unităţi de control impune ca starea tuturor subsistemelor să fie vizibilă la nivelul unităţii de control. Ori de câte ori se schimbă starea, noua situaţie trebuie să fie memorată automat la toate locaţiile, indiferent dacă această tranziţie de stare rezultă prin schimbarea condiţiilor periferale sau dintr-o acţiune operator şi indiferent de locul unde a fost introdus răspunsul operator: la un subsistem sau la consola sistem. Toate sistemele conectate trebuie să afişeze automat noua stare. O schimbare de stare iniţiază un proces de comunicare, ce actualizează automat toate sistemele integrate la noua informaţie de stare.

7. **Controlabilitatea pentru:**

a. semnale de alarmă;

b. activarea comenzii la distanţă a alarmei şi a semnalelor de cădere;

c. senzori de umiditate, ventilaţie, mişcare, camere video;

d. activare de comenzi pe evenimente.

8. **Umplerea**: Selecţia şi evaluarea înregistrărilor.

9. **Înscrierea în jurnalul de evenimente**: Evenimentele sunt înregistrate cronologic împreună cu:

a. starea sistemului;

b. cauzele alarmei;

c. evaluarea şi tipărirea datelor înregistrate.

10. **Autodiagnoza defectelor**: Unitatea de control monitorizează permanent, în timp real, factori interni care pot provoca funcţionarea defectuoasă a sistemului sau, în unele situaţii, pot produce „căderi" ale sistemului; gama de defecte monitorizate este amplă şi include, de fapt, toate nivelurile unui sistem de securitate, începând cu elemente de detecţie, linii de comunicaţie, echipamente ale sistemului de securitate (există o listă de defecte monitorizate de către o unitate de control).

Funcţiile mai sus prezentate, se completează cu cele prezentate concret în cadrul [2], unde este făcută o sinteză de aplicaţie, bazată pe o unitate de control de generaţie actuală (PC5010), produsă de compania canadiană "*Digital Security Controls*" una dintre cele mai mari companii producătoare de echipamente destinate sistemelor de securitate.

În afara funcţiilor menţionate mai sus, orice sistem de detecţie a pericolelor, şi anume, sistemele de avertizare a incendiului trebuie, în final, să alerteze oamenii în aşa fel încât ei să ştie cum să se comporte pentru a scăpa de pericol. În mod normal, alertarea se realizează de către avertizoare sonore. Acest concept este bun atâta timp cât oamenii sunt instruiţi şi antrenaţi şi atâta timp cât clădirea este mică şi foarte clar structurată. În aceste condiţii, reacţiile de panică şi consecinţele sale pot fi ocolite, în general. Totuşi, în clădirile mari nu mai este posibil acest lucru deoarece, pe de o parte, evenimentul produs poate genera panică generalizată cu consecinţe grave [1], iar, pe de altă parte, sunt necesare informaţii mai specifice, la orice moment de timp, în vederea salvării situaţiei. În astfel de condiţii, se impune utilizarea unui sistem de evacuare şi comunicare prin voce a urgenţelor *(Emergency Voice Communication and Evacuation Systems* – EVAC [1]).

Sistemele de comunicare prin voce a urgenţelor au rolul de a creşte siguranţa oamenilor prin trimiterea unor mesaje verbale în instalaţia de difuzoare cu specificaţiile următoare:

- informare despre o situaţie periculoasă şi dezvoltarea ei;
- instrucţiuni precise pentru o parte din clădire cum să se realizeze evacuarea;
- evacuarea întregii clădiri;

- reasigurarea oamenilor dacă nu mai este nici un pericol.

De asemenea, este necesar un sistem de interfonie de urgență, conectat în toată clădirea, care să sprijine pompierii în sarcina lor dificilă de evacuare a ocupanților. Principalele funcții ale unui astfel de sistem sunt:

1. **Alertă**: În scopul alertării populației, este trimis în întreaga clădire un semnal pulsatoriu (20 pulsații/minut). Acest semnal are cea mai mică prioritate (depinzând de reglementările locale, semnalul de alertă poate fi, de asemenea, un mesaj vocal electronic).
2. **Evacuare**: În același timp, un semnal EVAC (de 120 pulsații/minut) va fi transmis prin difuzoare, în zona direct afectată de pericol. Acest semnal va fi prioritar față de semnalul de alertă (depinzând de reglementările locale, semnalul de evacuare poate fi, de asemenea, un mesaj vocal electronic).
3. **Page (Semnal de informare audio)**: Ori de câte ori este nevoie, pompierii vor transmite instrucții precise, la microfoanele din toată clădirea sau numai în anumite zone. Acest semnal va fi prioritar față de semnalul de evacuare.

Selecția semnalului (canalului) cerut se poate face automat (cu ajutorul sistemului de alarmă în caz de incendiu) și /sau manual de către pompieri.

Sistemul de comunicare vocală ar trebui să fie proiectat în așa fel încât toate cele trei semnale (canale) descrise mai sus să poată fi selectate simultan, pentru diferite zone, adică toate cele trei semnale sunt în permanență disponibile prin toată clădirea, prin fiecare amplificator (magistrală audio). Dacă această funcție importantă există, sistemul se poate într-adevăr numi sistem cu 3 canale.

Complexitatea funcțiilor anterior prezentate, pe care un sistem de securitate trebuie să le poată executa, este dictată de complexitatea sarcinilor atribuite, în vederea asigurării în condiții optime a dezideratului de securitate fizică.

Practic, acest ansamblu complex de funcții care trebuie să poată fi executate la orice moment de timp, de către unitățile de control și, respectiv, de către terminale sistem din cadrul dispeceratelor, dictează imperativ o înaltă disponibilitate pentru sistemul de securitate.

3. Disponibilitatea, criteriu primordial al calității sistemelor de securitate

În cadrul [4], disponibilitatea a fost definită prin probabilitatea ca un sistem să opereze corect și să fie apt să-și execute funcțiile la un moment dat. După cum se observă, definiția disponibilității exprimă fidel cerința fundamentală a unui sistem de securitate.

Trebuie subliniat că disponibilitatea diferă față de fiabilitate prin faptul că fiabilitatea depinde de un interval de timp, pe când disponibilitatea se consideră la un moment dat. Astfel, un sistem ce are frecvente perioade de nefuncționare poate avea disponibilitate ridicată, dacă perioadele de nefuncționare sunt extrem de scurte. Cu alte cuvinte, disponibilitatea unui sistem depinde nu numai de cât de frecventă este perioada de nefuncționare, ci și de cât timp durează repararea. În acest punct, este important de stabilit clar care sunt factorii ce determină creșterea disponibilității unui sistem, astfel ca, acționând în sensul dorit asupra lor, să reușim atingerea dezideratului de înaltă disponibilitate pentru sistemul de securitate.

Foarte multe companii producătoare de sisteme sunt preocupate, la ora actuală, de crearea unei înalte disponibilități pentru sistemele lor, mai mult decât de intervalul de timp în care sistemul funcționează fără defecte, fapt care este în strânsă legătură cu fiabilitatea sistemului. Ca atare, viteza cu care un sistem poate fi reparat devine o parte critică a proiectării de sistem.

Viteza de reparare poate afecta dramatic disponibilitatea sistemului în cauză. În conformitate cu definiția disponibilității, ea poate fi aproximată ca raport între intervalul de timp în care sistemul este funcțional și intervalul total de timp scurs din momentul inițial, la care sistemul a fost pus în funcțiune. Cu alte cuvinte, disponibilitatea este procentul de timp în care sistemul este disponibil să-și execute funcțiile. De exemplu, dacă un sistem este pus în funcțiune la momentul inițial $t = 0$, el va funcționa corect o perioadă de timp (t_o), după care se va defecta, necesitând o reparare ce va dura un interval de timp t_r. Disponibilitatea la momentul t, va fi:

$$A(t) = \frac{t_o}{t_o + t_r}, \text{ unde } t = t_o + t_r \qquad (1)$$

Această relație se pretează la determinarea experimentală a disponibilității unui sistem. Din păcate, evaluarea experimentală a disponibilității este, adeseori, imposibilă din cauza timpului și costului implicat de această operațiune. Pe de altă parte, este util să existe un mijloc de estimare a disponibilității, înainte ca sistemul să fie

produs, astfel ca măsurile de creştere a disponibilităţii să poată fi implementate încă din faza de proiectare a sistemului. În literatura de specialitate [4], sunt prezentate două metode pentru estimarea disponibilităţii. O primă metodă se bazează pe o singură măsură parametrică, cum ar fi timpul mediu de funcţionare înainte de prima cădere (*Mean Time To Failure* – MTTF) şi timpul mediu de reparare (*Mean Time To Repair* – MTTR), şi furnizează aşa numita disponibilitate stare constantă (*steady-state availability* – A_{ss}), iar cea de-a doua metodă utilizează modelul Markov.

MTTF este intervalul de timp socotit între momentul punerii în funcţiune al sistemului şi până la momentul apariţiei primei căderi. De exemplu, dacă avem N sisteme puse în funcţiune la momentul t = 0 şi măsurăm timpul cât funcţionează fiecare dintre ele până la prima cădere (t_i cu i = 1,…,N), media acestor timpi va fi tocmai MTTF:

$$MTTF = \frac{\sum_{i=1}^{N} t_i}{N} \tag{2}$$

Timpul MTTF, poate fi calculat determinând valoarea presupusă (probabilă) a momentului primei căderi. Ca urmare, MTTF va avea următoarea expresie:

$$MTTF = \int_0^{\infty} t \cdot f(t)dt \tag{3}$$

unde f(t) este funcţia de densitate a căderilor, ea fiind definită pe intervalul de la 0 la ∞ deoarece această funcţie este nedefinită pentru t<0. În urma calculelor se obţine:

$$MTTF = \int_0^{\infty} R(t) \cdot dt \tag{4}$$

Relaţia de mai sus este satisfăcută pentru orice funcţie de fiabilitate, care satisface relaţia $R(\infty) = 0$. Dacă funcţia de fiabilitate respectă legea exponenţială a căderilor, atunci $R(t) = e^{-\lambda \cdot t}$, şi după calcule se obţine:

$$MTTF = \frac{1}{\lambda} \tag{5}$$

Cu alte cuvinte, timpul mediu de funcţionare a unui sistem, până la prima cădere MTTF, este inversul valorii ratei căderilor a sistemului. În acest caz, se poate calcula fiabilitatea sistemului chiar la momentul de timp egal cu MTTF, care va fi:

$$R(MTTF) = R\left(\frac{1}{\lambda}\right) = e^{-\lambda\left(\frac{1}{\lambda}\right)} = e^{-1} = 0{,}3678 \tag{6}$$

Conform acestui rezultat, un sistem ce respectă legea exponenţială a căderilor, are probabilitatea de a nu suferi o cădere înainte de scurgerea intervalului de timp egal cu MTTF, egală cu 0,3678.

Timpul mediu de reparare – MTTR – este, de fapt, timpul mediu necesar pentru repararea sistemului şi, practic, este dat de suma următorilor trei timpi:

- timpul necesar localizării defectului;
- timpul necesar reparării propriu-zise;
- timpul necesar reconectării sistemului.

Practica dovedeşte clar că procentul cel mai mare de timp (din total MTTR), este consumat cu operaţiunea de localizare a defectelor. Estimarea intervalului de timp necesar reparării sistemului (MTTR) este foarte dificilă. Acest timp poate fi determinat experimental, prin elaborarea unui set de defecte, „injectarea" lor, pe rând, în sistem şi, apoi, măsurarea timpului de reparare pentru fiecare defect în parte. În final, se va face media timpilor de reparare pentru fiecare defect în parte, determinând, astfel, timpul MTTR.

Astfel, dacă avem un set de N defecte şi defectul „i" reclamă un timp de reparare t_i atunci MTTR va fi dat de expresia:

$$MTTR = \frac{\sum_{i=1}^{N} t_i}{N} \tag{7}$$

Bineînţeles, determinarea lui MTTR poate fi mai exactă, introducând un factor de corecţie în relaţia de mai sus, ce ţine cont de abilitatea de reparare a mai multor persoane.

Astfel, dacă reparaţiile impuse de către setul celor N defecte sunt făcute de către M persoane, fiecare dintre ele reparând sistemul într-un timp mediu $MTTR_i$, atunci MTTR final va fi media acestor timpi medii individuali:

$$MTTR = \frac{\sum_{i=1}^{M} MTTR_i}{M} \tag{8}$$

Timpul MTTR este, de obicei, specificat prin termenul de rată a reparaţiilor μ, care este media numărului de reparaţii necesare, într-o anumită perioadă de timp. Legătura între cele două mărimi este:

$$MTTR = \frac{1}{\mu} \tag{9}$$

Bazat pe definirea anterioară a timpilor MTTF şi MTTR, se poate spune că, în medie, un sistem funcţionează un număr de MTTF ore până când apare prima cădere. După această cădere, sistemul va necesita un număr mediu de MTTR ore pentru reparare. Mai departe, sistemul va funcţiona din nou până la prima cădere şi ciclul se repetă.

Pentru un sistem ce suferă N căderi pe parcursul duratei de viaţă, timpul total cât el este operaţional va fi de $(N+1)\cdot MTTF$ ore, iar timpul cât el este în reparaţie va fi $N \cdot MTTR$ ore. Având în vedere relaţia (1), se poate scrie expresia disponibilităţii ca fiind:

$$A_{SS} = \frac{(N+1)\cdot MTTF}{(N+1)\cdot MTTF + N \cdot MTTR} \tag{10}$$

Introducând în relaţia (3) expresiile obţinute pentru timpii medii MTTF şi respectiv MTTR, se obţine disponibilitatea sistemului:

$$A_{SS} = \frac{(N+1)\cdot \frac{1}{\lambda}}{(N+1)\cdot \frac{1}{\lambda} + N \cdot \frac{1}{\mu}} \tag{11}$$

După efectuarea calculelor, expresia finală a disponibilităţii va fi:

$$A_{SS} = \frac{1}{1 + \frac{\lambda}{\mu} \cdot \frac{N}{N+1}} \tag{12}$$

unde μ reprezintă rata reparaţiilor şi este exprimată în reparaţii pe oră, iar rata căderilor λ este dată în căderi pe oră. Interpretarea relaţiei (12) arată că, dacă rata căderilor este 0 (adică sistemul nu are căderi niciodată) sau, altfel spus, dacă rata reparaţiilor tinde la ∞ (adică sistemul nu necesită timp pentru reparare (MTTR=0)), disponibilitatea sistemului va fi 1, ceea ce corespunde realităţii.

Referitor la relaţia (12) obţinută pentru disponibilitate, este de remarcat faptul că aceasta diferă faţă de aceeaşi relaţie prezentată în literatură [4], prin termenul suplimentar care apare la numitorul expresiei $\left(\frac{N}{N+1}\right)$ şi a cărui influenţă, consider că trebuie luată în calcul. Aceasta implică faptul că aplicarea relaţiei (12) conduce la o disponibilitate mai mare decât cea obţinută prin aplicarea relaţiei din literatură conform [4]. De fapt, după cum se observă din relaţia (12), influenţa acestui factor este mai pronunţată în sensul creşterii disponibilităţii, în cazul sistemelor ce suferă un număr de căderi (N) de valoare mică pe parcursul duratei de viaţă, această situaţie fiind caracteristică sistemelor de înaltă fiabilitate.

Pe de altă parte, rata reparaţiilor, μ, este un parametru important al atributului de întreţinere a sistemului. Inversul ratei reparaţiilor este timpul MTTR, care, după cum s-a văzut, este timpul mediu necesitat pentru executarea unei singure reparaţii.

În cadrul [3], au fost definite atributele de fiabilitate, disponibilitate, întreţinere, testare, siguranţă, drept măsuri utilizate pentru cuantificarea conceptului de dependenţă ce reprezintă, în final, calitatea serviciilor furnizate de către un sistem dat. Din definiţiile atributelor menţionate, se observă că între ele există legături intime, influenţându-se reciproc. De exemplu, întreţinerea înaltă a unui sistem, reclamă un scurt interval de timp necesar reparării lui. Prin reparare se înţelege localizarea defectului, reparaţia fizică propriu-zisă şi reconectarea sistemului. Întreţinerea unui sistem, este crucială [4], când viaţa umană, clădirile sau mediul înconjurător, sunt puse în pericol pe perioada cât sistemul este în reparaţie. „Căderea" unui sistem de securitate, se încadrează perfect în această situaţie, deci se impune pentru sistem, o întreţinere înaltă, adică un timp de reparare foarte scurt, care, după cum s-a văzut anterior, influenţează disponibilitatea în sens pozitiv. Pe de altă parte, creşterea posibilităţii de testare unui sistem se concretizează în creşterea puterii de detecţie şi de localizare a defectelor. Din acest punct de vedere, gradul de testare a unui sistem influenţează în mod direct întreţinerea sistemului, deoarece, după cum se ştie, din totalul timpului de reparare, procentul major de timp este consumat cu localizarea defectelor.

Iată cum creşterea gradului de testare a unui sistem, influenţează, prin intermediul întreţinerii acestuia, creşterea gradului de disponibilitate a sistemului. Pe de altă parte, relaţia obţinută pentru disponibilitate arată clar că, prin creşterea fiabilităţii (scăderea lui λ), are ca efect creşterea disponibilităţii sistemului.

Pe de altă parte, în cadrul lucrării [4], se indică drept soluţie potenţială de creştere a disponibilităţii unui sistem, utilizarea unui procesor suplimentar (în particular, cu referire la procesorul unităţii de control), care să fie utilizat ca rezervă, adică, atunci când procesorul primar se defectează, funcţionarea sistemului să fie asigurată de către procesorul suplimentar.

În acest mod, procesorul suplimentar este, de fapt, într-o fază de aşteptare permanentă a momentului de timp (defectarea procesorului primar), când trebuie să asigure funcţionarea sistemului, aceasta fiind, de fapt, cea mai comună măsură de creştere a disponibilităţii unui sistem.

Această soluţie potenţială, pentru creşterea disponibilităţii, va trebui racordată la deziderateleleile fundamentale ale unui sistem de securitate astfel ca, soluţia finală, adoptată pentru atingerea dezideratului de înaltă disponibilitate, să nu compromită în nici un fel, funcţii vitale (prezentate anterior), specifice sistemelor de securitate.

4. Clase de disponibilitate ale sistemelor de securitate

În literatura de specialitate [1], disponibilitatea sistemului de transmisie a alarmelor este determinată de intervalul de timp, pe durata căruia se ştie că sistemul este disponibil să transmită starea unei alarme la centrul predeterminat de recepţie a alarmelor; transmisia trebuie să se facă fără corupere şi în marja de întârziere a alarmelor permisă şi, când este cazul, să transmită un mesaj (de exemplu, o recunoaştere).

Când există mai mult de o interfaţă la sistemul de transmisie a alarmelor, sistemul de transmisie va fi considerat disponibil în cazul unui defect ce afectează una sau mai multe asemenea interfeţe, cu condiţia să existe cel puţin o cale de transmisie între o interfaţă la sistemul de alarmă şi centrul de recepţionare a alarmelor, în condiţiile când:

- fie semnalele sunt transmise şi recepţionate normal la toate interfeţele,
- fie semnalele sunt transmise şi recepţionate normal la o interfaţă primară de la fiecare capăt, iar, în cazul unei căderi, sistemul comută automat la o interfaţă secundară.

Timpul pentru care sistemul de transmisie va fi considerat disponibil va fi dat de perioada de la ultimul moment când sistemul s-a ştiut că este disponibil (adică fără defecte), până la momentul când este detectat un defect şi sistemul este reparat şi testat.

Pentru fiecare defect, se va considera perioada minimă de indisponibilitate de 15 min. Nu vor fi incluse defectele cauzate de încercări deliberate de compromitere a sistemului.

În cadrul lucrării [1] sunt specificate 5 clase de disponibilitate pentru sistemele de securitate, disponibilitatea lunară fiind cuprinsă între 75% şi 99,95%, iar disponibilitatea în orice perioadă de 12 luni fiind cuprinsă între 97% şi 99,99% corespunzător claselor menţionate. Este evident că, pentru obţinerea unei disponibilităţi ridicate – peste 98% (clasele 4 şi 5), se impune duplicarea părţilor comune ale sistemului.

5. Implementarea pentru testare a sistemelor de securitate

După cum se poate observa din analiza întreprinsă până la acest punct, există o paletă largă de tehnici menite a creşte disponibilităţii unui sistem. Astfel, structura finală a sistemului de securitate reclamă acoperirea mai multor direcţii: testare, fiabilitate, protecţie la acces neautorizat, protecţie *buffer* de evenimente şi, nu în ultimul rând, păstrarea dezideratelor fundamentale ale unui sistem de securitate [2].

Pentru soluţionarea problemelor menţionate propun o soluţie originală, care consider că poate răspunde favorabil la totalitatea problemele ce se cer rezolvate.

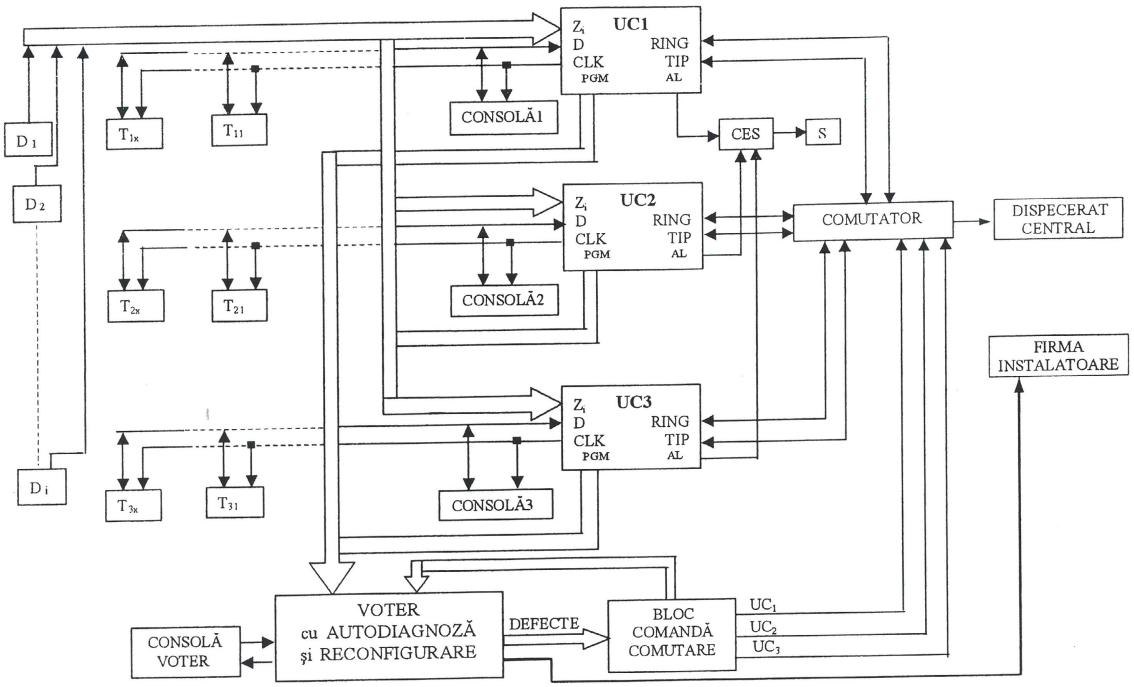

Figura 3.

Astfel, soluţia adoptată se bazează pe posibilitatea de urmărire a evenimentelor prin intermediul ieşirilor programabile ale unităţii de control. În acest sens, am optat pentru o structură redundantă statică globală, cu restabilire prin votare nodală. Structurile ce utilizează ca tehnică votarea asigură mascarea defectului astfel că ansamblul rămâne funcţional la apariţia unui defect; aceste structuri nu fac o diagnoză a defectului în sensul detecţiei şi localizării, astfel că ansamblul poate funcţiona cu un defect, dar el nu este detectat şi nici localizat ci doar mascat. Cu alte cuvinte, structura asigură creşterea fiabilităţii, dar nu şi a posibilităţii de testare. Pe de altă parte, la apariţia unui al doilea defect în cadrul ansamblului, prin votare se poate obţine un vot fals deoarece, în cadrul structurii, există deja un defect, astfel că, din acest moment, structura poate avea funcţionare defectuoasă.

Aceste aspecte m-au determinat să nu consider potrivită soluţia de votare simplă, ci să o combin cu o soluţie de diagnoză, care să asigure detecţia şi localizarea primului defect apărut în cadrul structurii, apoi să izolez defectul (reconfigurare) şi să invalidez procesul de votare (până la reparare) deoarece nu mai există un criteriu acceptabil de votare după apariţia primului defect. Astfel, după apariţia primului defect, nu se mai face votare, ci doar detecţie pentru cel de-al doilea defect potenţial, nemaiputându-se face, însă, localizare lui. În cadrul figurii 3, este prezentată structura adoptată, pe care, ţinând cont de funcţiile ce le realizează, am denumit-o structură redundantă statică globală, cu autotestare şi reconfigurare la defect.

Structura adoptată are în vedere cele precizate referitor la ipoteza defecţiunilor independente, fiind configurată în acest sens. Pentru respectarea acestui deziderat important, unităţile de control trebuie să fie complet independente, fiecare cu consolă sistem proprie, şi, dacă este cazul ca sistemul de securitate să conţină şi terminale de operare amplasate de-a lungul clădirii, acestea se vor tripla. Ansamblul adoptat are în componenţa sa 3 unităţi de control complet separate, cu console proprii, elementele de detecţie din teren furnizând semnalele simultan, la cele trei unităţi de control. Aceste semnale furnizate de elementele de detecţie se pot urmări prin intermediul ieşirilor programabile de tip PGM [5] [6], care, în acest mod, vor urmări evenimentele din sistem. În funcţie de cerinţele de testare, ieşirile PGM pot înregistra evenimente de pe un sector de risc sau de pe mai multe sectoare de risc, astfel că se pot forma vectori de test, care reprezintă, de fapt, o semnătură detaliată sau comprimată a evenimentelor din cadrul sistemului.

Cele trei unităţi de control utilizate, UC1, UC2, UC3, au ieşirile de alarmă (RING, TIP), conectate prin intermediul unui comutator electronic la linia telefonică, în vederea transmiterii codificate a mesajelor de alarmă [5] [6] către dispeceratul central şi, totodată, se permite accesul firmei instalatoare pentru operaţiunile de *downloading / up-loading* [5]. La un moment dat, numai una din unităţile de control este conectată la linia telefonică şi anume, o unitate considerată bună. În momentul în care este identificat un defect la unitatea conectată la linia telefonică (unitatea curentă), bazat pe ieşirile PGM, ce constituie intrări pentru voterul cu autodiagnoză şi reconfigurare (VAR), acesta va fi detectat şi localizat, iniţiindu-se proceduri de reconfigurare prin sinteza de către blocul de comandă comutare (BCC) a semnalelor de defect, care va furniza, totodată, şi semnalele UC_1, UC_2, UC_3, necesare comutatorului electronic pentru comutarea liniei telefonice de pe unitatea de control identificată cu defect, pe o unitate de control fără defect. O problemă ridicată de structura adoptată este legată de faptul că acest ansamblu trebuie, mai întâi, să facă detecţia şi localizarea defectului şi numai după aceea să facă comutarea liniei telefonice în situaţia că la unitatea curentă a apărut un defect. Dacă nu este identificat defect, nu se va comanda comutarea de pe unitatea curentă. Acest mod de lucru reclamă alocarea unui interval de timp necesar procesului de votare, timp în care informaţia ce trebuie transmisă pe linie telefonică trebuie să fie păstrată şi, apoi, după terminarea procesului de votare, transmisă de către o unitate de control certificată funcţional.

Ţinând cont de destinaţia semnalelor transmise pe linia telefonică şi anume dispeceratul central de intervenţie la pericol, precizez că o întârziere de ordinul secundelor, introdusă în transmiterea semnalelor de alarmă către acesta, nu prezintă nici un fel de impediment (unităţilor de intervenţie fizică ale dispeceratelor centrale le sunt necesare intervale de timp minime, cuprinse între 15 – 25 min., în cel mai fericit caz). Astfel, o întârziere de ordinul secundelor în transmiterea alarmelor către dispecerat este nesemnificativă faţă de timpul de intervenţie necesar, fiind, de fapt, mult mai important ca spre dispeceratul central să nu ajungă semnale de la unităţi de control cu defecte ceea ce însemnă mesaje eronate, adică aşa numitele alarme false. În acest mod (prin întârzierea acordată procesului de diagnoză), se reuşeşte atingerea unui alt deziderat major al sistemelor de securitate, concretizat în reducerea posibilităţilor de transmitere a alarmelor false (ca urmare a defectelor de UC), problemă foarte importantă deoarece orice mesaj de alarmă către dispecerat reclamă intervenţie fizică care implică personal înarmat şi, respectiv, mijloace de transport, iar, în cazul alarmelor false, deplasarea în vederea intervenţiei este de fapt inutilă. Această problemă a întârzierii în transmiterea mesajelor, în cadrul unităţilor de control, se poate rezolva foarte simplu cu ajutorul funcţiei „*Transmission Delay*" [5], care realizează tocmai o întârziere programabilă a mesajelor transmise către dispeceratul central. Întârzierea ce poate fi introdusă este cuprinsă între 1 şi 255 secunde.

Analiza soluţiei adoptate prin prisma cerinţelor enunţate evidenţiază avantajele şi oportunităţile create prin adoptarea acestei structuri originale, iar prin testarea ei, în condiţii de laborator, s-a obţinut disponibilitatea calculată a acestui sistem pe o perioadă de 12 luni – conform relaţiei (1):

$$A = \frac{360 - 2}{360} = \frac{358}{360} = 0{,}994$$

Deci, practic, durata totală a reparaţiilor necesitate de sistem pe parcursul a 12 luni a fost de 48 de ore, sistemul încadrându-se, din acest punct de vedere, în clasa 4 de disponibilitate – conform [1].

Prin rezervarea introdusă la nivelul unităţilor de control, activitatea de reparare nu mai produce indisponibilitatea sistemului deoarece, la apariţia unui defect, funcţionarea va fi asigurată de cele două rezerve bune, iar dacă repararea întârzie până la apariţia defectului următor (la a doua UC), se poate comuta pe ultima unitate de control bună, astfel că se asigură în continuare timp necesar procesului de reparare. Remarc cu toate acestea că, atunci când la structura adoptată (cele trei UC) apare primul defect, sistemul de securitate va funcţiona în continuare, dar este de dorit ca repararea unităţii defecte să fie făcută cât mai rapid şi unitatea să fie repusă în cadrul ansamblului funcţional pentru refacerea criteriului de vot al ansamblului.

Din punct de vedere funcţional al unui sistem de securitate, ansamblul adoptat va trebui să realizeze aceleaşi funcţii, ca şi în cazul în care există o singură unitate de control, şi acest lucru este perfect posibil cu privire la toate funcţiile. Din punct de vedere al regimului de armat /dezarmat (*arming/disarming*), ansamblul trebuie să funcţioneze unitar adică toate UC armate sau toate UC dezarmate. Acest deziderat se poate realiza manual, de la consola fiecărei unităţi de control, sau automat, prin utilizare funcţiei "*Automatic Arming*" [5], şi, respectiv, interacţiuni create, bazate pe funcţia „*Momentary Keysswitch Arm Zone*" [5].

6. Concluzii

Analiza întreprinsă până la acest nivel, a permis formularea următoarelor concluzii:

1. sistemele de securitate sunt prerecuzite, esenţiale pentru funcţionarea fiabilă şi eficientă a măsurilor de asigurare a vieţii, a protecţiei clădirilor, valorilor, informaţiilor şi, respectiv, a mediului înconjurător;
2. integrarea completă a sistemelor de detecţie şi protecţie a pericolului într-un sistem gazdă de management al clădirii, impune condiţii de securitate adiţionale, şi nu este recomandată datorită disponibilităţii ridicate pe care trebuie să o aibă un sistem de securitate;
3. un sistem de securitate reclamă, prin natura sarcinilor sale, o înaltă disponibilitate deziderat pentru a cărui realizare se impun, mai departe, măsuri ferme în direcţia creşterii posibilităţii de testare şi fiabilităţii nivelurilor componente ale sistemului de securitate. În acest sens, este dată o soluţie de implementare a sistemelor de securitate ce să asigure un grad ridicat de testare şi o limitare a vulnerabilităţii unor asemenea sisteme;
4. în primul rând, voterul adoptat fiind de fapt o unitate de control cu consolă proprie, el este perfect compatibil cu structura unui sistem de securitate astfel că operaţiunile reclamate la nivel de operator sistem, după cum s-a constatat, nu sunt diferite faţă de modul actual de operare astfel că ansamblul propus nu reclamă o instruire specială, care înseamnă de fapt costuri suplimentare. Din punct de vedere energetic, voterul astfel realizat, are autonomie energetică fiind de fapt o unitate de control;
5. experienţa practică dobândită prin realizarea unui număr mare de sisteme de securitate mi-a demonstrat că ponderea în preţul final al unităţii de control pentru un sistem complex este de aproximativ 10-15%. Aceasta înseamnă că, pentru implementarea structurii propuse, se ajunge la o majorare a preţului final cu aproximativ 20-23% - procent care justifică din plin aplicarea soluţiei propuse mai ales în cazul sistemelor de securitate cu complexitate ridicată.

Bibliografie

1. **CERBERUS AG**: Danger Management System, Switzerland, 1992.
2. **POPESCU C.:** Teza de doctorat: Contribuţii privind creşterea testabilităţii şi fiabilităţii sistemelor de securitate, Timişoara, 2001, 267p.
3. **POPESCU C., POPESCU D.E.:** Fiabilitatea şi testarea sistemelor, Editura Matrix Rom., Bucureşti, 2000, 280p. ISBN 973-685-299-9.
4. **JOHNSON, B.,W.:** Design and Analysis of Fault Tolerant Digital Systems, Addison-Wesley Series in Electrica Land Computer Engineering, New York, 1989, 583p.
5. * * * Digital Security Controls Ltd.: Panel Control PC5010 – Installation Manual, Canada, 1998, 70p
6. * * * Digital Security Controls Ltd.: Panel Control PC5010 – Programming Worksheets, Canada, 1998, 69p.