CURS

Tehnician pentru sisteme de detecție, supraveghere video, control acces

Cod COR: 313210

2010

CUPRINS

ASOCIAȚIA ROMÂNĂ PENTRU TEHNICA DE SECURITATE
BUCUREȘTI, Sector 6
Splaiul Independenței 319
O.B. 152 Etaj 2

www.arts.org.ro

SECURITATEA INDUSTRIALA
DEFINIRE, IMPLEMENTARE, MENTENANTA CONTINUA

- suport de curs adresat **tehnicienilor pentru sisteme de detecție, supraveghere video, control acces** -

CUPRINS

1. Noţiuni fundamentale privind securitatea

1.1. Ameninţare, vulnerabilitate, risc

Activităţile umane, economice, sociale, viata în colectivitate sau procesele naturale se caracterizează prin existenta unor interacţiuni, între subiect şi mediu, de la griji, preocupări, până la probleme interne sau externe, presiuni ori chiar atacuri. Oricare entităţi sau procese pot fi supuse unor ameninţări de diferite naturi, care, dacă nu sunt luate în considerare şi contracarate prin măsuri adecvate, pot conduce la evenimente nedorite, unele cu consecinţe foarte grave pentru integritatea corporală, viaţa oamenilor şi desfăşurarea activităţilor datorită manifestării interacţiunilor respective. Logic, se pune problema protecţiei bunurilor, valorilor, integrităţii şi vieţii persoanelor, precum şi a clădirilor, proceselor sociale, economice, de mediu etc; pe durata acestui curs, pentru toate aceste entităţi vom utiliza termenul de **obiectiv**.

De cele mai multe ori, interacţiunile sau atacurile nu sunt clare, iminente, palpabile, cunoaşterea şi evaluarea lor reprezentînd o chestiune de experienţă, pregătire şi specializare.

In acest sens, se poate defini **ameninţarea** ca *fiind un pericol potenţial, ce trebuie evidenţiat funcţie de natura obiectivului protejat şi de caracteristicile mediului din care acesta face parte şi care, dacă se concretizează, poate produce consecinţe defavorabile*. Evaluarea ameninţării se face printr-un studiu al intenţiilor şi capabilităţilor adversarilor potenţiali, al caracteristicilor mediului. Trebuie subliniat la această noţiune faptul că este un element acţional, intern sau extern , cu manifestare potenţială.

De ce “au succes “ ameninţările ? Pentru că, obiectul sau procesul în discutie, pe care ne interesează să-l protejăm, prezintă anumite caracteristici constructive sau funcţionale, din categoria slăbiciuni sau fisuri. ***Vulnerabilitatea*** *reprezintă ansamblul de elemente proprii, intrinseci, specifice obiectului sau procesului de protejat*, *care pot fi exploatate de acţiuni (ameninţări) şi pot conduce, de asemenea, la consecinţe defavorabile.*

Manifestarea simultană a acţiunilor din categoria “ameninţări”, corelată cu existenţa unor “vulnerabilităţi“ poate avea loc mai mult sau mai puţin frecvent, iar consecinţele defavorabile pot fi de la “neplăcute” până la “dezastruoase”. Caracterizarea acestui fenomen poartă numele de risc.

Prin ***risc*** se înţelege, aşadar, *probabilitatea de a se produce şi capabilitatea de a înfrunta un pericol, o situaţie neprevăzută sau de a suporta o pagubă, un eşec în acţiunea întreprinsă.* Sau, altfel spus, *riscul poate fi considerat o evaluare a probabilităţii ca o ameninţare să folosească cu succes o vulnerabilitate şi să producă consecinţe defavorabile.*

Se observă, cu acest prilej, diferenţa dintre noţiuni, riscul fiind o măsură, un element analitic, de evaluare a situaţiei unui obiectiv de protejat.

Ordonarea valorii riscului pe o scală se face în funcţie de caracteristicile obiectivului, de rolul său într-o anumită entitate şi de importanţa acestuia. Aşa cum se vede în Fig. 1., unde am prezentat o scală de la 0 la 5, de regulă, riscurile producerii unor evenimente de tip “dezastru” sunt asociate cu probabilităţi reduse de manifestare.

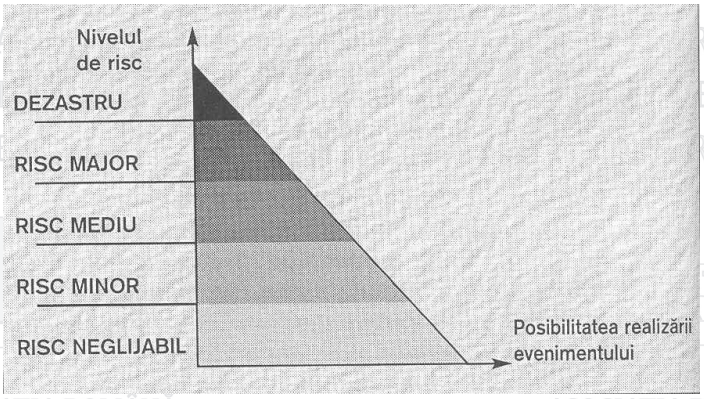


Fig. 1. *Ierarhizarea valorilor de risc*

Relația formală, principială, de calcul al riscului este: R = P x C,
unde:

- P reprezintă *probabilitatea* de producere a evenimentelor de securitate
- C este evaluarea *consecințelor* produse ca urmare a manifestărilor evenimentelor de securitate.

Din această relație rezultă că *riscul poate fi ridicat atunci când, fie probabilitatea de producere a pericolului este mare, fie când, în cazul producerii unui pericol, consecințele sunt pronunțat negative, dar este sigur ridicat când ambii factori sunt mari*.

In cazul unor activități generale, umane, evenimentele probabile şi consecințele producerii lor pot fi încadrate în categoriile din tabelele de mai jos:

Tabelul 1

PROBABILITATEA (P)		
Nivelul	**Probabilitatea**	**Frecvența de apariție a evenimentului**
5	Permanent	1 eveniment/zi
4	Frecvent	1 ev. la 10 zile
3	Probabil	1 ev. la 100 zile
2	Puțin probabil	1 ev. la 1000 zile
1	Aproape improbabil	1 ev. la 10.000 zile

CONSECINȚELE (C)	
Nivelul	**Consecințele**
5	Dezastruoase
4	Foarte mari
3	Mari
2	Moderate
1	Neglijabile

RISCUL (R = PxC)		
Rezultatul conjuncției	**Valoare risc**	**Clasificare risc**
20 – 25	5	Dezastru
10 – 19	4	Major
5 – 9	3	Mediu
2 – 4	2	Minor
1	1	Neglijabil

Din parcurgerea tabelelor de mai sus nu trebuie să ne imaginam că un eveniment încadrat drept "probabil", situat pe nivelul 3, are, implicit, consecințe aşezate pe nivelul 3 (mari) şi valoarea riscului va fi tot 3. Evaluarea riscului este o activitate deosebit de complexă şi de mare răspundere, care poate fi îndeplinită numai de persoane calificate special pe acest domeniu.

Rezultatul determinării riscului este necesar pentru stabilirea, de comun acord cu proprietarul/ beneficiarul obiectivului de protejat, a strategiei față de risc şi anume:

- **acceptarea** (tolerarea) - față de riscurile neglijabile şi de o mică parte a celor minore, care, dacă s-ar produce, ar determina pagube suportabile
- **reducerea selectivă -** față de riscurile minore, medii şi o mică parte a celor majore şi ar consta în adoptarea unor măsuri preventive care să reducă posibilitatea producerii evenimentelor nedorite şi utilizarea unor tehnici şi proceduri adecvate de reducere a consecințelor acestora
- **asigurarea -** se adoptă obligatoriu față de riscurile dezastruoase şi o parte a celor majore, pentru care măsurile de securitate proprii ar fi prea costisitoare sau prea complexe şi din aceste cauze aceste riscuri sunt inacceptabile.

Figura 2 prezintă asocierea uzuală a atitudinii față de risc:

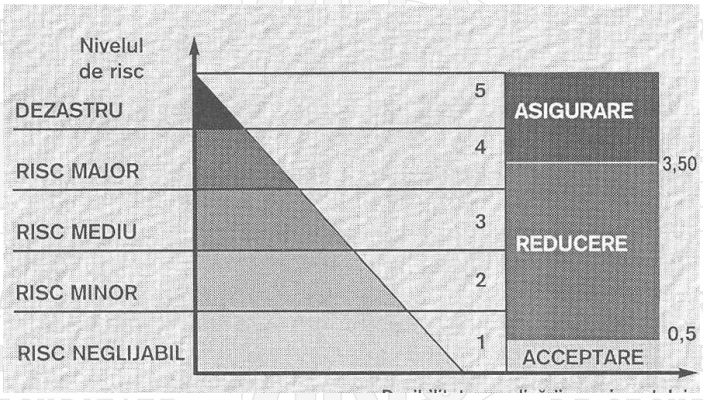


Fig. 2 *Atitudinea față de risc*

Alegerea scalei de reprezentare a valorii riscului aparţine specialistului în analiza de risc şi ea depinde de importanța şi criticitatea specifice obiectivului /procesului de protejat.

1.2. Conceptul de securitate

Într-o lume în care nesiguranța şi instabilitatea ating numeroase aspecte ale vieții cotidiene (familiale, sociale, economice, politice, militare ş.a.), acțiunile practice pentru obținerea regimului normal de funcționare pentru o entitate sau obiectiv au fost asociate cu eforturi teoretice susținute pentru definirea şi implementarea unor noi concepte în materie. Ca element de caracterizare a calității unui sistem, *securitatea este capacitatea sistemului de a-şi conserva caracteristicile funcționale sub acțiunea unor factori distructivi care ar putea să-l transforme în pericol pentru mediul înconjurător şi viața oamenilor aflați în zona de risc ori să provoace pagube materiale, informaționale sau morale.*

Elementele fundamentale ale securității sunt:

- siguranța - capacitatea de a rezista la atacuri
- stabilitatea - capacitatea de a funcționa într-o plajă de parametri ce îi conferă calitate şi de a permite revenirea în limitele prescrise în situația producerii unor perturbații interne sau externe.

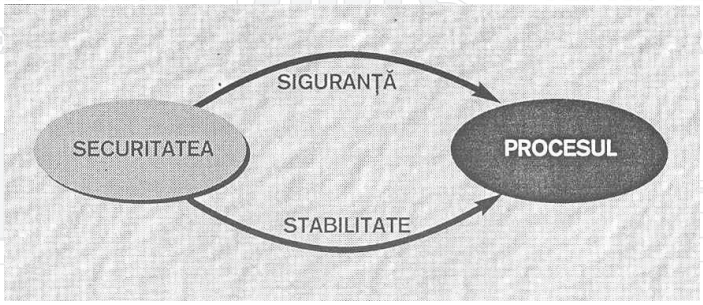


Fig. 3 *Elementele fundamentale ale securității*

Practic, noțiunea de securitate, poate fi echivalată cu "absența pericolului", chiar dacă acesta există, dar manifestarea lui nu va produce consecințe defavorabile obiectivului în discuție.

Cu titlu de informație adițională, în funcție de mediul în care ne situăm, putem vorbi despre

- securitate familială
- securitate urbană
- securitate socială
- securitate economică
- securitate energetică
- securitate industrială
- securitate națională, etc.

Dacă ne referim la conceptul în sine şi la gradul de acoperire a cerinţelor de securitate avem în vedere noţiunile:

- securitate suficientă
- securitate totală
- securitate deplină
- securitate maximală
- securitate minimală
- securitate vitală
- securitate obligatorie, ş.a.

Ca subiect principal al acestui text, menţionăm că **securitatea industrială** este *capacitatea sistemelor de protectie, ataşate proceselor economice derulate de entităţile juridice de interes public şi de societăţile comerciale de interes privat, de a asigura continuitatea derulării acestora în condiţiile confidenţialităţii complete a patrimoniului de informaţii încredinţat*. Din punct de vedere juridic, **securitatea industrială** *reprezintă sistemul de norme şi măsuri minimale care reglementeaă protecţia informaţiilor clasificate în domeniul activităţilor contractuale* (vezi Legea 182/2002, HG 585/2002 şi HG 781/2002).

Informaţiile clasificate sunt informaţiile, datele sau documentele de interes pentru securitatea naţională, care sunt încadrate în clase şi niveluri de secretizare, în funcţie de nivelurile de importanţă şi consecintele care s-ar produce prin dezvăluirea sau diseminarea lor neautorizate. Sunt două clase de secretizare:

- *clasa informaţiilor **secrete de serviciu*** -cele a căror dezvăluire poate produce prejudicii unei persoane juridice de drept public sau privat
- *clasa informaţiilor **secrete de stat*** -sunt informaţii relevante privind securitatea naţională şi a căror divulgare poate prejudicia siguranţa naţională şi apărarea ţării.

In interiorul clasei secret de stat se atribuie trei niveluri de secretizare:

- nivelul **secret**
- nivelul **strict secret**
- nivelul **strict secret de importanţă deosebită**.

Persoanele juridice de interes privat nu au dreptul să deţină informaţii clasificate, decât ca urmare a participării la un contract economic clasificat, promovat de persoane juridice de interes public, în condiţiile reglementărilor legale în materie.

Accesul şi derularea unui proiect / contract clasificat se fac cu respectarea reglementărilor legale în materie şi, în principal, au două faze importante:

- etapa de calificare la licitaţie / cerere de ofertă şi de negociere / câştigare a contractului
- etapa de derulare efectivă a contractului.

1.3. Asigurarea securităţii

Fie şi numai din enumerarea succintă a celor de mai sus se constată că asigurarea securităţii este o activitate deosebit de complexă şi cu implicaţii în numeroase domenii de activitate umană şi social-economică, având în vedere aspecte de natură :

- juridică
- ştiinţifică
- organizatorică
- economică
- fizico-tehnologică
- informaţională.

Din punct de vedere practic, abordarea asigurării securităţii pentru un obiectiv se poate face împărţindu-l, virtual, pe acesta, în patru componente:

- *componenta fizică* - ea conţine elementele constructive, precum şi măsurile şi echipamentele

instalaţiile propuse pentru oprirea intruziunilor nedorite
- *componenta funcţională* - formată din totalitatea proceselor predominante din obiectiv la care se adaugă măsurile şi echipamentele/ instalaţiile propuse pentru asigurarea continuităţii acestor activităţi definitorii ale obiectivului
- *componenta informaţională* - compusă din echipamentele de tehnică de calcul şi programele aferente, împreună cu măsurile şi echipamentele/ instalaţiile propuse pentru asigurarea confidenţialităţii, integrităţii şi disponibilităţii informaţiile deţinute şi vehiculate
- *componenta de personal* - care se referă la cerinţele privind personalul propriu şi modul de tratare a posibililor infractori, în corelare cu măsurile şi echipamentele/ instalaţiile propuse pentru protecţia personalului obiectivului şi contracararea ameninţărilor provenite de la eventualii infractori.

Activitatea de asigurare a securităţii este una deosebit de complexă, desfăşurată de la nivelul factorilor de conducere, la specialişti şi până la nivelul întregului personal şi este cunoscută sub numele de ***managementul riscului***.

Cunoaşterea riscului duce la alegerea atitudinii corespunzătoare: tolerare, reducere raţională, sau asigurare parţială, dar singura soluţie adecvată este controlul riscului.

Principalele etape ale managementului riscului sunt:
- identificarea riscului
- evaluarea riscului
- tratarea riscului.

Evaluarea riscului este o activitate de un înalt profesionalism, care trebuie să conducă la determinarea acelei valori care să fie cât mai apropiată de situaţia obiectivului, atât din punct de vedere constructiv-funcţional, cât, mai ales, din punctul de vedere al ameninţărilor caracteristice mediului.

În literatura de specialitate este cunoscută sub numele de ***analiza de risc*** şi presupune utilizarea de instrumente dedicate. Etapele principale ale aplicării unei asemenea metode sunt :
- identificarea resurselor (bunurilor, valorilor etc)
- identificarea ameninţărilor la resurse
- cunoaşterea vulnerabilităţilor obiectivului care pot conduce la „succesul" ameninţărilor
- evaluarea impactului pe care manifestarea ameninţărilor îl poate produce
- determinarea valorii riscului

Menţionez câteva metode, cu utilizare mai frecventă:
- metoda interdependenţelor funcţionale
- metoda matricelor de risc
- metoda arborelui de defectări
- metoda diagramei Fishbone
- metoda OCTAVE
- metoda MEHARI.

1.4. Reglementări legale şi norme în materie

Principalele reglementări privind activitatea de asigurare a securităţii obiectivelor sunt cuprinse în următoarele acte normative:
- Legea 10/1995, legea calităţii în construcţii
- Legea 333/2003, privind paza obiectivelor, bunurilor, valorilor şi protecţia persoanelor
- HG 1010/2004, se referă la condiţiile tehnice de aplicare a prevederilor legii 333
- HG 1698/2005, aduce precizări la HG 1010, privind parametrii necesari pentru proiectarea şi funcţionarea sistemelor de supraveghere prin TVCI
- Legea 307/2006, privind apărarea împotriva incendiilor
- Legea 182 /2002, privind protecţia informaţiilor clasificate

- HG 585/2002, Standardele naţionale de protecţie a informaţiilor clasificate în România
- HG 781/2002, privind protecţia informaţiilor clasificate „secret de serviciu”
- Legea 677/2001, pentru protecţia persoanelor cu privire la prelucrarea datelor cu caracter personal şi libera circulaţie a acestor date.

1.5. Costurile insecurităţii

Realizarea securităţii unui obiectiv necesită resurse umane de înalt nivel, materiale şi nu în ultimul rând, resurse financiare corespunzătoare. Din cauza faptului că una din caracteristicile ameninţărilor îl constituie aspectul nevizibil, potenţial, se observă adesea reticenţă în acordarea de fonduri suficiente pentru securitate.

Din acest motiv vom prezenta succint câteva aspecte specifice.

Costul efectelor unui eveniment nedorit, *Cn*, este:

$$Cn=Cp+Ca$$

în care:

Cp = costurile primare (bunuri distruse direct ca urmare a evenimentului produs)

Ca = costurile adiacente (reparaţii sau înlocuiri de bunuri distruse, cheltuieli cu restabilirea funcţionalităţii obiectivului, a asigurării continuităţii afacerii etc).

Să presupunem cazul unei firme care prestează servicii de telefonie sau INTERNET, la care se întâmplă distrugerea serverelor cu informaţii şi programe de serviciu. Costul *Cp*, de înlocuire a echipamentelor menţionate, poate fi ridicat, dar nu excesiv. Trecând la evaluarea lui *Ca*, vom constata că activitatea de refacere a datelor despre clienţi, a situaţiilor financiar-economice, costă de câteva ori mai mult decât *Cp*, durează săptămâni sau chiar luni de zile, la care se adaugă şi pierderea credibilităţii firmei pe piaţă. În majoritatea cazurilor, costurile adiacente sunt cu câteva ordine de mărime mai mari decât costurile primare şi cu implicaţii nemateriale deosebit de supărătoare.

2. Sisteme Integrate de Securitate- SIS

2.1. Funcţiile principale ale sistemelor integrate de securitate

Multidimensionalitatea conceptului de securitate, diversitatea ameninţărilor interne şi externe obiectivului de protejat, dinamica riscurilor, a prevenţiei şi a acţiunii atât în timpul producerii unor evenimente nedorite, cât şi pentru limitarea efectelor acestora după producere determină conceperea şi realizarea unei structuri de securitate complexe şi multifuncţionale.

Complexitatea multifuncţionalităţii este determinată de caracterul mixt om-maşină al mecanismului de securitate, de diversitatea ameninţărilor şi dinamica riscului, de interactivitatea întregului proces, precum şi de necesitatea deschiderii şi a perfecţionării.

Indiferent de strategia de securitate aleasă, mecanismul (sistemul) de securitate ales trebuie să asigure integrarea funcţională, din punct de vedere al securităţii, a procesului ce trebuie protejat, pe baza reglementărilor în vigoare, într-o structură ierarhică eficientă. El este implementat procesului şi nu exclude, ci include omul, fiind format din echipamente, dar şi dintr-un set coerent de proceduri operaţionale.

În scopul asigurării condiţiilor necesare funcţionării în siguranţă şi stabilitate a obiectivului, sistemul integrat de securitate, îşi propune să îndeplinească următoarele funcţii principale:

- Să prevină accesul neautorizat în perimetru şi în zonele stabilite din interiorul acestuia;
- Să detecteze şi să evalueze încercările de pătrundere în forţă sau pe ascuns la nivelul împrejmuirii perimetrale, precum şi în zone stabilite din interiorul perimetrului;
- Să detecteze şi să semnalizeze începuturile de incendii, inundaţii şi alte pericole;
- Să coreleze şi să intercondiţioneze automat funcţionarea elementelor subsistemelor componente

în scopul realizării funcţiilor sale;

- Să pună la dispoziţia operatorilor informaţii complete privind situaţia creată;
- Să asigure detecţia incipientă a evenimentelor de securitate, transmiterea alarmelor, analiza lor, precum şi comunicarea acestora, în timp util, către forţele de intervenţie
- Să precizeze operatorilor contramăsurile ce trebuie întreprinse în fiecare situaţie;
- Să alarmeze personalul şi forţele de intervenţie fie automat, fie prin intermediul operatorilor, funcţie de procedura prestabilită în fiecare situaţie;
- Să înregistreze şi să arhiveze datele furnizate de subsistemele componente în vederea analizării ulterioare a acestora.

Pentru integrarea şi gestionarea unitară a componentelor complexe ale unui sistem de securitate s-au conceput programe software cu diferite grade de complexitate. Avantajele utilizării unei aplicaţii de management de securitate unice rezultă din posibilitatea de a realiza integrarea diverselor subsisteme din componenţa unui sistem de securitate. Pentru a asigura funcţia de integrare a sistemului, echipamentele centrale ale subsistemelor şi staţiile de lucru pentru managementul sistemului conectate în reţeaua de securitate a obiectivului sunt reunite în dispecerat.

În principiu, un sistem de complex de securitate integrează următoarele subsisteme:

- subsistemul de detecţie şi alarmare perimetrală
- subsistemul de control acces
- subsistemul de televiziune cu circuit închis
- subsistemul de detecţie şi alarmare la efracţie
- subsistemul de detecţie şi alarmare/stingere la incendii, inundaţii şi alte pericole
- subsistemul comunicaţii de securitate şi transmiteri de date
- subsistemul Dispecerat
- subsistemul electroalimentare
- alte categorii de subsisteme integrabile:
  - subsisteme de sonorizare şi adresare publică
  - poşta pneumatică
  - detecţia şi alarmarea la încercări de furt în centrele comerciale
  - sisteme de management în clădiri „inteligente”
  - subsisteme de protecţie la scurgerea informaţiilor prin radiaţii parazite
  - subsisteme de protecţie a reţelelor interne de date ale organizaţiilor faţă de accesul neautorizat (prin INTERNET) sau încercări de introducere de software cu conţinut insidios (viruşi, viermi, malware etc)
  - sisteme de securitate de tip „antitero”.

Integrarea în acest caz înseamnă că producerea unui eveniment la unul din subsistemele de supraveghere menţionate declanşează acţiuni şi în celelalte subsisteme de supraveghere şi/sau avertizare. În acest mod, pe de o parte, informaţia asupra evenimentului produs devine mai bogată, iar pe de altă parte, modalităţile de acţiune pentru înlăturarea acestuia devin mai eficiente şi mai coordonate. Sistemul de management al securităţii obiectivelor primeşte informaţii de la elementele de achiziţie de date dispuse în obiectiv, prin intermediul echipamentelor de supraveghere şi reacţionează la aceste informaţii prin emiterea de mesaje sau comenzi înapoi în zonele supravegheate din obiectiv tot prin intermediul echipamentelor de supraveghere şi/sau echipamentele de avertizare sonoră. Managementul securităţii se realizează practic prin intermediul operatorilor de la staţiile de lucru din dispecerat, care primesc mesaje de la elementele de achiziţie de date: senzori de perimetru, cititoare de cartele de acces, senzori de efracţie, camere de luat vederi, senzori de incendiu via echipamente de supraveghere: centrala de monitorizare a senzorilor de perimetru, centrale de control acces, centrale de incendiu şi sonorizare, matrice video, centrale de semnalizare la efracţie, legăturile între aceste componente făcându-se pe linie serială şi/sau pe reţea de tip *Ethernet,* pe baza protocoalelor de comunicaţie specifice fiecărui tip de echipament de supraveghere. Aceste legături fac posibilă transmiterea de mesaje, atât de la senzorii de achiziţie de date spre echipamentele de supraveghere

şi apoi la staţiile de lucru din dispecerat legate într-o reţea locală, cât şi de la staţiile de lucru din dispecerat spre echipamentele de supraveghere şi tratarea mesajelor corespunzător cu evenimentul produs şi situaţia concretă ce trebuie gestionată.

PRINCIPIILE DE BAZĂ PRIVIND CONCEPŢIA ŞI REALIZAREA SISTEMELOR DE SECURITATE

Din analiza structurii şi funcţionării sistemelor de securitate, precum şi din experienţa trecută se relevă faptul că, oricât de mare ar fi gradul de asemănare între două obiective care trebuie protejate, este evident că nu se poate aplica principiul „copy and paste" în concepţia, proiectarea şi funcţionarea SIS. Capitolul la care se înregistrează cele mai multe diferenţe este cel al ameninţărilor.

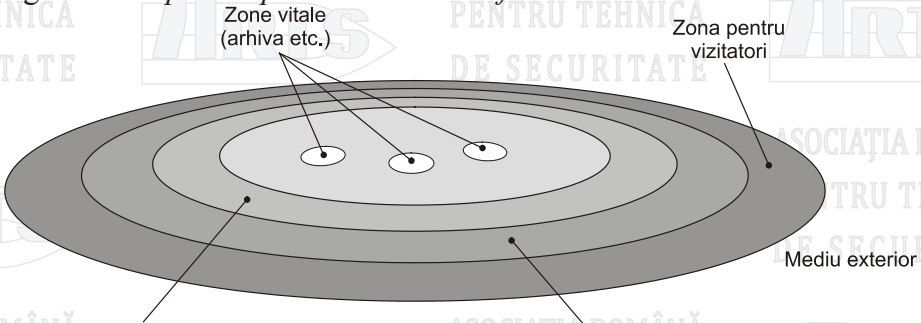
Pentru îndeplinirea obiectivului său, SIS trebuie să aibă la bază un concept deosebit, precum şi caracteristici constructiv-funcţionale, dintre care menţionez:

- să respecte principiile de realizare ale unui sistem din categoria C3I (comandă-control-comunicaţii şi informaţii)
- arhitectura de sistem să fie de tip deschis, adică să permită dezvoltări ulterioare, fără modificări ale interfeţelor existente
- sistemul să fie construit modular, pentru a facilita operaţiile de mentenanţă şi service
- structura sistemului să respecte principiul inelelor de securitate concentrice şi al protecţiei în adâncime
- pentru asigurarea tratării complete a tuturor ameninţărilor identificate în obiectiv se vor aborda, în aceeaşi concepţie şi elementele de protecţie a integrităţii corporale, a vieţii persoanelor şi sănătăţii acestora
- sistemul să asigure integrarea unitară a componentelor hardware şi software, precum şi a factorului uman (personal cu atribuţii în domeniul securităţii, personalul neimplicat al obiectivului, vizitatori etc)
- asigurarea corelării activităţilor de monitorizare cu măsurile de avertizare şi evacuare a personalului din obiectiv, în situaţiile de urgenţă
- aplicarea măsurilor de monitorizare, asigurând, în acelaşi timp, neintruziunea în viaţa privată şi respectarea confidenţialităţii datelor personale
- asigurarea redundanţei componentelor şi conexiunilor cu roluri deosebit de însemnate în funcţionarea sistemului
- efectuarea operaţiilor de back-up asupra bazelor de date operaţionale.

Preluând unele elemente ce ţin de practica şi teoria militară, se evidenţiază concepte de bază ale unui sistem de securitate, ca, de exemplu :

- protecţia în adâncime
- redundanţa elementelor vitale
- dispersarea lor în obiectiv.

Fig. 5 *Principiul dispunerii barierelor fizice*



2.1.1. Ciclul de viaţă al

sistemului de securitate

Realizarea şi funcţionarea unui sistem integrat de securitate pun în evidenţă caracterul ciclic, permanent, al activităţilor, în principal cele care reprezintă scopul pentru care a fost implementat, precum şi alte categorii de măsuri care concură la asigurarea finalităţii sistemului şi stabilităţii în funcţionare.

Principalele etape sunt:

- planificarea (care conţine: inspecţia în obiectiv, analiza de risc, elaborarea conceptului de sistem, proiectarea, instalarea, punerea în funcţiune) - **PLAN**
- derularea funcţiei principale a sistemului (utilizarea sistemului, asigurarea mentenanţei complexe) - **DO**
- controlul riscurilor (verificarea permanentă a gradului de răspuns al sistemului, în raport de cerinţele iniţiale de performanţă) **-CHECK**
- îmbunătăţirea funcţionării (adaptarea funcţionării sistemului la schimbările constructiv-funcţionale din obiectiv, precum şi la eventualele noi ameninţări care nu au fost prezente la faza iniţială. - **ACT**

Evident, ultima etapă presupune adaptarea unor elemente ale sistemului, fizice, tehnice sau operaţionale, adică revenirea la planificare şi reluarea ciclului.

2.3 Funcţiile subsistemelor

2.3.1 Subsistemul de Detecţie Perimetrală

În principiu, funcţiile unui subsistem de detecţie şi alarmare perimetrală sunt:

- detectarea încercărilor de pătrundere/ieşire frauduloasă în/din perimetrul protejat
- anunţarea operatorilor din dispecerat cu privire la tentativele de efracţie la nivelul împrejmuirii perimetrale, cu indicarea zonei în care au loc acestea
- alarmarea subsistemului TVCI în scopul atenţionării operatorilor şi comutării la afişare pe monitoarele de alarmă a camerelor video ce supraveghează zona în care se produce violarea perimetrului
- transmiterea către software-ul sistemului pentru managementul securităţii a semnalelor de alarmă/ sabotaj, oferindu-i-se acestuia controlul activării şi dezactivării zonelor de perimetru şi posibilitatea confirmării primirii semnalelor de alarmă
- dezactivarea/activarea individuală a zonelor de detecţie perimetrală pentru permiterea accesului legal, ocazional, în perimetru, cu comandă locală de la punctul de control acces sau cu comandă centrală, din dispecerat
  - dezactivarea/activarea individuală a zonelor de detecţie perimetrală în cazurile în care este necesară efectuarea de lucrări care, dacă s-ar efectua cu zonele activate, ar conduce la generarea de alarme false
  - alarmarea în timp util a forţelor de intervenţie.

2.3.2. Subsistemul de detecţie la efracţie

Mai detaliat, funcţiile subsistemului încorporat în cadrul unui sistem integrat de securitate (SIS) al unui obiectiv sunt:

- detectarea încercărilor de intruziune în zonele de securitate ale obiectivului
- semnalizarea operatorilor cu privire la tentativele de efracţie la nivelul zonelor de securitate, cu indicarea zonei în care au loc acestea
- alarmarea subsistemului de televiziune cu circuit închis în scopul atenţionării operatorilor şi comutării la afişare pe monitoare a camerelor video care supraveghează zona de securitate în care se produce evenimentul

- transmiterea către software-ul sistemului pentru managementul securității obiectivului a semnalelor de alarmă şi sabotaj, oferindu-i acestuia controlul activării şi dezactivării zonelor de securitate, posibilitatea confirmării primirii semnalelor de alarmă de către operatori şi acționării conform instrucțiunilor primite din partea sistemului pentru managementul securității
- dezactivarea individuală din dispecerat sau cu comandă locală a zonelor de securitate pentru permiterea accesului autorizat în acestea
- posibilitatea de programare/reprogramare din dispecerat a utilizatorilor, a nivelurilor de autorizare şi a codurilor de acces în vederea activării/dezactivării locale de la tastaturile amplasate lângă camerele cu destinație specială
- dezactivarea individuală a zonelor de securitate în cazul în care este necesară efectuarea de lucrări care, dacă zonele ar fi activate, ar putea genera alarme false
- alarmarea în timp util a forțelor de intervenție.

2.3.3. Subsistemul de control acces

Funcțiile subsistemului de control acces sunt următoarele:

- interzicerea accesului neautorizat al persoanelor şi vehiculelor în zonele de securitate ale obiectivului
- anunțarea operatorilor cu privire la tentativele de pătrundere neautorizată la nivelul inelelor de securitate, cu indicarea filtrului unde au loc acestea
- alarmarea subsistemului de televiziune cu circuit închis în scopul atenționării operatorilor şi comutării la afişare pe monitoare a camerelor video care supraveghează filtrul violat
- transmiterea de semnale de alarmă şi sabotaj, pe filtre, către subsistemul de detecție şi alarmare antiefracție
- transmiterea către software-ul sistemului pentru managementul securității a datelor privind accesele valide şi invalide, a semnalelor de alarmă şi sabotaj, oferind acestuia controlul filtrelor de control acces
- facilitarea obținerii de situații şi rapoarte privind prezența, circulația şi răspândirea personalului în zonele de securitate ale obiectivului
- dezactivarea automată a filtrelor de control acces la apariția de evenimente confirmate în subsistemul de detecție a incendiilor
- dezactivarea manuală a filtrelor de control acces în situații de urgență sau la nevoie.

2.3.4 Subsistemul de supraveghere prin televiziune cu circuit închis

Funcțiile subsistemului TVCI sunt:

- supravegherea video a împrejmuirii perimetrale a obiectivului şi a căilor de acces în obiectiv
- detectarea încercărilor de efracție la nivelul perimetrului prin procedeul detectării video a mişcării în zona supravegheată
- supravegherea zonei interioare dintre gard şi clădire
- urmărirea intruşilor în interiorul perimetrului
- supravegherea căilor de acces în clădire
- supravegherea unor zone din interiorul clădirii
- comutarea automată a camerelor ce supraveghează curtea şi a celor de interior (acolo unde acestea există) pe zonele de pe perimetru şi din clădire, la alarme generate de subsistemele de protecție perimetrală, antiefracție şi controlul accesului
- înregistrarea, stocarea şi arhivarea de imagini video pentru analize post-eveniment
- distribuirea imaginilor video la utilizatori conform autorizării stabilite de beneficiar.

2.3.5. Subsistemul de detecţie şi semnalizare /stingere la incendii, inundaţii şi alte pericole

Funcţiile subsistemului de detecţie şi semnalizare/stingere la incendii, inundaţii şi alte pericole sunt:

- detectarea în fază incipientă a incendiilor prin identificarea unuia sau a mai multor fenomene tipice focului, cum ar fi produşii de combustie: fumul, flăcările sau căldura
- anunţarea operatorilor cu privire la apariţia unui început de incendiu sau la declanşarea unei alarme tehnice, cu indicarea zonei în care s-a produs aceasta
- alarmarea subsistemului TVCI în scopul verificării alarmei
- declanşarea comenzilor de stingere în incintele supravegheate
- transmiterea către software-ul sistemului pentru managementul securităţii obiectivului a semnalelor de alarmă de incendiu sau alarme tehnice, oferindu-i acestuia controlul activării sau/şi dezactivării zonelor de detecţie
- dezactivarea individuală a zonelor de detecţie în cazul în care este necesară efectuarea de lucrări care ar duce la generarea de alarme false
- testarea integrală sau pe zone a subsistemului de detectare şi alarmare la incendii, inundaţii şi alte pericole
- alarmarea personalului
- la detectarea unui incendiu să poată comanda:
  - oprirea instalaţiei de ventilare
  - pornirea instalaţiei de evacuare mecanică a fumului
  - declanşarea de mesaje sonore de avertizare
  - acţionarea uşilor antifoc.
- alertarea automată a forţelor de intervenţie conform cu algoritmul prevăzut în Planul de apărare împotriva incendiilor al obiectivului
- detectarea apariţiei inundaţiilor şi alertarea forţelor de intervenţie
- monitorizarea incintelor supravegheate referitor la existenţa de substanţe toxice sau periculoase şi semnalizarea acestor situaţii .

2.3.6. Subsistemul de comunicaţii de securitate şi transmiteri de date

Subsistemul de comunicaţii poate fi format din subsisteme parţiale, profilate pe date, voce şi/ sau radio, având următoarele funcţii:

2.3.6.1. Funcţiile subsistemului de comunicaţii de securitate

- asigură transmisiile de date (secretizate) între componentele SIS, folosind echipamente active de reţea (tip switch), cu arhitectură modulară şi cabluri adecvate (fibră optică, de ex.)
- asigură redundanţa transmisiei de date prin prevederea, în arhitectura echipamentelor active de reţea, a unor module de rezervă (placă de management, surse etc.)
- asigură o lăţime de bandă corespunzătoare pentru desfăşurarea unui trafic intens de viteză şi calitate corespunzătoare
- foloseşte echipamente active de reţea care, prin standardele lor, oferă suport pentru realizarea de reţele virtuale private (VLAN – **V**irtual **L**ocal **A**rea **N**etwork), în scopul separării utilizatorilor din aceeaşi reţea, în grupuri distincte de lucru
- software-ul folosit oferă posibilitatea controlului complet al echipamentelor, precum şi o imagine fidelă a stării acestora
- asigură autentificarea utilizatorilor în reţea
- asigură protecţia reţelei de atacuri externe, în cazul interconectării cu reţeaua obiectivului protejat sau cu alte reţele, prin folosirea de echipamente hardware specializate.

2.3.6.2. Funcţiile subsistemului de comunicaţii voce

- acolo unde se impune, asigură comunicaţiile voce codificate sau secretizate între componentele SIS, folosind echipamente telefonice (centrală şi aparate telefonice), analogice sau digitale, cu facilităţi multiple şi algoritmi de criptare, care utilizează chei cu lungimi corespunzătoare
- completează funcţiile subsistemului de control acces, oferind posibilitatea convorbirilor între dispecerat şi Filtrele de Control Acces (toate sau numai cele mai importante)
- asigură interconectarea reţelei telefonice a SIS cu reţeaua telefonică a obiectivului protejat.

2.3.6.3. Funcţiile subsistemului de comunicaţii radio

- asigură o legătură la distanţă, secretizată, de rezervă, între dispecerat şi forţa de intervenţie mobilă şi unele puncte fixe importante din obiectiv
- foloseşte, pentru asigurarea legăturii, radiotelefoane fixe, mobile şi portabile în banda de frecvenţe aprobată şi modul de lucru stabilit (simplex, semiduplex alternat, duplex).

2.3.7. Subsistemul dispecerat

- Prin intermediul sistemului pentru managementul securităţii şi al operatorilor, în subsistemul dispecerat se realizează:
- concentrarea tuturor semnalelor şi imaginilor generate de senzorii şi subsistemele instalate în obiectiv
- corelarea şi intercondiţionarea automată a funcţionării elementelor subsistemelor componente în scopul realizării funcţiilor sistemului integrat de securitate
- evaluarea gradului de ameninţare în cazul unui atac
- punerea la dispoziţia operatorilor a informaţiilor complete privind situaţia creată
- precizarea contramăsurilor ce trebuie întreprinse de către operatori în fiecare situaţie
- permite generarea de comenzi şi transmiterea acestora către elementele de execuţie din obiectiv, în mod centralizat
- alarmarea personalului şi a forţelor de intervenţie fie automat, fie prin intermediul operatorilor, funcţie de procedura prestabilită în fiecare situaţie
- înregistrarea şi arhivarea datelor furnizate de subsistemele componente în vederea analizării ulterioare a acestora.

2.3.8 Subsistemul de Electroalimentare

Subsistemul de electroalimentare trebuie să asigure:
- alimentarea permanentă şi sigură a sistemului integrat de securitate
- alimentarea (de la reţea) complet separată a SIS de sistemul de electroalimentare al obiectivului protejat (alimentare de la intrarea în obiectiv), astfel ca întreruperea alimentării SIS să se producă numai atunci când cade reţeaua oraşului
- alimentarea cu surse neintreruptibile (UPS) cu puteri corespunzătoare în punctele importante ale SIS (consumatori vitali=dispecerat, camera tehnică etc.), care preiau alimentarea SIS în intervalul de timp necesar intrării în funcţiune a grupului electrogen al obiectivului (până la câteva zeci de minute, funcţie de puterea instalată)
- alimentarea echipamentelor SIS dispuse în obiectiv prin tablouri electrice separate, dispuse funcţie de răspândirea echipamentelor şi prevăzute cu elemente de protecţie diferenţială
- alimentarea neîntreruptă a echipamentelor şi cu ajutorul surselor proprii cu acumulatori sau cu surse neintreruptibile proprii.

3. Activitatea tehnicienilor pentru sisteme de detecţie, supraveghere video, control acces

3.1. Local şi rolul tehnicienilor de securitate în realizarea SIS

Deşi în titulatură este menţionat că acest curs se adresează tehnicienilor pentru ”sisteme de detecţie, supraveghere video şi control acces”, din activitatea practică s-a constatat că, în cele mai multe obiective, se întâlnesc şi alte categorii de echipamente şi sisteme de protecţie:

- detecţie, semnalizare / stingere incendii, inundaţii şi alte pericole (la centre comerciale, clădiri de birouri de înălţime mare, ş.a.)
- supraveghere şi detecţie perimetrală (la depozite, facilităţi aeroportuare şi navale etc)
- monitorizarea funcţionării sistemelor de securitate şi tratarea alarmelor
- comunicaţii de securitate şi transmiteri de date
- sonorizare şi adresare publică
- protecţia faţă de scurgerile de informaţii utile din cauza radiaţiilor parazite de la computere
- supravegherea integrităţii conductelor petroliere sau cu alte produse
- transporturile de bunuri sau valori
- protecţia informaţiilor clasificate,

în care activitatea specialiştilor sus amintiţi este strict necesară.

3.2. Principalele activităţi

Din textul prezentat în paginile anterioare compunerea şi funcţionarea unui sistem integrat de securitate înseamnă, in general :

- implementarea în obiectiv a unor categorii diverse de subsisteme de securitate, cerute de specificul obiectivului şi relevate de analiza de risc şi care sunt conţinute în proiectul de execuţie
- concentrarea semnalelor de la senzori, echipamente şi subsisteme într-o entitate centrala (cunoscută sub numele de subsistem de monitorizare, dispecerat sau control room)
- afişarea, înregistrarea şi prelucrarea primară a datelor şi informaţiilor adunate
- prelucrarea cu mijloace software speciale a informaţiilor primate
- analiza şi generare comenzi în sistem
- integrarea factorului uman (operatori, ingineri de sistem, manageri de securitate, forţe de intervenţie etc).
-

Aşa cum se observă din enumerarea succintă anterioară, la acest moment dat nu se poate vorbi despre asemenea echipamente complexe fără a sublinia rolul şi locul elementului uman.

Referitor la implicarea tehnicienilor în asigurarea funcţionării sistemului de securitate se impune menţionarea principalelor activităţi în care rolul acestora este determinant.

3.2.1. Gestionarea echipamentelor specifice

- respectarea prevederilor Legii 333/2003, privind comercializarea echipamentelor şi componentelor sistemelor de asigurare a securităţii
- la furnizarea echipamentelor către echipele de instalatori este necesar să se acorde o atenţie specială referitoare la încadrarea în clasele de mediu şi gradele de securitate, conform precizărilor standardelor SR EN 50130....50136

3.2.2. Studierea documentaţiei de execuţie a proiectului de securitate

- dacă proiectul/ contractul de implementat/ derulat este clasificat, personalul care solicită studierea documentaţiei de execuţie trebuie să fie autorizat în mod corespunzător cu clasa şi nivelul de secretizare al proiectului
- pregătirrea profesională a personalului se va face pe subsisteme şi echipamente specifice, în funcţie de cunoştinţele şi experienţa acumulate şi include:
  - ♦ verificarea şi pregătirea sculelor şi dispozitivelor necesare implementării
  - ♦ pregătirea echipamentelor auxiliare (scări, platforme ridicătoare etc)

3.2.3. Pregătirea din punctul de vedere al sănătăţii şi securităţii muncii

- verificarea stării de sănătate a personalului
- verificarea avizelor de lucru pentru condiţii grele (în exterior, lucrul la înălţime etc)
- pregătirea echipamentelor de protecţie (generale şi specifice, de exemplu măşti pentru activităţi în subsoluri sau canale)

3.2.4. Instalarea traseelor de cabluri şi a tubulaturii

Este necesar să fie subliniată necesitatea îndeplinirii prevederilor legale, conform legii 333/2003, HG 1010/2004 şi HG 1698/2005, înainte de a aborda concret activităţile de implementare a proiectului în obiectiv şi anume:

- proiectarea conform cerinţelor HG 1010/2004
- prezentarea spre avizare la serviciile abilitate ale poliţiei, de către investitor/ proprietar
- avizarea proiectului de către poliţie.

Numai după parcurgerea acestor etape se poate trece la lucrul efectiv de instalare. Mai este de subliniat faptul că, dacă contractul este clasificat, accesul în obiectiv şi începerea lucrului sunt permise doar după ce firma furnizoare primeşte, din partea ORNISS (Oficiul Registrului Naţional al Informaţiilor Secrete de Stat), Certificatul de Securitate Industrială (CSI).

Alte cerinţe specifice activităţii:

- respectarea prevederilor normativelor I18-1/2002 şi I18-2/2002
- asigurarea separării traseelor de cabluri faţă de alte categorii de instalaţii şi trasee (instalaţii sanitare, alte trasee de cureţi slabi, trasee de curenţi tari, ş.a.)
- separarea traseelor aparţinând subsistemului de securitate de alte trasee de curenţi slabi din obiectiv şi protejarea lor
- dispunerea “la vedere “ şi marcarea cu bandă adezivă viu colorată a canalelor de cabluri aferente canalelor cu circuite de transmitere a informaţiilor clasificate, în scopul sesizării imediate a încercărilor de afectare a integrităţii, confidenţialităţii şi disponibilităţii acestora (normele INFOSEC)
- marcarea şi etichetarea cablurilor, conform cu prevederile standardelor SR EN 50131… 50136

3.2.5. Montarea de echipamente

- montarea echipamentelor şi dispozitivelor cu respectarea proiectului de securitate
- se va avea în vedere respectarea prevederilor legii 677/2001, privitoare la protecţia persoanelor cu privire la prelucrarea datelor cu caracter personal
- respectarea cerinţelor ergonomice
- marcarea şi etichetarea echipamentelor, conform cu prevederile standardelor SR EN 50131…50136

3.2.6. Conectarea echipamentelor în cadrul subsistemelor şi între subsisteme

- activitatea are loc în condiţiile deconectării alimentării cu energie electrică a echipamentelor montate
- verificarea, măsurarea şi montarea, dacă e cazul, a unei prize noi de împământare
- asigurarea securităţii accesului la dozele şi cutiile de conexiuni
- asigurarea condiţiilor normale de funcţionare în căminele de cabluri îngropate
- luarea măsurilor adecvate de asigurare a condiţiilor de mediu în cazul conectorizării fibrelor optice

3.2.7. Efectuarea punerii în funcțiune a componentelor (PIF)

- abordarea sistemică a acestei activități:
  - ♦ întâi se pun în funcțiune echipamentele distribuite şi instalate în obiectiv (dispozitive independente, senzori, cititoare, elemente de execuție, controllere de zonă etc)
  - ♦ apoi echipamentele de centralizare pe subsisteme (centrale de efracție, de control acces, de detecție la incendiu etc)
  - ♦ urmează echipamentele care formează centrele de monitorizare / dispecerizare (monitoare, HDR-uri, matrici, switch-uri, stații de lucru, centrale de interfonie, asigurarea intercorelărilor între subsisteme, ş.a.)
- finalizarea şi verificarea integrării de tip hardware
- asigurarea integrării de tip software
- verificarea transmiterii comenzilor în sistem şi analiza reacțiilor determinate de aceste comenzi

Aplicarea unei asemenea abordări conduce la creşterea eficienței activității de acest tip, prin evitarea întoarcerilor la verificarea funcționării elementelor din camp.

3.2.8. Participarea la Testare & Evaluare

Tehnicienii au rol important în această activitate, deoarece cunosc foarte bine echipamentele aflate în proces de testare / evaluare, parametrii acestora, precum şi spațiul / zona de acoperire / supraveghere (în cazul senzorilor, camerelor video etc), în ambele faze:

- testarea –evaluarea fizică individuală a echipamentelor
- testarea –evaluarea operațională (conform Planului de testare/evaluare, elaborate de investitor /proprietar.

3.2.9. Asigurarea mentenanței necesare

Activitatea se desfăşoară atât pe durata asigurării garanției contractuale, după recepția sistemului, cât şi pe timpul lucrărilor efectuate în cadrul unui contract expres de mentenanță. Este de menționat faptul că, în prevederile legii 333/2003, este inclusă obligativitatea încheierii unui contract de mentenanță, cu o firmă specializată, la terminarea etapei de garanție contractuale.

Mentenanța poate fi:

- preventivă, atunci când se execută, de regulă, lucrări de:
  - curățenie
  - gresări periodice
  - aspectarea unor componente specifice
- corectivă, care conține, în principal, activitățile:
  - diagnosticare
  - înlocuire
  - reparare:
    - in site
    - la sediul furnizorului de servicii
    - la sediul producătorului.

Conform prevederilor standardelor SR EN 50131…50136 , în conținutul proiectului de securitate este obligatoriu să fie menționate date privind modul de desfăşurare a procesului de mentenanță:

- elementele şi componentele situate pe locuri importante privind mentenanța
- detalierea operațiilor specifice de mentenanță, pentru fiecare componentă în parte
- precizarea intervalelor de timp la care sunt prevăzute operațiile mai sus menționate.

4. Concluzii

Activitățile de realizare, punere în funcțiune, testare&evaluare şi mentenanță fac parte din ciclul de viață al produsului final- sistemul integrat de securitate. Deşi parte integrantă a lucrărilor de instalații electrice, în segmentul curenților slabi, toate aceste activități au caracter aparte, care este determinat de scopul specific al unui asemenea produs: asigurarea funcționării în condiții de siguranță şi stabilitate, adică în securitate deplină.

5. Bibliografie

1) Ing. T. URDAREANU, Dr. ing. Gh. ILIE, Ing. M. BLAHA: **Securitatea instituțiilor financiar-bancare**, Editura UTI, București, 1998

2) Dr. ing. Gh. ILIE, Ing. T. URDAREANU: **Securitatea deplină**, Editura UTI, București, 2001

3) Standardele **SR EN 50130…50136**

4) NP I7-2002 : **Normativ pentru proiectarea şi executarea instalațiilor electrice, cu tensiuni până la 1000 Vc.a. şi 1500 Vc.c.**

5) I18-1-2002: **Normativ pentru proiectarea şi executarea instalațiilor electrice interioare de curenți slabi aferente clădirilor civile şi de producție**.

6) I18-2-2002 : **Normativ pentru proiectarea şi executarea instalațiilor de semnalizare a incendiilor şi a sistemelor de alarmare împotriva efracției.**

Întocmit,

Lector : Ing. Adrian ROŞCA

PROTECȚIA MECANO-FIZICĂ

Lector: Mihai BĂNULEASA
Dipl. ing. Mecanic/Master Criminalistică

Capitole:
1. Definiții, cerințe legale
2. Elemente de protecție mecano-fizice
3. Standarde de referință

1. Definiții, cerințe legale

În țara noastră există obligativitatea ca bunurile, datele şi informațiile cu caracter secret de stat, valorile şi suporturile de stocare a documentelor deținute de diferite entități să aibă paza asigurată, să fie prevăzute cu mijloace mecano-fizice de protecție şi sisteme de alarmare împotriva efracției în locurile de păstrare, depozitare şi manipulare a acestora, precum şi în locurile unde se desfăşoară activități care au un asemenea caracter.

În accepțiunea legilor în vigoare, protecția mecano-fizică reprezintă acele componente ale sistemelor tehnice de securitate care asigură protecția împotriva efracției. În sensul Legii 333/2003 prin elemente de protecție mecano-fizice se înțelege: ziduri, plase, blindaje, case de fier, seifuri, dulapuri metalice, tezaure, geamuri şi folie de protecție, grilaje, uşi şi încuietori.

În proiectele de execuție a construcțiilor destinate producerii, păstrării sau detinerii unor bunuri ori valori importante sau a lucrărilor de modernizare, modificare şi transformare a acestora trebuie să se prevadă obligatoriu construirea sau introducerea mijloacelor de protecție mecano-fizice.

Elementele de protecție mecano-fizice incorporate imobilelor destinate păstrării, depozitării si manipulării bunurilor si valorilor de orice fel trebuie să fie certificate ca rezistente la efracție, corespunzător gradului de siguranță impus de caracteristicile obiectivului păzit. Furnizorii de echipamente de protecție mecano-fizice au obligativitatea de a comercializa numai acele echipamente care sunt certificate. Certificarea calității mijloacelor de protecție mecano-fizice şi a componentelor acestora, produse în România sau importate, se face de către un laborator de încercări din țară, autorizat şi acreditat, potrivit legii. Este obligatoriu ca în procesul comercializării elementelor de protecție mecano-fizice, acestea să fie însoțite de un certificat de calitate eliberat de un laborator autorizat din țară, să fie menționate standardele naționale sau internaționale în baza cărora au fost fabricate şi să fie precizată clasa de siguranță în care se încadrează, conform normelor europene (care sunt obligatorii şi pentru România).

Toți operatorii sistemelor de protecție mecano-fizice (importatori, distribuitori, instalatori autorizați persoane juridice sau lăcătuşi mecanici autorizați) au obligația conform legii de a păstra confidențialitatea informațiilor referitoare la beneficiarii sistemelor importate, distribuite sau instalate, precum şi a sistemelor pe care le au în întreținere sau efectuează ocazional intervenții asupra lor.

2. Elemente de protecție mecano-fizice

Protecția mecano-fizică este baza de la care se pleacă atunci când se concepe protecția unui obiectiv. Aceasta se îmbină armonios cu sistemele electronice şi paza. Elementele de protecție

mecano-fizice ca parte componentă a sistemelor tehnice de securitate care asigură protecția împotriva efracției sunt:

- Ziduri
- Plase
- Blindaje
- Case de fier
- Seifuri
- Dulapuri metalice
- Tezaure
- Geamuri şi folie de protecție
- Grilaje
- Uşi
- Încuietori

În practică se utilizează diferite combinații ale acestor elemente, în funcție de specificul obiectivului de protejat, grupate în următoarele categorii de echipamente:

2.1. Seifuri, tezaure, camere de tezaur, uşi de tezaur

Seifurile (sau case de fier) sunt acele dulapuri metalice fabricate într-o construcție robustă, care au diferite protecții împotriva atacurilor brutale la deschidere prin forțare şi foc, destinate păstrarii banilor, documentelor şi a altor bunuri. Un seif este definit atunci când este îndeplinită condiția ca cel puțin una din laturile exterioare ale acestuia să fie mai mică de 1m. Dacă toate laturile exterioare ale seifului depaşesc 1 m, atunci acesta iese din categoria seifurilor şi intra in categoria tezaurelor.

Din punct de vedere constructiv seifurile pot fi tip dulap (independente), înglobate (în pardoseală sau perete) sau seifuri distribuitoare de bani (tip ATM). Tehnologiile moderne de fabricație permit executarea seifurilor şi din elemente prefabricate.

Aceste seifuri trebuie să aibă posibilitatea de a fi ancoarte în pardoseală şi/sau perete şi să răspundă la cerinte minime de rezistență la efracție. Seifurile se clasifică în 11 clase de rezistență (pe o scara de la 0 la 10), în funcție de: rezistența la efracție, rezistența la ancorare, clasa de siguranță a încuietorilor folosite, rezistența la taiere cu flacără oxiacetilenică, rezistența la gauritul cu scule diamantate, rezistența la explozibili.

Rezistența de ancorare se determină pentru seifurile cu masă sub 1000 Kg şi constă în verificarea, cu ajutorul unui echipament de încercare, a rezistenței construcției seifului şi a sistemului de ancorare în elementul de construcție în care se face prinderea.

Rezistența la acțiunea uneltelor de efracție se calculează pe baza timpilor înregistrați şi a tipurilor de unelte folosite la realizarea accesului parțial şi a accesului complet. Standardul stabileşte

tipurile şi categoriile de unelte folosite, fiecărui tip şi categorie fiindu-i alocat un anumit coeficient şi o anumită valoare de bază. Uneltele de efracție folosite sunt cele care în opinia colectivului de încercări determină valorile minime ale rezistenței. Accesul parțial implică realizarea unei deschideri de: 125 cm^2, la nivelul peretelui sau a uşii seifului, iar accesul complet implică fie realizarea la nivelul peretelui sau a uşii seifului a unei deschideri de 990 cm^2, fie îndepărtarea sau deschiderea uşii seifului, creându-se un spațiu de minimum 300 mm lățime şi de peste 80% din înălțimea interioară a volumului de depozitare. În cazul seifurilor înglobate, îndepărtarea acestora din materialul în care se face înglobarea se consideră acces complet. Controlul realizării accesului se face cu ajutorul unor şabloane rigide standardizate.

Fazele încercării de determinare a rezistenței de ancorare sunt următoarele:

- montarea pe seif a echipamentului de încercare, prin intermediul sistemului de ancorare recomandat de producător, ce trece prin una din găurile de ancorare, conform instrucțiunilor de instalare a seifului;
- aplicarea unei forțe de 50 kN sau 100 kN (funcție de clasa de rezistență urmărită) în sistemul de ancorare; încărcarea se face lent, timp de 2 - 3 min;
- menținea încărcării timp de 1 min după care se face descărcarea;
- înregistrarea forței aplicate şi evaluarea stării sistemului de ancorare şi a zonei orificiului de trecere (sistemul de ancorare nu trebuie să se rupă sau să treacă prin perete).

Fazele încercării de determinare a rezistenței la acțiunea uneltelor de efracție sunt următoarele:

- stabilirea pe baza documentației tehnice şi a inspectării eşantionului a metodelor de atac şi a uneltelor cele mai indicate pentru obținerea valorilor minime ale rezistenței;
- realizarea accesului parțial şi a accesului complet cu cronometrarea timpilor de utilizare a fiecărei unelte;
- calcularea valorii rezistenței cu ajutorul unei relații stabilite prin standard, pe baza timpilor măsurați şi a coeficienților şi valorilor de bază ale uneltelor folosite.

Clasa de rezistență la efracție (de la 0 la X) se determină pe baza cerințelor stabilite prin standard în funcție de:

- valoarea rezistenței la acțiunea uneltelor de efracție pentru realizarea accesului parțial şi accesului complet;
- valoarea rezistenței de ancorare;
- numărul şi clasa de rezistență a încuietorilor.

Tezaurele sunt incinte special amenajate pentru pastrat valori, la care toate laturile exterioare depaşesc 1m. Camerele de tezaur şi uşile de tezaur se clasifică în 14 clase de rezistență (pe o scară de la 0 la 13) în funcție de rezistența la efracție cu unelte, clasa încuietorilor şi cerințele suplimentare de rezistență la atacul cu scule diamantate şi explozibili. Astfel, standardele prevăd următoarele încercări :

- pentru camerele de tezaur complet echipate, cel puțin o încercare cu unelte de efracție pentru realizarea accesului complet la nivelul peretelui camerelor de tezaur şi o încercare cu unelte de efracție pentru realizarea accesului complet la nivelul uşilor camerelor de tezaur;
- pentru camerele de teazaur fără uşă, cel puțin o încercare cu unelte de efracție pentru realizarea accesului complet la nivelul peretelui camerelor de tezaur;
- pentru uşile de tezaur, cel puțin o încercare cu unelte de efracție pentru realizarea accesului complet la nivelul uşilor (inclusiv rama şi secțiunile adiacente de perete, dacă este necesar).

Rezistența la acțiunea uneltelor de efracție se calculează pe baza timpilor înregistrați şi a tipurilor de unelte folosite la realizarea accesului complet. Uneltele de efracție folosite sunt cele care în opinia colectivului de încercări determină valorile minime ale rezistenței. Accesul complet implică, fie realizarea unei deschideri de 990 cm^2, la nivelul peretelui şi /sau a uşii camerei, sau îndepărtarea sau deschiderea uşii, creându-se un spațiu de minimum 300 mm lățime şi de peste 80% din înălțimea interioară a volumului de depozitare. Controlul realizării accesului se face cu ajutorul unor şabloane rigide standardizate.

Fazele încercării de determinare a rezistenței la acțiunea uneltelor de efracție sunt următoarele:

- stabilirea pe baza documentației tehnice și a inspectării eșantionului a metodelor de atac și a uneltelor cele mai indicate pentru obținerea valorilor minime ale rezistenței;
- realizarea accesului parțial și a accesului complet cu cronometrarea timpilor de utilizare a fiecărei unelte;
- calcularea valorii rezistenței cu ajutorul unei relații stabilite prin standard, pe baza timpilor măsurați și a coeficienților și valorilor de bază ale uneltelor folosite.

Clasa de rezistență la efracție (de la 0 la XIII) se determină pe baza cerințelor stabilite prin standard în funcție de:

- valoarea rezistenței la acțiunea uneltelor de efracție pentru accesul complet;
- numărul și clasa de rezistență a încuietorilor.

Seifurile destinate ATM-urilor au o construcție specifică, prin care se pot transfera în mod automat bani din interiorul acestuia catre exterior, pastrând caracteristicile unui seif. Există 9 clase de rezistență ale acestor tipuri de seifuri (clasa L, și de la 1 la 8). Standardele prevăd două încercări ale acestor seifuri :

- încercarea de determinare a rezistenței de ancorare;
- încercarea de determinare a rezistenței la acțiunea uneltelor de efracție.

Rezistența de ancorare a seifurilor ATM-urilor se evaluează prin aplicarea unei forțe orizontale de 100 kN asupra unui eșantion de încercare și măsurarea unghiului de înclinare și a deplasării eșantionului de încercare.

Rezistența la acțiunea uneltelor de efracție se calculează pe baza timpilor înregistrați și a tipurilor de unelte folosite la realizarea accesului parțial, a accesului complet sau pentru tăierea sau distrugerea prinderii ATM-ului de elementul de construcție de rezistență. Standardul stabilește tipurile și categoriile de unelte folosite, fiecărui tip și categorie fiindu-i alocat un anumit coeficient și o anumită valoare de bază. Uneltele de efracție folosite sunt cele care în opinia colectivului de încercări determină valorile minime ale rezistenței. Accesul parțial implică realizarea la nivelul peretelui sau a ușii seifului a unei deschideri de: 125 cm^2, iar accesul complet implică fie realizarea la nivelul peretelui sau a ușii seifului a unei deschideri de 990 cm^2, fie îndepărtarea sau deschiderea ușii seifului, creându-se un spațiu de minimum 300 mm lățime și de peste 80% din înălțimea interioară a volumului de depozitare. Se consideră acces complet și taierea sau distrugerea prinderilor dintre seif și elementul de construcție de care acesta se ancorează. Controlul realizării accesului se face cu ajutorul unor șabloane rigide standardizate.

Fazele încercării de determinare a rezistenței de ancorare sunt următoarele:

- montarea seifului ATM-ului pe o placă de încercare utilizând metoda de prindere recomandată de producător; Pentru seifurile ATM-urilor montate în zid, seifurile se rotesc la 90^0 și se prind pe placa orizontală de încercare, astfel încât să se simuleze peretele vertical de montaj;
- realizarea unei încercări cu unelte de efracție pentru îndepărtarea sau slăbirea oricăror prinderi exterioare;
- aplicarea pe direcție orizontală a unei forțe de 50 kN sau 100 kN (funcție de clasa de rezistență urmărită); încărcarea se face lent, timp de 2 - 3 min;
- menținea încărcării timp de 1 min după care se măsoară unghiul de înclinare al seifului ATM-ului;
- după descărcare se măsoară distanța pe care seiful s-a deplasat sub acțiunea forței;
- înregistrarea forței aplicate, a unghiului sub care seiful s-a înclinat și a distanței pe care seiful ATM-ului a fost deplasat sub acțiunea forței aplicate. Aplicarea forței nu trebuie să producă deplasarea seifului ATM-ului pe mai mult de 200 mm sau înclinarea sub un unghi mai mare de 60^0.

Încercarea de determinare a rezistenței la acțiunea uneltelor de efracție pentru clasele I - VIII ale seifurile ATM-urilor trebuie să cuprindă cel puțin o încercare cu unelte de efracție pentru realizarea:

a) accesului parțial la nivelul uşii sau corpului;
b) accesului complet la nivelul uşii sau corpului;
c) tăierii sau distrugerii prinderii prin atac direct asupra oricărei dotări de prindere.

Încercări suplimentare cu unelte de efracție, conform a) sau b) trebuie realizate asupra oricărei zone a eşantionului de încercare care are o construcție diferită şi pentru care se aşteaptă ca valoarea de rezistență să poate fi mai mică (de ex. zona cu găuri deja existente).

Încercarea pentru realizarea accesului parțial la clasele I - VIII ale seifurilor ATM-urilor trebuie să cuprindă:

a) cel puțin o încercare cu unelte de efracție la nivelul corpului sau uşii realizată astfel încât orificiile preexistente (obturate sau nu) să facă parte din golul accesului parțial.
b) cel puțin o încercare cu unelte de efracție care trebuie realizată pentru obținerea unui acces parțial prin mărirea unei deschideri neobturate de eliberare a numerarului sau a unei deschideri neobturate de intoducere a unei depuneri (dacă pe eşantion există o astfel de deschidere).
c) încercări cu unelte de efracție care trebuie realizate la nivelul deschiderilor obturate de eliberare a numerarului sau deschiderilor obturate de introducere a depunerilor (pe eşantion trebuind să fie prezentă o deschidere obturată).

Încercările suplimentare cu unelte de efracție pentru realizarea accesului parțial trebuie realizate la nivelul oricărei zone sau dotări a eşantionului de încercare, incluzând diferite mijloace de obturare şi pentru care valoarea de rezistență previzionată se aşteaptă a fi mai mică.

Încercarea pentru realizarea accesului complet la clasele I - VIII a seifurilor ATM-urilor trebuie să cuprindă o încercare cu unelte de efracție la nivelul corpului şi uşii. Încercările suplimentare cu unelte de efracție trebuie realizate la nivelul oricărei zone a eşantionului de încercare pentru care sunt previzionate să apară valori de rezistență inferioare. De asemenea este necesară o încercare cu unelte de efracție la nivelul dotărilor de prindere prin tăierea sau distrugerea prinderilor.

Toate seifurile ATM-urilor de clasă L trebuie supuse unei încercări cu unelte de efracție pentru realizarea:

a) unui acces parțial la nivelul uşii;
b) unui acces complet la nivelul uşii;
c) tăierii sau distrugerii prinderilor prin încercare cu unelte de efracție la nivelul oricărei dotări de prindere.

În funcție de construcția seifului (grosimi şi rezistențe de rupere a materialelor utilizate, tipuri de cordoane de sudură) pot fi necesare încercări suplimentare pentru realizarea accesului parțial şi complet la nivelul corpului.

Fazele încercării de determinare a rezistenței la acțiunea uneltelor de efracție sunt următoarele:

- stabilirea pe baza documentației tehnice şi a inspectării eşantionului a metodelor de atac şi a uneltelor cele mai indicate pentru obținerea valorilor minime ale rezistenței;
- realizarea accesului parțial şi a accesului complet cu cronometrarea timpilor de utilizare a fiecărei unelte;
- calcularea valorii rezistenței cu ajutorul unei relații stabilite prin standard, pe baza timpilor măsurați şi a coeficienților şi valorilor de bază ale uneltelor folosite.

Clasa de rezistență la efracție se determină pe baza cerințelor stabilite prin standard în funcție de:

- valoarea rezistenței la acțiunea uneltelor de efracție pentru accesul parțial (general şi utilizând orificiile existente) şi accesul complet;
- valoarea rezistenței de ancorare;
- valoarea rezistenței la acțiunea uneltelor de efracție pentru distrugerea sau îndepărtarea dotărilor de prindere;
- numărul şi clasa de rezistență a încuietorilor.

În cazul seifurilor prefabricate, seifurilor înglobate (în pardoseală şi perete), seifurilor şi postamentelor distribuitoarelor de bani pe bază de card (ATM-urilor), uşilor de tezaur, camerelor

de tezaur (cu sau fără uşă) rezistente la tentativele de efracţie realizate cu explozivi, standardele stabilesc, suplimentar faţă de încercările prezentate mai sus, realizarea unei încercări de determinare a rezistenţei la acţiunea unei cantităţi standardizate de exploziv (tetranitrat de pentaeritritol).

În cazul seifurilor, se încearcă un eşantion cu volumul interior cuprins între 300 şi 400 dm^3, iar încărcătura explozivă se plasează în centrul geometric al volumului interior de depozitare. După detonare se efectuează o încercare cu unelte de efracţie pentru realizarea accesului complet. Această încercare trebuie înregistrată ca încercări de efracţie post detonare.

În cazul uşilor şi camerelor de tezaur pentru introducerea încărcăturii explozive se pot realiza deschideri în eşantioanele de încercare prin încercări de efracţie exploratorii. Atât durata acestor încercări, cât şi tipurile de unelte de efracţie sunt stabilite de către standard. Încărcătura explozivă este introdusă în deschiderea astfel realizată, se burează şi se detonează. După explozie, se continuă încercarea cu unelte de efracţie până la realizarea accesului complet.

Calculul valorii de rezistenţă la efracţie pentru încercările post-detonare se face cu ajutorul unei relaţii stabilite prin standard, pe baza timpilor măsuraţi şi a coeficienţilor şi valorilor de bază ale unealtelor folosite.

Clasa de rezistenţă la efracţie se determină pe baza cerinţelor stabilite prin standard în funcţie de:

- valoarea rezistenţei la acţiunea uneltelor de efracţie pentru accesul parţial şi complet;
- valoarea rezistenţei la efracţie pentru încercările post-detonare;

numărul şi clasa de rezistenţă a încuietorilor

2.2. Geamurile de securitate

Geamurile de securitate sunt geamuri special fabricate cu rezistenţă la atacuri manuale sau la acţiunea armelor de foc. Se pot utiliza şi folii de acoperire de tip antiefracţie sau antivandal, clasificările conform standardelor se aplică în această situaţie pentru ansamblul folie-geam.

Standardele prevăd încercarea şi clasificarea geamurilor rezistente la atacuri manuale, fără a face o distincţie între destinaţia vitrajului (anti-vandal sau anti-efracţie). Pentru alegerea tipului de vitraj în funcţie de destinaţie se recomandă solicitarea avizului unui expert sau direct a producătorului. Ca regulă generală vitrajele cu până la 3 straturi de PVB (butiral polivinilic) sunt considerate ca vitraje antivandal, iar cele cu peste 4 straturi de PVB ca fiind vitraje antiefracţie (au rol de întârziere a pătrunderii prin efracţie).

Standardul specifică două metode de încercare:

- încercarea la acţiunea unei bile lăsate să cadă de la o anumită înălţime pe vitraj;
- încercarea la acţiunea uneltelor manuale de efracţie.

Geamurile rezistente la atacuri manuale se clasifică în 8 clase de rezistenţă. În laboratoarele de testare se utilizează ca unelte manuale de efracţie ciocanul şi toporul. Încercarea se desfăşoară pe un stand ce asigură repetabilitatea condiţiilor de încercare, inclusiv unghiul de lovire. Obiectivul încercării este de a realiza în placa de vitraj o deschidere de 400 X 400 mm. În acest scop se aplică, într-o primă etapă, o serie de lovituri, capul toporului fiind înlocuit cu un cap de ciocan. Numărul minim de lovituri aplicate în fiecare punct este de 12, efectul loviturilor fiind acela de penetrare a tuturor straturilor ce formează vitrajul. După spargerea geamului, se înlocuieşte capul de ciocan cu capul de secure şi se aplică lovituri pe conturul deja spart până la penetrarea foilor de geam. Loviturile se aplică până la realizarea deschiderii de 400 X 400 mm, în geam, proba încetând în momentul în care partea decupată se desprinde şi cade. În funcţie de numărul de lovituri aplicate se încadrează tipul de geam încercat într-o categorie de rezistenţă.

Geamurile rezistente la armele de foc se împart în doua categorii : cele rezistente la puştile de vânătoare cu alice (grupate în două clase : SG1 şi SG2) şi cele rezistente la arme de foc cu glonţ : pistoale, puşti, carabine (grupate în 7 clase de la BR1 la BR7).

Standardele descriu modul de încercare şi clasificare a geamurilor rezistente la acţiunea armelor de foc (puşti/carabine, pistoale şi arme de vânătoare), în funcţie de calibrul armei, forma şi

materialul glonțului. Pentru alegerea tipului de vitraj în funcție de destinație se recomandă solicitarea avizului unui expert sau direct a producătorului.

Încercările de tragere se efectuează pe 3 eşantioane de geam, iar proba se consideră reuşită dacă prin toate cele 3 eşantioane glonțul sau părți ale acestuia nu trec prin geam.

În plus standardul face distincție între geamurile din care în urma impactului cu glonțul se desprind sau nu aşchii de sticlă, prin introducerea după clasa de rezistență a mențiunii S - pentru tipurile de geam din care se desprind aşchii, sau NS - pentru tipurile de geam din care nu se desprind aşchii.

De reținut faptul că nivelele BR1.... BR7 sunt ordonate în funcție de nivelul de protecție oferit, de exemplu un panou ce satisface exigențele definite pentru o anumită clasă, satisface şi exigențele claselor inferioare. Vitrajele din clasele SG nu satisfac în mod automat şi exigențele definite pentru clasele BR, muniția utilizată fiind diferită.

EXEMPLU DE SIMBOLIZARE:

BR1(S) - geam antiglonț rezistent la acțiunea glonțelor din plumb, de formă conico-cilindric, trase de o armă cu calibrul 0,22 LR, în urma impactului cu glonțul, din fața opusă loviturii existând posibilitatea de desprindere de aşchii;

BR1(NS) - geam antiglonț rezistent la glonț conico-cilindric, din plumb, tras de o armă cu calibrul 0,22 LR, în urma impactului cu glonțul, ne desprinzându-se aşchii din fața opusă loviturii.

2.3. Maşini blindate pentru transportul valorilor

În prezent, pentru maşinile blindate de transport valori nu există standarde de încercare şi clasificare. Pentru construcția, dotarea şi exploatarea maşinilor blindate destinate transportului de valori sunt luate în considerație în principal: asigurarea reistenței la efracție şi rezistența la acțiunea armelor de foc.

Pe plan european s-au stabilit cerințe generale tehnice de siguranță şi ergonomie, care să asigure protecția angajaților, pe cât posibil, împotriva atacurilor şi incidentelor şi care prin asigurarea bunului transportat trebuie să descurajeze semnificativ tentativele de atac. Pentru aceasta au fost luate în considerare în mod semnificativ cerințe tehnice de siguranță din alte domenii profesionale comparabile.

Maşinile blindate pentru transportul valorilor sunt vehicule cu construcții şi dotări de protecție la pătrunderea prin efracție şi rezistență la acțiunea armelor de foc, inclusiv sisteme suplimentare de siguranță, care protejează personalul, în mare parte contra atacurilor şi care prin măsurile de asigurare a conținutului transportat descurajează semnificativ tentativele de atac.

Construcția şi dotarea : Cabinele de conducere şi construcțiile care servesc la protecția personalului împotriva atacurilor trebuie executate integral în soluții constructive care asigură protecției la pătrunderi prin efracție cu ajutorul uneltelor simple şi rezistența la acțiunea armelor de foc. Acestea se referă de exemplu şi pentru plafoane, podea, locaşul roților şi parbrize.

Ca măsuri eficiente, suplimentare în vederea reducerii tentației de atac asupra maşinii blindate se recomandă următoarele construcții:

- Construcția unei incinte destinete transportului de valori legate solid de şasiu şi asigurate contra îndepărtării ei nedorite;
- Deschiderea acestei incinte să nu poată fi posibilă pe parcursul derulării transportului, chiar şi de către personalul de însoțire;
- Instalarea unui sistem lansator de fum colorat, în caz de atac care să funcționeze eficient şi cu un debit corespunzător de fum. Pătrunderea fumului în compartimentul ocupat de persoane trebuie înpiedicată prin masuri de etanşare a coartimentului şi prevederea unor sisteme eficiente de ventilare;

- Geamurile laterale trebuie să nu poată fi coborâte, iar toate vitrajele trebuie să fie fixate rigid şi asigurate împotriva desprinderii;
- Vopsirea exterioară a maşinilor, în special a plafonului să se facă în culori puternic reflectorizante, tonuri deschise reducându-se astfel efectele căldurii.

Instalații de încălzire şi ventilare, sisteme de răcire a aerului şi climatizare : maşinile blindate pentru transportul valorilor trebuie dotate cu instalații pentru încălzire şi ventilare. Instalațiile trebuie să fie astfel executate încât să fie corespunzător dimensionate şi să funcționeze şi independent de motorul maşinii. Instalațiile pentru încălzire şi ventilare, ca şi agregatele de răcire trebuie să fie construite şi instalate astfel încât să fie excluse pericolele de incendiu şi explozie şi să nu pericliteze sănătatea ocupanților, prin gazele eşapate, lipsa de oxigen, temperaturi ridicate la ieşirea aerului sau suprafețe incinse. Se recomandă ca instalațiile să nu producă curenți de aer în zona tuturor scaunelor şi să asigure o temperatură, în cabină, în poligonul de confort, chiar şi pe perioadele de staționare.

Uşi, deschideri şi ieşiri de urgență: prin modul de construcție a uşilor, deschiderilor şi ieşirilor de siguranță, trebuie să se asigure ca în timpul încărcării şi descărcării, precum şi la urcarea, respectiv la coborârea curierilor ce manipulează valori în zonele accesibile publicului, un atac direct asupra persoanelor de însoțire rămase în maşină şi asupra conținutului comartimentului de valori să nu fie posibil. Acesta se realizează prin prevederea unor compartimente intermediare (ecluze) sau a unor sisteme de închidere cu acces restricționat supravegheat.

Toate uşile exterioare, deschiderile şi ieşirile de siguranță trebuie prevăzute cu sisteme de închidere în minim 5 puncte, iar deschiderea din exterior să se facă numai prin intermediul unor încuietori de securitate. Sunt acceptate şi alte sisteme de închidere şi asigurare în condițiile în care rezistența lor este certificată corespunzător.

Toate uşile de acces trebuie prevăzute cu vitraje care să permită observarea eventualelor pericole. Vitrajele trebuie să asigure acelaşi grad de protecție la tentativele de atac prin efracție şi la acțiunea armelor de foc ca şi restul construcției maşinii.

La maşinile blindate pentru transportul valorilor trebuie să existe în mod obligatoriu cel puțin o ieşire de urgență, dimensionată corespunzător (spațiul de evacuare să fie de 600 mm X 600 mm) şi care să nu se găsească pe aceiaşi parte cu uşa exterioară de acces. În cazul în care maşina este prevăzută cu mai multe compartimente în care se află persoane, este permisă existența unor deschideri de trecere între compartimente.

Toate uşile şi deschiderile trebuie să poată fi deschise uşor din interior şi în orice moment şi trebuie să fie astfel executate încât să reziste tentativelor de efracție sau forțărilor din exterior efectuate cu unelte simple.

Scaune, centuri de siguranță şi tetiere: scaunele pentru şofer şi ale tuturor însoțitorilor trebuie să fie astfel realizate şi poziționate încât să evite, pe cât posibil, rănirea personalului.

Scaunele trebuie astfel aranjate încât axa longitudinală a scaunului să fie paralelă cu axă longitudinală a maşinii. Scaunul şoferului trebuie să poată fi reglat corespunzător taliei acestuia.

Toate scaunele trebuie prevăzute cu centuri de siguranță în trei puncte, cu dispozitive ce adaptează automat centurile funcție de utilizator şi cu mecanism de blocare care să acționeze în caz de necesitate. Toate scaunele trebuie să fie dotate cu tetiere în modalitatea constructivă livrată de producător sau într-o formă aprobată de autorități.

Instalații pentru supravegherea zonei înconjurătoare: pentru asigurarea posibilității de observare a zonei inconjurătoare maşinile blindate pentru transportul valorilor trebuie prevăzute cu sisteme supliementare. Acestea pot fi ferestre, oglinzi sau sisteme video.

Instalații radio şi de alarmare: maşinile blindate pentru transportul valorilor trebuie prevăzute cu un aparat de radio emisie-recepție sau cu un sistem de comunicație prin care să se poată lua legătura cu dispeceratul sau alte posturi (centrala operativă, locul de destinație, poliția etc). Suplimentar se recomandă contactul radio între maşină şi curierii care transportă valorile.

Maşinile blindate pentru transportul valorilor trebuie prevăzute cu o instalație de alarmare ce acționează sonor şi vizual. Dispozitivul de declanşare a alarmei trebuie să se găsească la persoanele rămase în maşină pentru asigurarea protecției.

Inscripționarea exterioară a plafonului : maşinile blindate pentru transportul valorilor trebuie inscripționate pe exteriorul plafonului asfel încât să fie posibilă indentificarea lor din aer.

Instalații şi mijloace ajutătoare pentru asigurarea încărcăturii: în compartimentele de transport a valorilor trebuie să existe dispozitive pentru asigurarea încărcăturii care să fie astfel concepute, încât la utilizări curente, să împiedice căderea, alunecarea sau răsturnarea încărcăturii. Dacă încărcătura nu este asigurată suficient numai cu ajutorul acestor dispozitive, trebuie să fie disponibile mijloace auxiliare pentru asigurarea încărcăturii. Aceasta este valabil şi pentru dotările tehnice transportate în maşină în scopul descurajării tentației de atac. Astfel de sisteme pot fi: suporturi de încărcare, perți rezistenți la lovire, suporturi pentru aparatura însoțitoare, curele, dispozitive de oprire şi imobilizare, puncte de fixare, plase, prelate etc.

Există o procedură elaborată în detaliu referitoare la încercarea rezistenței maşinilor blindate la acțiunea armelor de foc.

2.4. Dulapuri, camere şi containere rezistente la foc destinate depozitării purtătorilor de date

Standardele stabilesc clasificarea dulapurilor de date în funcție de natura purtătorilor de date şi durata expunerii la foc în următoarele clase de protecție

Clasa de protecție		Creşterea maximă a temperaturii	Umiditatea relativă maximă
60 min	120 min		
S 60 P	S 120 P	150 ^{0}C	nici o cerință
S 60 D	S 120 D	50 ^{0}C	85 %
S 60 DIS	S 120 DIS	30 ^{0}C	85 %

unde **S** reprezintă simbolul aplicat dulapurilor pentru date rezistente la foc.
Valorile numerice, din clasa de protecție, reprezintă timpii de expunere la foc, la încercări, exprimați în minute, iar literele caracterizează tipurile de purtători de date ce pot fi protejați, în fiecare clasă, după cum urmează:

P - Documente pe hârtie termosensibilă, mai puțin categoriile de hârtie ce pierd informațiile sub 170 ^{0}C.

D - Purtători de date sensibili la umiditate şi temperatură, cum ar fi purtătorii magnetici şi hârtia termosensibilă, mai puțin purtătorii care pierd informațiile sub 70 ^{0}C.

DIS - Purtători de date sensibili la umiditate şi temperatură, cum ar fi dischetele, mai puțin purtătorii care pierd informațiile sub 50 ^{0}C.

Prin standarde se specifică două încercări pentru determinarea rezistenței la foc, şi anume:

- încercarea de determinare a rezistenței la foc;
- încercarea de determinare a rezistenței la şoc termic şi impact.

Rezistența la foc se evaluează pe baza expunerii eşantionului de încercare la un regim încălzire - răcire, în cuptor, conform unei relații standardizate, temperatură - timp, determinându-se umiditatea şi temperaturile maxime atinse în anumite puncte din interiorul eşantionului.

Rezistența la şoc termic şi impact se evaluează pe baza expunerii eşantionului la un regim încălzire - răcire, în cuptor, combinat cu o încercare de determinare a rezistenței la impact a eşantionului, realizată prin căderea eşantionului de la o înălțime de 9,15 ± 0,05m pe un pat de pietriş de râu, cu grosimea de 0,5m

2.5. Tâmplăria de securitate

Tâmplărie rezistentă la efracție: clasele de rezistență sunt în număr de 6. Responsabilitatea pentru utilizarea şi alegerea claselor de rezistență revine de regula utilizatorului, de exemplu

proprietarului imobilului, arhitectectului, companiei de asigurări, poliției. Trebuie ținut cont că un produs cu o clasă de rezistență mai mare va costa mai mult.

Clasa de rezistență	Metoda anticipată de a realiza pătrunderea
1	Spărgătorul ocazional încearcă să spargă fereastra, ușa sau jaluzeaua utilizând violența fizică de exemplu lovind, forțând cu umărul, ridicând, rupând/smulgând
2	Spărgătorul ocazional încearcă în plus să spargă fereastra, ușa sau jaluzeaua utilizând unelte simple, de exemplu șurupelnițe, clești, pene
3	Spărgătorul încearcă să realizeze pătrunderea utilizând o șurupelniță suplimentară și o rangă
4	Spărgătorul experimentat utilizează în plus ferăstraie, ciocane, topor, dălți și mașini de găurit portabile alimentate de la baterii
5	Spărgătorul experimentat utilizează în plus unelte electrice portabile, de exemplu mașini de găurit, fierăstrău pendular și cu lanț și polizor de colț cu un disc de max. ∅ 125 mm
6	Spărgătorul experimentat utilizează în plus unelte electrice portabile puternice, de exemplu mașini de găurit, fierăstrău pendular și cu lanț și polizor de colț cu un disc de max. ∅ 230 mm

Tentativele de efracție se execută în zonele de atac definite mai jos:

- atacuri asupra componentelor de încuiere;
- atacuri asupra componentelor mobile;
- atacuri asupra corpului elementelor;
- atacuri asupra dotărilor mecanice (feroneriei);
- atacuri asupra altor zone relevante.

Tâmplărie rezistentă la acțiunea armelor de foc: standardele se aplică atacurilor cu pistoale, revolvere, carabine, puști și arme de vânătoare, asupra ferestrelor, ușilor, obloanelor și jaluzelelor, împreună cu umpluturile și ramele lor, utilizate atât la exteriorul cât și la interiorul clădirilor.

Jaluzelele și obloanele trebuie încercate separat și nu împreună cu o fereastră sau o ușă, pentru clasificarea în ceea ce privește rezistența la glonț.

Sunt definite de către standarde 7 clase de rezistență (de la FB1 la FB7).

În tabelul de mai jos este prezentată concordanța dintre clasele de rezistență la acțiunea armelor de foc ale ferestrelor, ușilor și jaluzelelor și cele ale geamurilor antiglonț.

Clasa	Clasa minimă a geamului ce trebuie folosit la încercări (conform EN 1063)
FB1	BR1
FB2	BR2
FB3	BR3
FB4	BR4
FB5	BR5
FB6	BR6
FB7	BR7
FSG	SG2

2.6. Zidurile

Pentru a constitui o barieră de protecție în cadrul unor obiective cum ar fi pereții unei incinte de procesat banii, zidurile trebuie să aibă grosimea de minim 40 cm şi să fie din cărămidă plină, fără goluri la interior. O grosime mai mică de 40 cm impune utilizarea unor panouri metalice suplimentare de blindare.

2.7. Casele de transfer

Casele de transfer sunt minisisteme de tip ecluză, utilizate pentru transferul unor volume relativ mari, pachete speciale, transportul acestor valori efectuându-se pe o podea, fie cu role, fie telescopică, sau cu ajutorul unui minicărucior.

2.8. Dispozitivele de închidere

Dispozitivele de închidere reprezintă acele dispozitive (părți active) ale sistemelor de securitate mecanice care receptionează cheia fizică sau virtuală (sub forma unui cod), o recunoaşte, o decodifică şi permite activarea unei funcții de blocare/deblocare a cel puțin unui element fizico-mecanic cu menirea de blocare/deblocare (prin retragerea unor zăvoare, de exemplu) a componentelor pasive cum ar fi: uşi, ferestre, trape etc.

În cazul **seifurilor**, aceste dispozitive de închidere sunt clasificate în 4 clase (A-D) şi sunt prevăzute următoarele cerințe pentru toate încuietorile: codul de deschidere trebuie să fie singurul capabil să permită deschiderea încuietorii, să nu poată fi schimbat sau modificat decât printr-un cod de autorizare, existența unor mijloace din construcție care să asigure blocarea încuietorii sau să poată realiza mişcarea unui element de blocare a încuietorii.
Se iau în considerare:

- *rezistența la manipulare* (manipularea este metoda de atac ce are drept scop anularea funcției de blocare a încuietorii, fără producerea de stricăciuni evidente);
- *rezistența la spionare* (orice informații introduse într-o încuietoare electronică trebuie să nu mai fie recunoscută după 30 de secunde de la introducerea, chiar şi dacă numai o parte din codul de deschidere a fost modificat);
- *rezistența la efracție distructivă* (efracție distructivă este metoda de atac ce are drept scop anularea funcției de blocare prin care încuietorii i se produc stricăciuni ce nu mai pot fi ascunse);
- *rezistența electrică şi electromagnetică* (sursele de alimentare ale încuietorilor trebuie să rămână în condiții normale de funcționare pe perioada variațiilor, căderilor de tensiune sau întreruperilor de scurtă durată ale alimentării.)

Ca soluții constructive de dispozitivele de încuiere pentru seifuri putem avea încuietoarea mecanică cu cifru mecanic, cu cifru electronic, încuietoarea cu carduri de proximitate sau încuietoarea biometrică. Există şi dispozitive cu deschidere temporizată, pentru a preveni tentativele de deschidere prin efracție.

În cazul **uşilor de acces**, aceste dispozitive de închidere sunt sub forma unor broaşte îngropate sau aplicate prevăzute cu cilindri de siguranță (butuci), sau broaşte îngropate/aplicate prevăzute cu verturi. Acestea pot sa fie cu închidere/blocare pe toc monopunct sau multipunct, pe 2, 3 sau 4 laturi. Există şi variante electro-mecanice.

Cilindri de siguranță (butucii) se fabrică într-o varietate de modele şi nivele de securitate. Standardul SR EN 1303 reglementează nivelele de securitate; acestea trebuie să fie în concordanță cu specificațiile de securitate ale beneficiarului. Un cilindru de înaltă securitate trebuie să folosească o cheie cu un profil restricționat (posibilitatea procurării cheilor brute limitată, implicit duplicarea neautorizată), nivel crescut de securitate datorită componentelor mecanice interne, un număr mare de combinații pentru a evita aparitia în timp a aceleiaşi combinații şi a fi pretabil la un sistem de acces de tip Master Key.

2.9. Echiparea casieriilor

În proiectarea compartimentului casieriei, a amplasării acestuia față de alte săli adiacente (sala clienților, camera de numărat bani), se impune luarea în considerație a unor măsuri cu caracter conceptual şi constructiv privind atât securitatea personalului cât şi a valorilor sau bunurilor materiale:

- Zona de primire clienți trebuie să fie separată de zona unde lucrează angajații, iar clienții să aibă accesul controlat (printr-un filtru la intrare).
- Clienții vor avea la dispoziție fie încăperi separate, fie spații special dotate cu mese compartimentate cu geamuri/materiale transparente pentru verificarea numerarului de către clienți – spații ce pot fi supravegheate.

Compartimentul de casierie este un spațiu închis/deschis special amenajat, separat de celelalte compartimente din bancă, unde se desfăşoară următoarele activități: depozitarea, pentru scurt timp, a valorilor; încasări şi plăți de numerar; grupe de verificare a numerarului; primiri şi eliberări de metale prețioase şi alte valori." Fiecare bancă poate organiza diferite tipuri de casierie (casierii operative de încasări şi/sau plăți, de încasări serale, de primire valori spre păstrare, de schimb valutar etc.) corespunzător solicitărilor, însă trebuie ținut cont că acest compartiment poate fi amenințat de atacuri cu mână armată, dublate de luarea de ostateci, ținta atacului constituind-o conținutul seifurilor, banii în numerar etc. Protecția antiglonț a compartimentului devine obligatoriu o prioritate, deci trebuie introduse în proiect principii tehnico-constructive conform normelor sau se pot folosi casierii deschise echipate cu TCD sau TCR sau cu seifuri speciale de casierie cu temporizator.

Pereții de acces ai compartimentului (zonei) de casierie trebuie să corespundă cu rezistența şi duritatea pereților de cărămidă plină cu grosimea de 40 cm. Uşile de intrare în compartiment se vor confecționa din metal sau lemn de esență tare – (cu grosimea de minim 4 cm) şi/sau placată cu sticlă de securitate şi se vor dota cu încuietori de siguranță (încuietoare cu cilindru, cu cel puțin 5 ştifturi, protejată împotriva găuririi, prevăzută cu 4 puncte de închidere sigură). Tocul uşii de acces în compartiment se va confecționa din metal sau lemn de esență tare. La casierii se va folosi zidărie sau alte materiale rezistente antiglonț (calibru 7,62 mm) şi sertar de preluare-predare de siguranță antiglont (preluare indirectă). Structurile de limitare în toate direcțiile vor fi executate de la nivelul podelei până la nivelul plafonului rigid.

La executarea casieriilor se poate renunța la prevederile anterioare, dacă se folosesc echipamente de casierie care previn săvârşirea infracțiunilor: case de bani cu temporizare, sisteme automate de depozit/plată cu comandă computerizată sau panouri de separare din materiale antiglonț care se interpun între sala clienților şi casierie la declanşarea alarmei.

Grupele de verificare îşi desfăşoară activitatea în spații separate de celelalte activități din compartiment în condiții de sigurare a securității valorilor. Casierii grupelor de verificare vor avea seifuri, iar verificatorii de bani vor avea mese de verificat numerarul, compartimentate cu geamuri transparente.

Uşile de acces spre spațiul casieriei sunt uşi de siguranță, echipate cu sisteme de închidere acționate mecanic sau cu cartelă.

Toată structura de protecție se recomandă să fie rezistentă antiglonț (calibru 7,62 mm) şi prevăzută cu un sertar de preluare-predare de siguranță (evitarea contactului fizic). "tructurile de limitare în toate direcțiile vor fi executate de la nivelul podelei la nivelul plafonului rigid. La casieriile executate în linie se poate renunța la prescripțiile punctului anterior pentru pereții despărțitori dintre cabine. Uşile casieriilor se vor dota cu încuietori de siguranță, asigurându-se închiderea separată. Casieriile pot fi acoperite special. Nu se admit orificii.

Iată în continuare sugestii de amenajare a ghişeelor: ghişee blindate complet, de la sol la plafonul fals, ce sunt prevăzute cu sertar de transfer, blat interfon; ghişeu modular, cu sertar de transfer, geam blindat cu fante orizontale pentru transmisia fonică de numerar după programul normal de lucru sau amplasării în spații deschise); ferestre blindate cu rame antiglonț pentru montare în gol de zidărie.

Pentru comunicarea dintre client şi casier se poate alege una din variantele: transmisie fonică indirectă (geam antiglonț dintr-o singură placă continuă) folosind interfon; transmisie fonică directă (geam antiglonț cu 2-3 plăci cu suprapunere, creându-se o fantă fonică şi o grilă de aerisire; cu orificiu de comunicare / aerisire acoperit de o sticlă de suprafață mai mare).

Considerentele de siguranță impun ca transferul de valori să se realizeze fără contact direct care ar putea facilita jaful şi pune în pericol viața funcționarilor şi a clienților. În funcție de volumul şi greutatea fondurilor sau a valorilor transferabile disponibile sistemele de transfer se pot clasifica în:

- sertare de transfer pentru operații curente;
- case de transfer pentru operații curente la volume mari;
- case/sasuri de transfer între transport şi trezorerie.

Sertarele de transfer pentru operații curente sunt dispozitive destinate efectuării în deplină siguranță a operațiilor la ghişee, fiind componente integrate într-un set complet de montaj (alături de: geam blindat, sistem de intercomunicații, sisteme de iluminare etc.) folosite în bănci, case de schimb s.a. Executate din materiale dure, ele se clasifică după rezistența antiglonț, corespunzător standardului DIN 52290, partea 2, pentru înrămări şi materiale, în clasele M1-M5, însă gradul de siguranță al ansamblului în care sunt înglobate este dat de cel mai mic grad de siguranță acordat fiecărui element component. Aplicând prevederile legale coroborate cu tabelul de echivalență la clase şi tipuri de arme, ar rezulta că pot fi folosite doar cele din clasa M4 şi superioare. Există o varietate de modele constructive pentru sertarele de transfer: sertare activate mecanic (cu contraplacă de protecție): fixe, cu un sertar mobil, cu un sertar fix şi un sertar mobil, cu două sertare mobile care se desfăşoară în sens opus – construcția lor fiind astfel concepută încât transferul documentelor şi al banilor să se facă simultan; sertare cu activare electrică (cu unul sau două sertare mobile).

Casierii deschise: păstrarea banilor se permite numai în:

- seifuri automate de depozit / plată
- seifuri cu încuietori temporizate
- distribuitoare automate de numerar deservite de casieri

3. Standarde de referință

SR EN 1047 - 1 - Unități de depozitare de securitate. Clasificare şi metode de încercare pentru determinarea rezistenței la foc. Partea 1 Dulapuri pentru date.

SR EN 1047 - 2 - Unități de depozitare de securitate. Clasificare şi metode de încercare pentru determinarea rezistenței la foc. Partea 2 Camere şi containere pentru date.

EN 356 – Geamuri rezistente la atacurile manuale

EN 1063 – Geamuri rezistente la atacurile armelor de foc

SR EN 1143-1:1997/A2 - Unități de depozitare de securitate. Cerințe, clasificare şi metode de încercare pentru determinarea rezistenței la efracție. Partea 1: Seifuri, uşi de tezaur şi camere de tezaur.

Standard SR ENV 1627 - Ferestre, uşi şi jaluzele - Rezistența la efracție - cerințe şi clasificare.

SR ENV 1628 - Ferestre, uşi şi jaluzele - Rezistența la efracție - Metoda de încercare pentru determinarea rezistenței la încărcare statică.

SR ENV 1629 - Ferestre, uşi şi jaluzele - Rezistența la efracție - Metoda de încercare pentru determinarea rezistenței la încărcare dinamică.

SR ENV 1630 - Ferestre, uşi şi jaluzele - Rezistența la efracție - Metoda de încercare pentru determinarea rezistenței la atacuri manuale.

SR ENV 1627 - stabileşte cerințele şi clasele de rezistență pe baza încercărilor stabilite prin celelalte standarde.

SR EN 1522 - Ferestre, uşi, obloane şi jaluzele - Rezistența la glonț– Cerințe şi clasificare.

SR EN 1523 - Ferestre, uşi, obloane şi jaluzele - Rezistența la glonț – Metoda de încercare.

EN 1300 – Încuietori

EN 1303 – Cilindri de siguranță

SECURITATE SI SANATATE IN MUNCA

A. LEGEA SECURITATII SI SANTATII IN MUNCA, NR.319/2006

GENERALITATI, TERMINOLOGIE

In domeniul securitatii si sanatatii in munca, **legea de baza** in vigoare, in tara noastra, este **Legea nr.319** denumita **Legea securitatii si sanatatii in munca** adoptata in data de 14 iulie 2006 si publicata in Monitorul Oficial nr.646 din 26 iulie 2006.

Legea securitatii si sanatatii in munca, nr.319/2006, transpune **Directiva Consiliului nr.89/391/CEE** privind introducerea de masuri pentru promovarea imbunatatirii securitatii si sanatatii lucratorilor la locul de munca,

Legea securitatii si sanatatii in munca a intrat în vigoare la data de 01.10.2006.

Legea securitatii si sanatatii in munca are ca scop instituirea de măsuri privind promovarea îmbunătăţirii securităţii şi sănătăţii în muncă a lucrătorilor.

Convenţiile internaţionale şi contractele bilaterale încheiate de persoane juridice române cu parteneri străini, în vederea efectuării de lucrări cu personal român pe teritoriul altor ţări, vor cuprinde clauze privind securitatea şi sănătatea în muncă.

Legea securitatii si sanatatii in munca se aplică în toate sectoarele de activitate, atât publice, cât şi private.

Prevederile legii securitatii si sanatatii in munca se aplică angajatorilor, lucrătorilor şi reprezentanţilor lucrătorilor.

Fac **excepţie** de la prevederile legii securitatii si sanatatii in munca cazurile în care particularităţile inerente ale anumitor activităţi specifice din serviciile publice, cum ar fi forţele armate sau poliţia, precum şi cazurile de dezastre, inundaţii şi pentru realizarea măsurilor de protecţie civilă, vin în contradicţie cu legea securitatii si sanatatii in munca.

Termeni şi expresii definitorii:

a) **lucrător** - persoană angajată de către un angajator, potrivit legii, inclusiv studenţii, elevii în perioada efectuării stagiului de practică, precum şi ucenicii şi alţi participanţi la procesul de muncă, cu excepţia persoanelor care prestează activităţi casnice;

b) **angajator** - persoană fizică sau juridică ce se află în raporturi de muncă ori de serviciu cu lucrătorul respectiv şi care are responsabilitatea întreprinderii şi/sau unităţii;

c) **alţi participanţi la procesul de muncă** - persoane aflate în întreprindere şi/sau unitate, cu permisiunea angajatorului, în perioada de verificare prealabilă a aptitudinilor profesionale în vederea angajării, persoane care prestează activităţi în folosul comunităţii sau activităţi în regim de voluntariat, precum şi şomeri pe durata participării la o formă de pregătire profesională şi persoane care nu au contract individual de muncă încheiat în formă scrisă şi pentru care se poate face dovada prevederilor contractuale şi a prestaţiilor efectuate prin orice alt mijloc de probă;

d) **reprezentant al lucrătorilor cu răspunderi specifice în domeniul securităţii şi sănătăţii lucrătorilor** - persoană aleasă, selectată sau desemnată de lucrători, în conformitate cu prevederile legale, să îi reprezinte pe aceştia în ceea ce priveşte problemele referitoare la protecţia securităţii şi sănătăţii lucrătorilor în muncă;

e) **prevenire** - ansamblul de dispoziţii sau măsuri luate ori prevăzute în toate etapele procesului de muncă, în scopul evitării sau diminuării riscurilor profesionale;

f) **eveniment** - accidentul care a antrenat decesul sau vătămări ale organismului, produs în timpul procesului de muncă ori în îndeplinirea îndatoririlor de serviciu, situaţia de persoană dată dispărută sau accidentul de traseu ori de circulaţie, în condiţiile în care au fost implicate persoane angajate, incidentul periculos, precum şi cazul susceptibil de boală profesională sau legată de profesiune;

g) **accident de muncă** - vătămarea violentă a organismului, precum şi intoxicaţia acută profesională, care au loc în timpul procesului de muncă sau în îndeplinirea îndatoririlor de serviciu şi care provoacă incapacitate temporară de muncă de cel puţin 3 zile calendaristice, invaliditate ori deces;

h) **boală profesională** - afecţiunea care se produce ca urmare a exercitării unei meserii sau profesii, cauzată de agenţi nocivi fizici, chimici ori biologici caracteristici locului de muncă, precum şi de suprasolicitarea diferitelor organe sau sisteme ale organismului, în procesul de muncă;

i) **echipament de muncă** - orice maşină, aparat, unealtă sau instalaţie folosită în muncă;

j) **echipament individual de protecţie** - orice echipament destinat a fi purtat sau mânuit de un lucrător pentru a-l proteja împotriva unuia ori mai multor riscuri care ar putea să îi pună în pericol securitatea şi sănătatea la locul de muncă, precum şi orice supliment sau accesoriu proiectat pentru a îndeplini acest obiectiv;

k) **loc de muncă** - locul destinat să cuprindă posturi de lucru, situat în clădirile întreprinderii şi/sau unităţii, inclusiv orice alt loc din aria întreprinderii şi/sau unităţii la care lucrătorul are acces în cadrul desfăşurării activităţii;

l) **pericol grav şi iminent de accidentare** - situaţia concretă, reală şi actuală căreia îi lipseşte doar prilejul declanşator pentru a produce un accident în orice moment;

m) **stagiu de practică** - instruirea cu caracter aplicativ, specifică meseriei sau specialităţii în care se pregătesc elevii, studenţii, ucenicii, precum şi şomerii în perioada de reconversie profesională;

n) **securitate şi sănătate în muncă** - ansamblul de activităţi instituţionalizate având ca scop asigurarea celor mai bune condiţii în desfăşurarea procesului de muncă, apărarea vieţii, integrităţii fizice şi psihice, sănătăţii lucrătorilor şi a altor persoane participante la procesul de muncă;

o) **incident periculos** - evenimentul identificabil, cum ar fi explozia, incendiul, avaria, accidentul tehnic, emisiile majore de noxe, rezultat din disfuncţionalitatea unei activităţi sau a unui echipament de muncă sau/şi din comportamentul neadecvat al factorului uman care nu a afectat lucrătorii, dar ar fi fost posibil să aibă asemenea urmări şi/sau a cauzat ori ar fi fost posibil să producă pagube materiale;

p) **servicii externe** - persoane juridice sau fizice din afara întreprinderii/unităţii, abilitate să presteze servicii de protecţie şi prevenire în domeniul securităţii şi sănătăţii în muncă, conform legii;

q) **accident uşor** - eveniment care are drept consecinţă leziuni superficiale care necesită numai acordarea primelor îngrijiri medicale şi a antrenat incapacitate de muncă cu o durată mai mică de 3 zile;

r) **boală legată de profesiune** - boala cu determinare multifactorială, la care unii factori determinanţi sunt de natură profesională.

OBLIGAŢIILE ANGAJATORULUI (Extras din Legea nr.319/14 iulie 2006)

1. Obligaţii generale.

a) să asigure securitatea şi sănătatea lucrătorilor în toate aspectele legate de muncă;
   - în cazul în care apelează la servicii externe, angajatorul nu este exonerat de responsa bilităţile sale în domeniu;
   - obligaţiile lucrătorilor în domeniul securităţii şi sănătăţii în muncă nu aduc atingere principiului responsabilităţii angajatorului.

b) în cadrul responsabilităţilor sale, angajatorul are obligaţia să ia măsurile necesare pentru:
   - asigurarea securităţii şi protecţia sănătăţii lucrătorilor;
   - prevenirea riscurilor profesionale;
   - informarea şi instruirea lucrătorilor;

- asigurarea cadrului organizatoric şi a mijloacelor necesare securităţii şi sănătăţii în muncă;

2. Obligaţii generate de natura activităţilor desfăşurate.

a) să evalueze riscurile pentru securitatea şi sănătatea lucrătorilor, inclusiv alegerea echipamentului de muncă şi/sau a substanţelor chimice utilizate la amenajarea locurilor de muncă;
b) să ia în considerare capacităţile lucrătorului în ceea ce priveşte securitatea şi sănătatea în muncă, atunci când îi încredinţează sarcini;
c) să consulte lucrători şi/sau reprezentanţii acestora în ceea ce priveşte consecinţele asupra securităţii şi sănătăţii lucrătorilor, determinate de alegerea echipamentelor, de condiţiile şi mediul de muncă;
d) să ia măsurile corespunzătoare pentru ca în zonele cu risc ridicat, accesul să fie permis numai lucrătorilor care au primit şi şi-au însuşit instrucţiunile adecvate;
e) măsurile privind securitatea, sănătatea şi igiena în muncă, nu trebuie să comporte în nici o situaţie obligaţii financiare pentru lucrători.
f) în funcţie de mărimea unităţii şi/sau riscurile la care sunt expuşi lucrătorii să desemneze unul sau mai mulţi lucrători pentru a se ocupa de activităţile de protecţie şi de prevenire a riscurilor profesionale - denumiţi lucrători desemnaţi;
g) dacă în unitate nu se poate organiza activitatea de prevenire şi de protecţie din lipsa personalului competent, conform legii, angajatorul trebuie să apeleze la servicii externe;
h) să ia toate măsurile necesare pentru coordonarea primului ajutor, stingerea incendiilor, evacuarea personalului şi să stabilească legăturile necesare cu serviciile specializate (serviciul medical de urgenţă, salvare şi pompieri);
i) să desemneze un număr de lucrători adecvat mărimii şi/sau riscurilor specifice unităţii care în situaţii de pericol grav şi iminent trebuie să:
   - să informeze cât mai curând posibil toţi lucrătorii care pot fi expuşi unui pericol grav şi iminent şi riscurile implicate în acest pericol;
   - să furnizeze instrucţiuni pentru oprirea lucrului şi părăsirea imediată a locului de muncă în locuri sigure.

3. Alte obligaţii ale angajatorilor:

a) să *realizeze* şi să fie în posesia unei evaluări a riscurilor specifice activităţii pe care o desfăşoară;
b) să decidă asupra măsurilor de protecţie care trebuie luate şi, după caz, asupra echipamentului de protecţie care trebuie utilizat;
c) să ţină evidenţa tuturor evenimentelor care au loc în timpul procesului de muncă şi/sau în îndeplinirea îndatoririlor de serviciu ale lucrătorilor;
   - accidente de muncă şi/sau profesionale cu incapacitate temporară de muncă de cel putin 3 zile calendaristice (accidente de traseu, accidente uşoare, accidente colective, incidente periculoase etc.);
   - accidente de muncă ce au ca urmare invaliditate sau deces.
d) să elaboreze rapoarte privind accidentele de muncă suferite de lucrători săi, şi să le înainteze autorităţilor competente, conform prevederilor stabilite prin Ordin al Ministerului Muncii, Solidarităţii Sociale şi Familiei.

3.1. Obligaţii generate de asigurarea condiţiilor de securitate şi sănătate în muncă, prevenirea accidentelor de muncă şi bolilor profesionale.

a) să adopte pentru toate fazele de derulare a activităţilor şi/sau proceselor de muncă, soluţii conforme prevederilor legale în vigoare privind securitatea şi sănătatea în muncă, prin a căror aplicare să fie eliminate sau diminuate riscurile de accidentare şi de îmbolnăvire a lucrătorilor;

b) să întocmească un plan de prevenire şi protecţie compus din măsuri tehnice, sanitare şi organizatorice, bazat pe evaluarea riscurilor, pe care să le aplice corespunzător condiţiilor de muncă specifice activităţilor desfăşurate;

c) să obţină autorizaţia de funcţionare din punct de vedere al securităţii şi sănătăţii în muncă înainte de începerea oricărei activităţii conform prevederilor legale;

d) să stabilească pentru lucrători, prin fişa postului, atribuţiile şi răspunderiile ce le revin în domeniul securităţii şi sănătăţii în muncă, corespunzător funcţiilor exercitate;

e) să elaboreze instrucţiuni proprii pentru completarea şi/sau aplicarea reglementărilor de securitate şi sănătate în muncă ţinând seama de particularităţile activităţilor şi ale locurilor de muncă aflate în responsabilitatea lor;

f) să asigure şi să controleze cunoaşterea şi aplicarea de către toţi lucrătorii a măsurilor prevăzute în planul de prevenire şi de protecţie stabilit, precum şi a prevederilor legale în domeniul securităţii şi sănătăţii în muncă, prin lucrătorii desemnaţi, prin propria competenţă sau prin servicii externe;

g) să ia măsuri pentru asigurarea de materiale necesare instruirii lucrătorilor cu privire la securitatea şi sănătatea în muncă (afişe, filme etc.);

h) să asigure informarea fiecărei persoane, anterior angajării în muncă, asupra riscurilor la care aceasta este expusă la locul de muncă, precum şi asupra măsurilor de prevenire şi de protecţie necesare;

i) să ia măsuri pentru autorizarea exercitării meseriilor şi profesiilor prevăzute în legislaţia specifică;

j) să angajeze numai persoane care, în urma examenului medical şi, după caz, a testării psihologice a aptitudinilor, corespund sarcinii de muncă pe care urmează să o execute şi să asigure controlul medical periodic şi/sau controlul psihologic periodic, ulterior angajării;

k) să ţină evidenţa zonelor cu risc ridicat şi specific activităţilor desfăşurate în unitate;

l) să asigure funcţionarea permanentă şi corectă a sistemelor şi dispozitivelor de protecţie, a aparaturii de măsură şi control, precum şi a instalaţiilor de captare, reţinere şi neutralizare a substanţelor nocive degajate în desfăşurarea proceselor tehnologice;

m) să prezinte documentele şi să dea relaţiile solicitate de inspectorii de muncă în timpul controlului sau al cercetării evenimentelor;

n) să asigure realizarea măsurilor dispuse de inspectorii de muncă cu prilejul vizitelor de control şi al cercetării evenimentelor;

o) să desemneze, la solicitarea inspectorului de muncă, lucrătorii care să participe la efectuarea controlului sau la cercetarea evenimentelor;

p) să nu modifice starea de fapt rezultată din producerea unui accident mortal sau colectiv, în afară de cazurile în care menţinerea acestei stării ar genera alte accidente ori ar pere-clita viaţa accidentaţilor şi a altor persoane;

q) să asigure echipamente de muncă fără pericol pentru securitatea şi sănătatea lucrătorilor;

r) să asigure echipament individual de protecţie, iar în cazul degradării sau al pierderii calităţilor de protecţie, să acorde obligatoriu alt echipament nou;

s) să acorde în mod obligatoriu şi gratuit alimentaţia de protecţie pentru lucrătorii care lucrează în condiţii de muncă ce impun acest lucru, stabilită prin contract colectiv de muncă şi/sau contract individual de muncă;

t) să acorde în mod obligatoriu şi gratuit, materialele igienico-sanitare necesatre lucrătorilor care lucrează în locuri de muncă ce impun acordarea acestora, stabilite prin contract colectiv de muncă şi/sau contract individual de muncă;

3.2. Informarea, consultarea şi participarea lucrătorilor:

a) să ia măsuri corespunzătoare astfel încât angajatorii din exterior care desfăşoară activităţi în unitatea sa, să primească informaţii adecvate privind aspectele legate de securitatea şi sănătatea în muncă care privesc aceşti lucrători;

b) consultă lucrătorii şi/sau reprezentanţii lor şi permit participarea acestora la discutarea problemelor referitoare la securitatea şi sănătatea în muncă;

c) pentru informarea, consultarea şi participarea lucrătorilor şi/sau reprezentanţilor acestora pentru realizarea prevederilor legate de securitatea şi sănătatea în muncă la nivelul angajatorului, se înfiinţează, se organizează şi funcţionează comitetul de securitate şi sănătate în muncă în conformitate cu prevederile legale în domeniu.

d) să asigure condiţii pentru ca fiecare lucrător să primească o instruire suficientă şi adecvată, în special sub formă de informaţii şi instrucţiuni de lucru, specifice locului de muncă şi postului său;

e) supravegherea sănătăţii lucrătorilor este obligatorie şi este asigurată prin medicii de medicina muncii la intervale regulate conform reglementărilor legale de specialitate.

3.3. Obligaţii privind comunicarea, cercetarea şi raportarea evenimentelor.

a) orice eveniment produs în timpul procesului de muncă ori în îndeplinirea îndatoririlor de serviciu, se comunică, de îndată angajatorului, de conducătorul locului de muncă sau orice altă persoană care are cunoştinţă despre producerea acestuia;

b) angajatorul are obligaţia să comunice evenimentele, de îndată, după cum urmează:
- Inspectoratul Teritorial de Muncă;
- Asigurătorului;
- Organelor de urmărire penală, după caz.

c) în cazul accidentelor de circulaţie produse pe drumurile publice, organele de poliţie rutieră vor trimite în termen de 5 zile, un exemplar al procesului verbal de cercetare la faţa locuim;

d) cercetarea evenimentelor este obligatorie şi se desfăşoară după cum urmează:
- de către angajator, în cazul evenimentelor care au produs incapacitate temporară de muncă;
- de către Inspectoratul Teritorial de Muncă în cazul evenimentelor cu invaliditate, deces, colective, incuidente periculoase, persoane dispărute etc.;
- de Inspecţia Muncii în cazul accidentelor colective, generate de evenimente deosebite (avarii şi explozii);
- de autorităţile de sănătate publică în cazul bolilor profesionale.

e) rezultatul cercetării evenimentului se consemnează într-un proces verbal;

f) în cazul decesului persoanei accidentate, instituţia medico-legală este obligată să înainteze Inspectoratului Teritorial de Muncă în termen de 7 zile de la data decesului, o copie a raportului de constatare medico-legală.

IV. OBLIGAŢIILE LUCRĂTORILOR (Extras din Legea nr.319/14 iulie 2006)

1. Fiecare lucrător trebuie să îşi desfăşoare activitatea în conformitate cu pregătirea şi instruirea sa, precum şi cu instrucţiunile primite din partea angajatorului, astfel încât să nu expună la pericol de accidentare sau îmbolnăvire profesională atât propria persoană, cât şi alte persoane care pot fi afectate de acţiunile sau omisiunile sale în timpul procesului de muncă, drept pentru care îi revin următoarele obligaţii:

a) să utilizeze corect maşinile, aparatura, substanţele periculoase, echipamentele de transport şi alte mijloace de producţie;
b) să utilizeze corect echipamentul individual de protecţie acordat şi după utilizare, să-l pună la locul destinat pentru păstrare;
c) să nu procedeze la scoaterea din funcţiune, la modificarea, schimbarea sau înlăturarea arbitrară a dispozitivelor de securitate proprii, în special ale maşinilor, aparaturii, uneltelor, instalaţiilor tehnice ţşi clădirilor şi să utilizeze corect aceste dispozitive;
d) să comunice imediat angajatorului şi/sau lucrătorilor desemnaţi orice situaţie de muncă pe care o consideră un pericol pentru securitatea şi sănătatea lucrătorilor, precum şi orice deficienţă a sistemelor de protecţie;
e) să aducă la cunoştinţa conducătorului locului de muncă şi/sau angajatorului accidentele suferite de propria persoană;
f) să coopereze cu angajatorul şi/sau cu lucrătorii desemnaţi pentru:
   - a face posibilă realizarea oricăror măsuri sau cerinţe dispuse de către inspectorii de muncă şi inspectorii sanitari, pentru protecţia securităţii şi sănătăţii lucrătorilor;
   - a permite angajatorului să se asigure că mediul de muncă şi condiţiile de lucru sunt sigure şi fără riscuri pentru securitatea şi sănătatea în domeniul său de activitate.
g) să îşi însuşească şi să respecte prevederile legislaţiei în domeniul securităţii şi sănătăţii în muncă şi măsurile de aplicare a acestora;
h) să dea relaţiile solicitate de către inspectori de muncă şi inspectori sanitari.

2. Obligaţiile lucrătorilor în domeniul securităţii şi sănătăţii în muncă nu aduc atingere principiului responsabilităţii angajatorului.

B.NORME METODOLOGICE de aplicare a prevederilor Legii securităţii şi sănătăţii în muncă nr. 319/2006(HG 1425/2006)

TERMINOLOGIE

- În înţelesul normelor metodologice, termenii şi expresiile folosite au următoarea semnificaţie:

- **autorizare a funcţionării din punct de vedere al securităţii şi sănătăţii în muncă** - asumarea de către angajator a responsabilităţii privind legalitatea desfăşurării activităţii din punct de vedere al securităţii şi sănătăţii în muncă;
- **serviciu intern de prevenire şi protecţie** - totalitatea resurselor materiale şi umane alocate pentru efectuarea activităţilor de prevenire şi protecţie în întreprindere şi/sau unitate;
- **comitet de securitate şi sănătate în muncă** - organul paritar constituit la nivelul angajatorului, în vederea participării şi consultării periodice în domeniul securităţii şi sănătăţii în muncă, în conformitate cu art. 18 alin. (1)-(3) din lege;
- **zone cu risc ridicat şi specific** - acele zone din cadrul întreprinderii şi/sau unităţii în care au fost identificate riscuri ce pot genera accidente sau boli profesionale cu consecinţe grave, ireversibile, respectiv deces sau invaliditate;
- **accident care produce incapacitate temporară de muncă (ITM)** - accident care produce incapacitate temporară de muncă de cel puţin 3 zile calendaristice consecutive, confirmată prin certificat medical;

- **accident care produce invaliditate (INV)** - accident care produce invaliditate confirmată prin decizie de încadrare într-un grad de invaliditate, emisă de organele medicale în drept;
- **accident mortal (D**) - accident în urma căruia se produce decesul accidentatului, confirmat imediat sau după un interval de timp, în baza unui act medico-legal;
- **accident colectiv** - accidentul în care au fost accidentate cel puţin 3 persoane, în acelaşi timp şi din aceleaşi cauze, în cadrul aceluiaşi eveniment;
- **accident de muncă de circulaţie** - accident survenit în timpul circulaţiei pe drumurile publice sau generat de traficul rutier, dacă persoana vătămată se afla în îndeplinirea îndatoririlor de serviciu;
- **accident de muncă de traseu**:
  - accident survenit în timpul şi pe traseul normal al deplasării de la locul de muncă la domiciliu şi invers şi care a antrenat vătămarea sau decesul;
  - accident survenit pe perioada pauzei reglementare de masă în locuri organizate de angajator, pe traseul normal al deplasării de la locul de muncă la locul unde ia masa şi invers, şi care a antrenat vătămarea sau decesul;
  - accident survenit pe traseul normal al deplasării de la locul de muncă la locul unde îşi încasează salariul şi invers şi care a antrenat vătămarea sau decesul;
- **accident în afara muncii** - accident care nu îndeplineşte condiţiile prevăzute la art. 5 lit. g) şi la art. 30 din lege;
- **invaliditate** - pierdere parţială sau totală a capacităţii de muncă, confirmată prin decizie de încadrare într-un grad de invaliditate, emisă de organele medicale în drept;
- **invaliditate evidentă** - pierdere a capacităţii de muncă datorată unor vătămări evidente, cum ar fi un braţ smuls din umăr, produse în urma unui eveniment, până la emiterea deciziei de încadrare într-un grad de invaliditate de către organele medicale în drept;
- **intoxicaţie acută profesională** - stare patologică apărută brusc, ca urmare a expunerii organismului la noxe existente la locul de muncă;
- **îndatoriri de serviciu** - sarcini profesionale stabilite în: contractul individual de muncă, regulamentul intern sau regulamentul de organizare şi funcţionare, fişa postului, deciziile scrise, dispoziţiile scrise ori verbale ale conducătorului direct sau ale şefilor ierarhici ai acestuia;
- **comunicare** - procedura prin care angajatorul comunică producerea unui eveniment, de îndată, autorităţilor prevăzute la art. 27 alin. (1) din lege;
- **evidenţă** - mijloacele şi modalităţile de păstrare a informaţiilor referitoare la evenimentele produse;
- **cercetare a bolilor profesionale** - procedură efectuată în mod sistematic, cu scopul de a stabili caracterul de profesionalitate a bolii semnalate;
- **semnalare a bolilor profesionale** - procedură prin care se indică pentru prima oară faptul că o boală ar putea fi profesională;
- **raportare a bolilor profesionale** - procedură prin care se transmit informaţii referitoare la bolile profesionale declarate potrivit legii la Centrul naţional de coordonare metodologică şi informare privind bolile profesionale şi la Centrul Naţional pentru Organizarea şi Asigurarea Sistemului Informaţional şi Informatic în Domeniul Sănătăţii Bucureşti.

AUTORIZARE A FUNCȚIONĂRII DIN PUNCT DE VEDERE AL SECURITĂȚII ŞI SĂNĂTĂȚII ÎN MUNCĂ

În vederea asigurării condițiilor de securitate şi sănătate în muncă şi pentru prevenirea accidentelor şi a bolilor profesionale, angajatorii au obligația să obțină autorizația de funcționare din punct de vedere al securității şi sănătății în muncă, înainte de începerea oricărei activități.

Nu se autorizează, potrivit prevederilor prezentelor norme metodologice, persoanele fizice, asociațiile familiale şi persoanele juridice pentru care autorizarea funcționării, inclusiv din punct de vedere al securității şi sănătății în muncă, se efectuează în temeiul Legii nr. 359/2004 privind simplificarea formalităților la înregistrarea în registrul comerțului a persoanelor fizice, asociațiilor familiale şi persoanelor juridice, înregistrarea fiscală a acestora, precum şi la autorizarea funcționării persoanelor juridice, cu modificările şi completările ulterioare.

Asumarea de către angajator a responsabilității privind legalitatea desfăşurării activității din punct de vedere al securității şi sănătății în muncă se face pentru activitățile care se desfăşoară la sediul social, la sediile secundare sau în afara acestora.

În vederea autorizării din punct de vedere al securității şi sănătății în muncă, angajatorul are obligația să depună la inspectoratul teritorial de muncă pe raza căruia îşi desfăşoară activitatea o cerere, completată în două exemplare semnate în original de către angajator, conform modelului prevăzut în anexa nr. 1.la Normele Metodologice.

Cererea va fi însoțită de următoarele acte:

a)copii de pe actele de înființare;

b)declarația pe propria răspundere, conform modelului prezentat în anexa nr. 2, din care rezultă că pentru activitățile declarate sunt îndeplinite condițiile de funcționare prevăzute de legislația specifică în domeniul securității şi sănătății în muncă.

În vederea autorizării din punct de vedere al securității şi sănătății în muncă, inspectoratele teritoriale de muncă procedează după cum urmează:

a)înregistrează cererile de autorizare a funcționării din punct de vedere al securității şi sănătății în muncă;

b)verifică actele depuse în susținerea acestora, precum şi declarația pe propria răspundere;

c)completează şi emit certificatul constatator, conform modelului prezentat în anexa nr. 3 la Normele Metodologice.;

d)asigură evidența certificatelor constatatoare eliberate, conform modelului prezentat în anexa nr. 4 la Normele Metodologice.;

e)asigură arhivarea documentației în baza căreia s-au emis certificatele constatatoare.

Termenul de eliberare a certificatului constatator este de 5 zile lucrătoare, calculat de la data înregistrării cererii.

Certificatul constatator, emis în baza declarației pe propria răspundere, dă dreptul angajatorilor să desfăşoare activitățile pentru care au obținut certificatul.

ATENTIE

În cazul în care în cadrul controalelor se constată abateri de la respectarea prevederilor legale din domeniul securității şi sănătății în muncă, inspectorul de muncă sistează activitatea şi propune inspectoratului teritorial de muncă înscrierea mențiunii în certificatul constatator.

În situația prevăzută mai sus, angajatorul poate relua activitatea numai după ce demonstrează că a remediat deficiențele care au condus la sistarea activității şi a obținut autorizarea conform Normelor Metodologice..

ACTIVITATI DE PREVENIRE ŞI PROTECŢIE

Angajatorul trebuie să asigure planificarea, organizarea şi mijloacele necesare activităţii de prevenire şi protecţie în unitatea şi/sau întreprinderea sa.

Activităţile de prevenire şi protecţie desfăşurate în cadrul întreprinderii şi/sau al unităţii sunt următoarele:

1. identificarea pericolelor şi evaluarea riscurilor pentru fiecare componentă a sistemului de muncă, respectiv executant, sarcină de muncă, mijloace de muncă/ echipamente de muncă şi mediul de muncă pe locuri de muncă/posturi de lucru;
2. elaborarea şi actualizarea planului de prevenire şi protecţie;
3. elaborarea de instrucţiuni proprii pentru completarea şi/sau aplicarea reglementărilor de securitate şi sănătate în muncă, ţinând seama de particularităţile activităţilor şi ale unităţii/întreprinderii, precum şi ale locurilor de muncă/ posturilor de lucru;
4. propunerea atribuţiilor şi răspunderilor în domeniul securităţii şi sănătăţii în muncă, ce revin lucrătorilor, corespunzător funcţiilor exercitate, care se consemnează în fişa postului, cu aprobarea angajatorului;
5. verificarea cunoaşterii şi aplicării de către toţi lucrătorii a măsurilor prevăzute în planul de prevenire şi protecţie, precum şi a atribuţiilor şi responsabilităţilor ce le revin în domeniul securităţii şi sănătăţii în muncă, stabilite prin fişa postului;
6. întocmirea unui necesar de documentaţii cu caracter tehnic de informare şi instruire a lucrătorilor în domeniul securităţii şi sănătăţii în muncă;
7. elaborarea tematicii pentru toate fazele de instruire, stabilirea periodicităţii adecvate pentru fiecare loc de muncă, asigurarea informării şi instruirii lucrătorilor în domeniul securităţii şi sănătăţii în muncă şi verificarea cunoaşterii şi aplicării de către lucrători a informaţiilor primite;
8. elaborarea programului de instruire-testare la nivelul întreprinderii şi/sau unităţii;
9. asigurarea întocmirii planului de acţiune în caz de pericol grav şi imminent şi asigurarea ca toţi lucrătorii să fie instruiţi pentru aplicarea lui;
10. evidenţa zonelor cu risc ridicat şi specific;
11. stabilirea zonelor care necesită semnalizare de securitate şi sănătate în muncă, stabilirea tipului de semnalizare necesar şi amplasarea conform prevederilor Hotărârii Guvernului nr. 971/2006 privind cerinţele minime pentru semnalizarea de securitate şi/sau sănătate la locul de muncă;
12. evidenţa meseriilor şi a profesiilor prevăzute de legislaţia specifică, pentru care este necesară autorizarea exercitării lor;
13. evidenţa posturilor de lucru care necesită examene medicale suplimentare;
14. evidenţa posturilor de lucru care, la recomandarea medicului de medicina muncii, necesită testarea aptitudinilor şi/sau control psihologic periodic;
15. monitorizarea funcţionării sistemelor şi dispozitivelor de protecţie, a aparaturii de măsură şi control, precum şi a instalaţiilor de ventilare sau a altor instalaţii pentru controlul noxelor în mediul de muncă;
16. verificarea stării de funcţionare a sistemelor de alarmare, avertizare, semnalizare de urgenţă, precum şi a sistemelor de siguranţă;
17. informarea angajatorului, în scris, asupra deficienţelor constatate în timpul controalelor efectuate la locul de muncă şi propunerea de măsuri de prevenire şi protecţie;
18. întocmirea rapoartelor şi/sau a listelor prevăzute de hotărârile Guvernului emise în temeiul art. 51 alin. (1) lit. b) din lege, inclusiv cele referitoare la azbest, vibraţii, zgomot şi şantiere temporare şi mobile;
19. evidenţa echipamentelor de muncă şi urmărirea ca verificările periodice şi, dacă este cazul, încercările periodice ale echipamentelor de muncă să fie efectuate de persoane competente, conform prevederilor din Hotărârea Guvernului nr. 1.146/2006 privind cerinţele minime de securitate şi sănătate pentru utilizarea în muncă de către lucrători a echipamentelor de muncă;

20. identificarea echipamentelor individuale de protecţie necesare pentru posturile de lucru din întreprindere şi întocmirea necesarului de dotare a lucrătorilor cu echipament individual de protecţie, conform prevederilor Hotărârii Guvernului nr. 1.048/2006 privind cerinţele minime de securitate şi sănătate pentru utilizarea de către lucrători a echipamentelor individuale de protecţie la locul de muncă;

21. urmărirea întreţinerii, manipulării şi depozitării adecvate a echipamentelor individuale de protecţie şi a înlocuirii lor la termenele stabilite, precum şi în celelalte situaţii prevăzute de Hotărârea Guvernului nr. 1.048/2006;

22. participarea la cercetarea evenimentelor conform;

23. întocmirea evidenţelor conform competenţelor;

24. elaborarea rapoartelor privind accidentele de muncă suferite de lucrătorii din întreprindere şi/ sau unitate, în conformitate cu prevederile art. 12 alin. (1) lit. d) din lege;

25. urmărirea realizării măsurilor dispuse de către inspectorii de muncă, cu prilejul vizitelor de control şi al cercetării evenimentelor;

26. colaborarea cu lucrătorii şi/sau reprezentanţii lucrătorilor, serviciile externe de prevenire şi protecţie, medicul de medicina muncii, în vederea coordonării măsurilor de prevenire şi protecţie;

27. colaborarea cu lucrătorii desemnaţi/serviciile interne/serviciile externe ai/ale altor angajatori, în situaţia în care mai mulţi angajatori îşi desfăşoară activitatea în acelaşi loc de muncă;

28. urmărirea actualizării planului de avertizare, a planului de protecţie şi prevenire şi a planului de evacuare;

29. propunerea de sancţiuni şi stimulente pentru lucrători, pe criteriul îndeplinirii atribuţiilor în domeniul securităţii şi sănătăţii în muncă;

30. propunerea de clauze privind securitatea şi sănătatea în muncă la încheierea contractelor de prestări de servicii cu alţi angajatori, inclusiv la cele încheiate cu angajatori străini;

31. întocmirea unui necesar de mijloace materiale pentru desfăşurarea acestor activităţi.

Organizarea activităţilor de prevenire şi protecţie

Organizarea activităţilor de prevenire şi protecţie este realizată de către angajator, în următoarele moduri:

a) prin asumarea de către angajator, a atribuţiilor pentru realizarea măsurilor prevăzute de lege;

b) prin desemnarea unuia sau mai multor lucrători pentru a se ocupa de activităţile de prevenire şi protecţie;

c) prin înfiinţarea unui serviciu intern de prevenire şi protecţie;

d) prin apelarea la servicii externe de prevenire şi protecţie.

- **(1)** În cazul **întreprinderilor** cu **până la 9 lucrători** inclusiv angajatorul poate efectua activităţile din domeniul securităţii şi sănătăţii în muncă, dacă se îndeplinesc cumulativ următoarele condiţii:

a) activităţile desfăşurate în cadrul întreprinderii nu sunt dintre cele prevăzute în anexa nr. 5 la lege;

b) angajatorul îşi desfăşoară activitatea profesională în mod efectiv şi cu regularitate în întreprindere şi/sau unitate;

c) angajatorul îndeplineşte cerinţele minime de pregătire în domeniul securităţii şi sănătăţii în muncă, corespunzătoare cel puţin nivelului de bază.

(2) în situaţia în care nu sunt îndeplinite condiţiile prevăzute la alin. (1), angajatorul trebuie să desemneze unul sau mai mulţi lucrători,, sau poate organiza serviciul intern de prevenire şi protecţie, şi/sau să apeleze la servicii externe.

(3) în situaţia în care sunt îndeplinite condiţiile de la alin. (1), dar angajatorul nu realizează

în totalitate activitățile de prevenire şi protecție, pentru activitățile pe care nu le realizează angajatorul trebuie să apeleze la servicii externe.

- **(1)**În cazul **întreprinderilor** care au între **10 şi 49 de lucrători** inclusiv, angajatorul poate efectua activitățile din domeniul securității şi sănătății în muncă, dacă se îndeplinesc cumulativ următoarele condiții:

a) activitățile desfăşurate în cadrul întreprinderii nu sunt dintre cele prevăzute în anexa nr. 5;
b) riscurile identificate nu pot genera accidente sau boli profesionale cu consecințe grave, ireversibile, respectiv deces sau invaliditate;
c) angajatorul îşi desfăşoară activitatea profesională în mod efectiv şi cu regularitate în întreprindere şi/sau unitate;
d) angajatorul îndeplineşte cerințele minime de pregătire în domeniul securității şi sănătății în muncă corespunzătoare cel puțin nivelului de bază.

(2) În situația în care nu sunt îndeplinite condițiile prevăzute la alin. (1), angajatorul trebuie să desemneze unul sau mai mulți lucrători sau poate organiza serviciul intern de prevenire şi protecție, şi/sau să apeleze la servicii externe.

(3) În situația în care sunt îndeplinite condițiile prevăzute la alin. (1) şi (2), dar angajatorul, lucrătorii desemnați sau serviciul intern nu realizează în totalitate activitățile de prevenire şi protecție, angajatorul trebuie să apeleze la servicii externe.

- **(1)** În cazul **întreprinderilor şi/sau unităților între 50 şi 149 de lucrători**, angajatorul trebuie să desemneze unul sau mai mulți lucrători sau să organizeze serviciu intern de prevenire şi protecție pentru a se ocupa de activitățile de prevenire şi protecție din cadrul întreprinderii.

(2)Î n cazul întreprinderilor şi/sau unităților prevăzute la alin. (1), care desfăşoară activități dintre cele prevăzute în anexa nr. 5, angajatorul trebuie să organizeze serviciu intern de prevenire şi protecție.

(3) În cazul în care lucrătorii desemnați/serviciul intern de prevenire şi protecție nu au capacitățile şi aptitudinile necesare pentru efectuarea tuturor activităților de prevenire şi protecție prevăzute la art. 15, angajatorul trebuie să apeleze la unul sau mai multe servicii externe.

- **(1)**În cazul **întreprinderilor şi/sau unităților care au peste 150 de lucrători**, angajatorul trebuie să organizeze serviciul intern de prevenire şi protecție.

(2) În cazul în care serviciul intern de prevenire şi protecție nu are capacitățile şi aptitudinile necesare pentru efectuarea tuturor activităților de prevenire şi protecție, angajatorul trebuie să apeleze la unul sau mai multe servicii externe.

3. Cerințele minime de pregătire în domeniul securității şi sănătății în muncă

Nivelurile de pregătire în domeniul securității şi sănătății în muncă, necesare pentru dobândirea capacităților şi aptitudinilor corespunzătoare efectuării activităților de prevenire şi protecție, sunt următoarele:

a) nivel de bază;
b) nivel mediu;
c))nivel superior.

- **(1) Cerințele minime** de pregătire în domeniul securității şi sănătății în muncă corespunzătoare **nivelului de bază** sunt:

a) studii în învățământul liceal filiera teoretică în profil real sau filiera tehnologică în profil tehnic;
b) curs în domeniul securității şi sănătății în muncă, cu conținut minim conform celui prevăzut în anexa nr. 6 lit. A, cu o durată de cel puțin 40 de ore.

(2) Nivelul de bază prevăzut la alin. (1) se atestă prin diploma de studii şi certificatul de absolvire a cursului prevăzut la alin. (1) lit. b).

- **(1) Cerinţele minime** de pregătire în domeniul securităţii şi sănătăţii în muncă corespunzătoare **nivelului mediu** sunt:

a) studii în învăţământul postliceal în profil tehnic;
b) curs în domeniul securităţii şi sănătăţii în muncă, cu conţinut minim conform celui prevăzut în anexa nr. 6 lit. B, cu o durată de cel puţin 80 de ore.

(2) Nivelul mediu prevăzut la alin. (1) se atestă prin diploma de studii şi certificatul de absolvire a cursului prevăzut la alin. (1) lit. b).

- **(1) Cerinţele minime** de pregătire în domeniul securităţii şi sănătăţii în muncă corespunzătoare **nivelului superior** sunt:

a) studii superioare tehnice;
b) curs în domeniul securităţii şi sănătăţii în muncă, cu conţinut minim conform celui prevăzut în anexa nr. 6 lit. B, cu o durată de cel puţin 80 de ore;
c) curs postuniversitar de evaluare a riscurilor cu o durată de cel puţin 180 de ore.

(2) Nivelul superior prevăzut la alin. (1) se atestă prin diploma de studii şi certificatele de absolvire a cursurilor prevăzute la alin. (1) lit. b) şi c).

(3) Cerinţa minimă prevăzută la alin. (1) lit. b) este considerată îndeplinită şi în situaţia în care persoana a absolvit o formă de învăţământ postuniversitar în domeniul securităţii şi sănătăţii în muncă.

ATENTIE

Cursurile în domeniul securităţii şi sănătăţii în muncă, se efectuează de către furnizori de formare profesională autorizaţi conform prevederilor art. 18 - 27 din Ordonanţa Guvernului nr. 129/2000 privind formarea profesională a adulţilor, aprobată cu modificări şi completări prin Legea nr. 375/2002, republicată, cu modificările şi completările ulterioare.

Lucrători desemnaţi

Desemnarea nominală a lucrătorului/ lucrătorilor pentru a se ocupa de activităţile de prevenire şi protecţie se face prin decizie a angajatorului.

Angajatorul va consemna în fişa postului activităţile de prevenire şi protecţie pe care lucrătorul desemnat are capacitatea, timpul necesar şi mijloacele adecvate să le efectueze.

Observatii

- ✓ Pentru a putea să desfăşoare activităţile de prevenire şi protecţie, lucrătorul desemnat trebuie să îndeplinească cerinţele minime de pregătire în domeniul securităţii şi sănătăţii în muncă corespunzătoare cel puţin nivelului mediu
- ✓ Angajatorul va stabili numărul de lucrători desemnaţi în funcţie de mărimea întreprinderii şi/ sau unităţii şi/sau riscurile la care sunt expuşi lucrătorii, precum şi de distribuţia acestora în cadrul întreprinderii şi/sau unităţii.
- ✓ Angajatorul trebuie să asigure mijloacele adecvate şi timpul necesar pentru ca lucrătorii desemnaţi să poată desfăşura activităţile de prevenire şi protecţie conform fişei postului.

Serviciile interne de prevenire şi protecţie

Serviciul intern de prevenire şi protecţie trebuie să fie format din lucrători care îndeplinesc cerinţele minime de pregătire în domeniul securităţii şi sănătăţii în muncă corespunzătoare nivelului mediu şi/sau superior, şi, după caz, alţi lucrători care pot desfăşura activităţi auxiliare.

Conducătorul serviciului de prevenire şi protecţie trebuie să îndeplinească cerinţele minime de pregătire în domeniul securităţii şi sănătăţii în muncă corespunzătoare nivelului superior.

Serviciul intern de prevenire şi protecţie se organizează în subordinea directă a angajatorului ca o structură distinctă.

Lucrătorii din cadrul serviciului intern de prevenire şi protecţie trebuie să desfăşoare numai activităţi de prevenire şi protecţie şi cel mult activităţi complementare cum ar fi: prevenirea şi stingerea incendiilor şi protecţia mediului.

Angajatorul va consemna în regulamentul intern sau în regulamentul de organizare şi funcţionare activităţile de prevenire şi protecţie pentru efectuarea cărora serviciul intern de prevenire şi protecţie are capacitate şi mijloace adecvate.

Serviciul intern de prevenire şi protecţie trebuie să aibă la dispoziţie resursele materiale şi umane necesare pentru îndeplinirea activităţilor de prevenire şi protecţie desfăşurate în întreprindere.

Angajatorul va stabili structura serviciului intern de prevenire şi protecţie în funcţie de mărimea întreprinderii şi/sau unităţii şi/sau riscurile la care sunt expuşi lucrătorii, precum şi de distribuţia acestora în cadrul întreprinderii şi/sau unităţii.

Angajatorul trebuie să asigure mijloacele adecvate pentru ca serviciul intern de prevenire şi protecţie să poată desfăşura activităţile specifice.

Când angajatorul îşi desfăşoară activitatea în mai multe puncte de lucru, serviciul de prevenire şi protecţie trebuie să fie organizat astfel încât să se asigure în mod corespunzător desfăşurarea activităţilor specifice.

În situaţia în care activitatea de prevenire şi protecţie este asigurată prin mai multe servicii interne, acestea vor acţiona coordonat pentru asigurarea eficienţei activităţii.

Serviciul intern de prevenire şi protecţie poate să asigure şi supravegherea medicală, dacă dispune de personal cu capacitate profesională şi de mijloace materiale adecvate.

Servicii externe de prevenire şi protecţie

Serviciul extern de prevenire şi protecţie asigură, pe bază de contract, activităţile de prevenire şi protecţie în domeniu.

Serviciul extern trebuie să aibă acces la toate informaţiile necesare desfăşurării activităţii de prevenire şi protecţie.

Serviciul extern de prevenire şi protecţie trebuie să îndeplinească următoarele cerinţe:

a)să dispună de personal cu capacitate profesională adecvată şi de mijloacele materiale necesare pentru a-şi desfăşura activitatea;

b)să fie abilitat de Comisia de abilitare a serviciilor externe de prevenire şi protecţie şi de avizare a documentaţiilor cu caracter tehnic de informare şi instruire în domeniul securităţii şi sănătăţii în muncă.

Serviciul extern de prevenire şi protecţie trebuie să fie format din lucrători care îndeplinesc cerinţele minime de pregătire în domeniul securităţii şi sănătăţii în muncă corespunzătoare nivelului mediu şi/sau superior, şi, după caz, alţi lucrători care pot desfăşura activităţi auxiliare.

Conducătorul serviciului extern de prevenire şi protecţie trebuie să îndeplinească cerinţele minime de pregătire în domeniul securităţii şi sănătăţii în muncă corespunzătoare nivelului superior.

În cazul în care serviciul extern de prevenire şi protecţie este format dintr-o singură persoană, aceasta trebuie să îndeplinească cerinţele minime de pregătire în domeniul.

COMITETUL DE SECURITATE ŞI SĂNĂTATE ÎN MUNCĂ

Organizarea comitetului de securitate şi sănătate în muncă

Comitetul de securitate şi sănătate în muncă se constituie în unităţile care au un număr de cel puţin 50 de lucrători, inclusiv cu capital străin, care desfăşoară activităţi pe teritoriul României.

Inspectorul de muncă poate impune constituirea comitetului de securitate şi sănătate în muncă în unităţile cu un număr mai mic de 50 de lucrători în funcţie de natura activităţii şi de riscurile identificate.

În cazul în care activitatea se desfăşoară în unităţi dispersate teritorial, se pot înfiinţa mai multe comitete de securitate şi sănătate în muncă; numărul acestora se stabileşte prin contractul colectiv de muncă aplicabil sau prin regulamentul intern ori regulamentul de organizare şi funcţionare.

Comitetul de securitate şi sănătate în muncă se constituie şi în cazul activităţilor care se desfăşoară temporar, respectiv cu o durată mai mare de 3 luni.

În unităţile care au mai puţin de 50 de lucrători, atribuţiile comitetului de securitate şi sănătate în muncă revin reprezentanţilor lucrătorilor, cu răspunderi specifice în domeniul securităţii şi sănătăţii lucrătorilor.

Componenta comitetului de securitate si sanatate in munca

Comitetul de securitate şi sănătate în muncă este constituit din reprezentanţii lucrătorilor cu răspunderi specifice în domeniul securităţii şi sănătăţii lucrătorilor, pe de o parte, şi angajator sau reprezentantul său legal şi/sau reprezentanţii săi în număr egal cu cel al reprezentanţilor lucrătorilor şi medicul de medicina muncii, pe de altă parte.

Angajatorul sau reprezentantul său legal este preşedintele comitetului de securitate şi sănătate în muncă.

Lucrătorul desemnat sau reprezentantul serviciului intern de prevenire şi protecţie este secretarul comitetului de securitate şi sănătate în muncă.

Reprezentanţii lucrătorilor în comitetele de securitate şi sănătate în muncă vor fi desemnaţi de către lucrători dintre reprezentanţii lucrătorilor cu răspunderi specifice în domeniul securităţii şi sănătăţii lucrătorilor, după cum urmează:

a) de la 50 la 100 de lucrători - 2 reprezentanţi;
b) de la 101 la 500 de lucrători - 3 reprezentanţi;
c) de la 501 la 1.000 de lucrători - 4 reprezentanţi;
d) de la 1.001 la 2.000 de lucrători - 5 reprezentanţi;
e) de la 2.001 la 3.000 de lucrători - 6 reprezentanţi;
f) de la 3.001 la 4.000 de lucrători - 7 reprezentanţi;
g) peste 4.000 de lucrători - 8 reprezentanţi.

Reprezentanţii lucrătorilor în comitetul de securitate şi sănătate în muncă vor fi aleşi pe o perioadă de 2 ani.

Modalitatea de desemnare a reprezentanţilor lucrătorilor în comitetele de securitate şi sănătate în muncă va fi stabilită prin contractul colectiv de muncă, regulamentul intern sau regulamentul de organizare şi funcţionare.

Angajatorul are obligaţia să acorde fiecărui reprezentant al lucrătorilor în comitetele de securitate şi sănătate în muncă timpul necesar exercitării atribuţiilor specifice.

Timpul alocat acestei activităţi va fi considerat timp de muncă şi va fi de cel puţin:

a) 2 ore pe lună în unităţile având un efectiv de până la 99 de lucrători;
b) 5 ore pe lună în unităţile având un efectiv între 100 şi 299 de lucrători;
c) 10 ore pe lună în unităţile având un efectiv între 300 şi 499 de lucrători;
d) 15 ore pe lună în unităţile având un efectiv între 500 şi 1.499 de lucrători;
e) 20 de ore pe lună în unităţile având un efectiv de 1.500 de lucrători şi peste.

Instruirea necesară exercitării rolului de membru în comitetul de securitate şi sănătate în muncă trebuie să se realizeze în timpul programului de lucru şi pe cheltuiala unității.

Membrii comitetului de securitate şi sănătate în muncă se nominalizează prin decizie scrisă a preşedintelui acestuia, iar componența comitetului va fi adusă la cunoştință tuturor lucrătorilor.

La întrunirile comitetului de securitate şi sănătate în muncă vor fi convocați să participe lucrătorii desemnați, reprezentanții serviciului intern de prevenire şi protecție şi, în cazul în care angajatorul a contractat unul sau mai multe servicii externe de prevenire şi protecție, reprezentanții acestora.

La întrunirile comitetului de securitate şi sănătate în muncă pot fi invitați să participe inspectori de muncă.

Funcționarea comitetului de securitate şi sănătate în muncă

Comitetul de securitate şi sănătate în muncă funcționează în baza regulamentului de funcționare propriu.

Angajatorul are obligația să asigure întrunirea comitetului de securitate şi sănătate în muncă cel puțin o dată pe trimestru şi ori de câte ori este necesar.

Ordinea de zi a fiecărei întruniri este stabilită de către preşedinte şi secretar, cu consultarea reprezentanților lucrătorilor, şi este transmisă membrilor comitetului de securitate şi sănătate în muncă, inspectoratului teritorial de muncă şi, dacă este cazul, serviciului extern de protecție şi prevenire, cu cel puțin 5 zile înaintea datei stabilite pentru întrunirea comitetului.

Secretarul comitetului de securitate şi sănătate în muncă convoacă în scris membrii comitetului cu cel puțin 5 zile înainte de data întrunirii, indicând locul, data şi ora stabilite.

La fiecare întrunire secretarul comitetului de securitate şi sănătate în muncă încheie un proces-verbal care va fi semnat de către toți membrii comitetului.

Comitetul de securitate şi sănătate în muncă este legal întrunit dacă sunt prezenți cel puțin jumătate plus unu din numărul membrilor săi.

Comitetul de securitate şi sănătate în muncă convine cu votul a cel puțin două treimi din numărul membrilor prezenți.

Secretarul comitetului de securitate şi sănătate în muncă va afişa la loc vizibil copii ale procesului-verbal încheiat.

Secretarul comitetului de securitate şi sănătate în muncă transmite inspectoratului teritorial de muncă, în termen de 10 zile de la data întrunirii, o copie a procesului-verbal încheiat.

Atribuțiile comitetului de securitate şi sănătate în muncă

Pentru realizarea informării, consultării şi participării lucrătorilor, în conformitate cu art. 16, 17 şi 18 din lege, comitetul de securitate şi sănătate în muncă are cel puțin următoarele atribuții:

a) analizează şi face propuneri privind politica de securitate şi sănătate în muncă şi planul de prevenire şi protecție, conform regulamentului intern sau regulamentului de organizare şi funcționare;

b) urmăreşte realizarea planului de prevenire şi protecție, inclusiv alocarea mijloacelor necesare realizării prevederilor lui şi eficiența acestora din punct de vedere al îmbunătățirii condițiilor de muncă;

c) analizează introducerea de noi tehnologii, alegerea echipamentelor, luând în considerare consecințele asupra securității şi sănătății, lucrătorilor, şi face propuneri în situația constatării anumitor deficiențe;

d) analizează alegerea, cumpărarea, întreținerea şi utilizarea echipamentelor de muncă, a echipamentelor de protecție colectivă şi individuală;

e) analizează modul de îndeplinire a atribuțiilor ce revin serviciului extern de prevenire şi protecție, precum şi menținerea sau, dacă este cazul, înlocuirea acestuia;

f) propune măsuri de amenajare a locurilor de muncă, ţinând seama de prezenţa grupurilor sensibile la riscuri specifice;

g) analizează cererile formulate de lucrători privind condiţiile de muncă şi modul în care îşi îndeplinesc atribuţiile persoanele desemnate şi/sau serviciul extern;

h) urmăreşte modul în care se aplică şi se respectă reglementările legale privind securitatea şi sănătatea în muncă, măsurile dispuse de inspectorul de muncă şi inspectorii sanitari;

i) analizează propunerile lucrătorilor privind prevenirea accidentelor de muncă şi a îmbolnăvirilor profesionale, precum şi pentru îmbunătăţirea condiţiilor de muncă şi propune introducerea acestora în planul de prevenire şi protecţie;

j) analizează cauzele producerii accidentelor de muncă, îmbolnăvirilor profesionale şi evenimentelor produse şi poate propune măsuri tehnice în completarea măsurilor dispuse în urma cercetării;

k) efectuează verificări proprii privind aplicarea instrucţiunilor proprii şi a celor de lucru şi face un raport scris privind constatările făcute;

l) dezbate raportul scris, prezentat comitetului de securitate şi sănătate în muncă de către conducătorul unităţii cel puţin o dată pe an, cu privire la situaţia securităţii şi sănătăţii în muncă, la acţiunile care au fost întreprinse şi la eficienţa acestora în anul încheiat, precum şi propunerile pentru planul de prevenire şi protecţie ce se va realiza în anul următor.

Obligaţiile angajatorului referitoare la comitetul de securitate şi sănătate în muncă

- Angajatorul trebuie să furnizeze comitetului de securitate şi sănătate în muncă toate informaţiile necesare, pentru ca membrii acestuia să îşi poată da avizul în cunoştinţă de cauză.
- Angajatorul trebuie să prezinte, cel puţin o dată pe an, comitetului de securitate şi sănătate în muncă un raport scris care va cuprinde situaţia securităţii şi sănătăţii în muncă, acţiunile care au fost întreprinse şi eficienţa acestora în anul încheiat, precum şi propunerile pentru planul de prevenire şi protecţie ce se vor realiza în anul următor.
- Angajatorul trebuie să transmită raportul prevăzut la alin. (1), avizat de membrii comitetului de securitate şi sănătate în muncă, în termen de 10 zile, inspectoratului teritorial de muncă.
- Angajatorul trebuie să supună analizei comitetului de securitate şi sănătate în muncă documentaţia referitoare la caracteristicile echipamentelor de muncă, ale echipamentelor de protecţie colectivă şi individuală, în vederea selecţionării echipamentelor optime.
- Angajatorul trebuie să informeze comitetul de securitate şi sănătate în muncă cu privire la evaluarea riscurilor pentru securitate şi sănătate, măsurile de prevenire şi protecţie atât la nivel de unitate, cât şi la nivel de loc de muncă şi tipuri de posturi de lucru, măsurile de prim ajutor, de prevenire şi stingere a incendiilor şi evacuare a lucrătorilor.
- Angajatorul comunică comitetului de securitate şi sănătate în muncă punctul său de vedere sau, dacă este cazul, al medicului de medicina muncii, serviciului intern sau extern de prevenire şi protecţie, asupra plângerilor lucrătorilor privind condiţiile de muncă şi modul în care serviciul intern sau extern de prevenire şi protecţie îşi îndeplineşte atribuţiile.

INSTRUIREA LUCRĂTORILOR ÎN DOMENIUL SECURITĂŢII ŞI SĂNĂTĂŢII ÎN MUNCĂ

Instruirea în domeniul securităţii şi sănătăţii în muncă are ca scop însuşirea cunoştinţelor şi formarea deprinderilor de securitate şi sănătate în muncă.

Instruirea lucrătorilor în domeniul securităţii şi sănătăţii în muncă la nivelul întreprinderii şi/ sau al unităţii se efectuează în timpul programului de lucru si este considerata timp de munca

Instruirea lucrătorilor în domeniul securităţii şi sănătăţii în muncă cuprinde **3 faze:**

a) instruirea introductiv-generală;

b) **instruirea la locul de muncă;**

c)**instruirea periodică.**

La instruirea personalului în domeniul securității şi sănătății în muncă vor fi folosite mijloace, metode şi tehnici de instruire, cum ar fi: expunerea, demonstrația, studiul de caz, vizionări de filme, diapozitive, proiecții, instruire asistată de calculator.

Fiecare angajator are obligația să asigure baza materială corespunzătoare unei instruiri adecvate.

Angajatorul trebuie să dispună de un program de instruire - testare, pe meserii sau activități.

Rezultatul instruirii lucrătorilor în domeniul securității şi sănătății în muncă se consemnează în mod obligatoriu în fişa de instruire individuală, conform modelului prezentat în anexa nr. 11, cu indicarea materialului predat, a duratei şi datei instruirii.

Completarea fişei de instruire individuală se va face cu pix cu pastă sau cu stilou, imediat după verificarea instruirii.

După efectuarea instruirii, fişa de instruire individuală se semnează de către lucrătorul instruit şi de către persoanele care au efectuat şi au verificat instruirea.

Fişa de instruire individuală va fi păstrată de către conducătorul locului de muncă şi va fi însoțită de o copie a fişei de aptitudini, completată de către medicul de medicina muncii în urma examenului medical la angajare.

Pentru persoanele aflate în întreprindere şi/sau unitate cu permisiunea angajatorului, angajatorul stabileşte, prin regulamentul intern sau prin regulamentul de organizare şi funcționare, reguli privind instruirea şi însoțirea acestora în întreprindere şi/sau unitate.

Pentru lucrătorii din întreprinderi şi/sau unități din exterior, care desfăşoară activități pe bază de contract de prestări de servicii în întreprinderea şi/sau unitatea unui alt angajator, angajatorul beneficiar al serviciilor va asigura instruirea lucrătorilor privind activitățile specifice întreprinderii şi/sau unității respective, riscurile pentru securitate şi sănătate în muncă, precum şi măsurile şi activitățile de prevenire şi protecție la nivelul întreprinderilor şi/sau unității, în general si se va
în fişa de instruire colectivă, conform modelului prezentat în anexa nr. 12la Normele Metodologice.

Fişa de instruire colectivă se întocmeşte în două exemplare, din care un exemplar se va păstra de către angajator/lucrător desemnat/serviciu intern de prevenire şi protecție care a efectuat instruirea şi un exemplar se păstrează de către angajatorul lucrătorilor instruiți sau, în cazul vizitatorilor, de către conducătorul grupului.

Reprezentanții autorităților competente în ceea ce priveşte controlul aplicării legislației referitoare la securitate şi sănătate în muncă vor fi însoțiți de către un reprezentant desemnat de către angajator, fără a se întocmi fişă de instructaj.

Instruirea introductiv-generală

Instruirea introductiv-generală se face:

a) la angajarea lucrătorilor definiți conform art. 5 lit. a) din lege;
b) lucrătorilor detaşați de la o întreprindere şi/sau unitate la alta;
c) lucrătorilor delegați de la o întreprindere şi/sau unitate la alta;
d) lucrătorului pus la dispoziție de către un agent de muncă temporar.

Scopul instruirii introductiv-generale este de a informa despre activitățile specifice întreprinderii şi/sau unității respective, riscurile pentru securitate şi sănătate în muncă, precum şi măsurile şi activitățile de prevenire şi protecție la nivelul întreprinderii şi/sau unității, în general.

Instruirea introductiv-generală se face de către:

a) angajatorul care şi-a asumat atribuțiile din domeniul securității şi sănătății în muncă; sau
b) lucrătorul desemnat; sau
c) un lucrător al serviciului intern de prevenire şi protecție; sau
d) serviciul extern de prevenire şi protecție.

Instruirea introductiv-generală se face individual sau în grupuri de cel mult 20 de persoane.

Durata instruirii introductiv-generale depinde de specificul activități şi de riscurile pentru securitate şi sănătate în muncă, precum şi de măsurile şi activitățile de prevenire şi protecție la nivelul întreprinderii şi/sau al unității, în general.

Angajatorul stabileşte prin instrucţiuni proprii durata instruirii introductiv-generale; aceasta nu va fi mai mică de 8 ore.

In cadrul instruirii introductiv-generale se vor expune, în principal, următoarele probleme:

a) legislaţia de securitate şi sănătate în muncă;

b) consecinţele posibile ale necunoaşterii şi nerespectării legislaţiei de securitate şi sănătate în muncă;

c) riscurile de accidentare şi îmbolnăvire profesională specifice unităţii;

d) măsuri la nivelul întreprinderii şi/sau unităţii privind acordarea primului ajutor, stingerea incendiilor şi evacuarea lucrătorilor.

Conţinutul instruirii introductiv-generale trebuie să fie în conformitate cu tematica aprobată de către angajator.

Instruirea introductiv-generală se va finaliza cu verificarea însuşirii cunoştinţelor pe bază de teste.

Rezultatul verificării va fi consemnat în fişa de instruire.

ATENTIE

Lucrătorii nu vor putea fi angajaţi dacă nu şi-au însuşit cunoştinţele prezentate în instruirea introductiv-generală.

Instruirea la locul de muncă

Instruirea la locul de muncă se face după instruirea introductiv-generală şi are ca scop prezentarea riscurilor pentru securitate şi sănătate în muncă, precum şi măsurile şi activităţile de prevenire şi protecţie la nivelul fiecărui loc de muncă, post de lucru şi/sau fiecărei funcţii exercitate.

Instruirea la locul de muncă se face tuturor lucrătorilor, inclusiv la schimbarea locului de muncă în cadrul întreprinderii şi/sau al unităţii.

Instruirea la locul de muncă se face de către conducătorul direct al locului de muncă, în grupe de maximum 20 de persoane.

Fişa de instruire se păstrează de către conducătorul locului de muncă.

Durata instruirii la locul de muncă depinde de riscurile pentru securitate şi sănătate în muncă, precum şi de măsurile şi activităţile de prevenire şi protecţie la nivelul fiecărui loc de muncă, post de lucru şi/sau fiecărei funcţii exercitate.

Durata instruirii la locul de muncă nu va fi mai mică de 8 ore şi se stabileşte prin instrucţiuni proprii de către conducătorul locului de muncă respectiv, împreună cu:

a) angajatorul care şi-a asumat atribuţiile din domeniul securităţii şi sănătăţii în muncă; sau

b) lucrătorul desemnat; sau

c) un lucrător al serviciului intern de prevenire şi protecţie; sau

d) serviciul extern de prevenire şi protecţie.

Instruirea la locul de muncă se va efectua pe baza tematicilor întocmite de către angajatorul care şi-a asumat atribuţiile din domeniul securităţii şi sănătăţii în muncă/lucrătorul desemnat/serviciul intern de prevenire şi protecţie/serviciul extern de prevenire şi protecţie şi aprobate de către angajator, care vor fi păstrate la persoana care efectuează instruirea.

Instruirea la locul de muncă va cuprinde:

a) informaţii privind riscurile de accidentare şi îmbolnăvire profesională specifice locului de muncă şi/sau postului de lucru;

b) prevederile instrucţiunilor proprii elaborate pentru locul de muncă şi/sau postul de lucru;

c) măsuri la nivelul locului de muncă şi/sau postului de lucru privind acordarea primului ajutor, stingerea incendiilor şi evacuarea lucrătorilor;

d) prevederi ale reglementărilor de securitate şi sănătate în muncă privind activităţi specifice ale locului de muncă şi/sau postului de lucru;

e) instruirea la locul de muncă va include în mod obligatoriu demonstrații practice privind activitatea pe care persoana respectivă o va desfăşura şi exerciții practice privind utilizarea echipamentului individual de protecție, a mijloacelor de alarmare, intervenție, evacuare şi de prim ajutor.

Începerea efectivă a activității la postul de lucru de către lucrătorul instruit se face numai după verificarea cunoştințelor de cate şeful ierarhic superior celui care a făcut instruirea şi se consemnează în fişa de instruire individuală.

Instruirea periodică

Instruirea periodică se face tuturor lucrătorilor şi are drept scop reîmprospătarea şi actualizarea cunoştințelor în domeniul securității şi sănătății în muncă.

Instruirea periodică se efectuează de către conducătorul locului de muncă.

Intervalul dintre două instruiri periodice va fi stabilit prin instrucțiuni proprii, în funcție de condițiile locului de muncă şi/sau postului de lucru, şi nu va fi mai mare de 6 luni.

Pentru personalul tehnico-administrativ intervalul dintre două instruiri periodice va fi de cel mult 12 luni.

Verificarea instruirii periodice se face de către şeful ierarhic al celui care efectuează instruirea şi prin sondaj de către angajator/lucrătorul desemnat/serviciul intern de prevenire şi protecție/serviciile externe de prevenire şi protecție, care vor semna fişele de instruire ale lucrătorilor, confirmând astfel că instruirea a fost făcută corespunzător.

Instruirea periodică se va completa în mod obligatoriu şi cu demonstrații practice.

Instruirea periodică se va efectua pe baza tematicilor întocmite de către angajatorul care şi-a asumat atribuțiile din domeniul securității şi sănătății în muncă/lucrătorul desemnat/serviciul intern de de prevenire şi protecție/serviciul extern de prevenire şi protecție şi aprobate de către angajator, care vor fi păstrate la persoana care efectuează instruirea.

Instruirea periodică se face suplimentar celei programate în următoarele cazuri:

a) când un lucrător a lipsit peste 30 de zile lucrătoare;
b) când au apărut modificări ale prevederilor de securitate şi sănătate în muncă privind activități specifice ale locului de muncă şi/sau postului de lucru sau ale instrucțiunilor proprii, inclusiv datorită evoluției riscurilor sau apariției de noi riscuri în unitate;
c) la reluarea activității după accident de muncă;
d) la executarea unor lucrări speciale;
e) la introducerea unui echipament de muncă sau a unor modificări ale echipamentului existent;
f) la modificarea tehnologiilor existente sau procedurilor de lucru;
g) la introducerea oricărei noi tehnologii sau a unor proceduri de lucru.

Durata instruirii periodice in cazurile a)-g) de la paragraful anterior nu va fi mai mică de 8 ore şi se stabileşte în instrucțiuni proprii de către conducătorul locului de muncă respectiv, împreună cu:

a) angajatorul care şi-a asumat atribuțiile din domeniul securității şi sănătății în muncă; sau
b) lucrătorul desemnat; sau
c) un lucrător al serviciului intern de protecție şi prevenire; sau
d) serviciul extern de protecție şi prevenire.

Instruirea periodică se va efectua pe baza tematicilor întocmite de către angajatorul care şi-a asumat atribuțiile din domeniul securității şi sănătății în muncă/lucrătorul desemnat/serviciul intern de prevenire şi protecție/serviciul extern de prevenire şi protecție şi aprobate de către angajator, care vor fi păstrate la persoana care efectuează instruirea.

COMUNICAREA, CERCETAREA, ÎNREGISTRAREA ŞI RAPORTAREA EVENIMENTELOR

Comunicarea evenimentelor

Orice eveniment, va fi comunicat de îndată angajatorului, de către conducătorul locului de muncă sau de orice altă persoană care are cunoştinţă despre producerea acestuia.

Angajatorul are obligaţia să comunice evenimentele, de îndată, după cum urmează:

a) inspectoratelor teritoriale de muncă, toate evenimentele;
b) asigurătorului, potrivit Legii nr. 346/2002 privind asigurarea pentru accidente de muncă şi boli profesionale, cu modificările şi completările ulterioare, evenimentele urmate de incapacitate temporară de muncă, invaliditate sau deces, la confirmarea acestora;
c) organelor de urmărire penală, după caz.

Cercetarea evenimentelor

Cercetarea evenimentelor este obligatorie şi se efectuează după cum urmează:

a) de către angajator, în cazul evenimentelor care au produs incapacitate temporară de muncă;
b) de către inspectoratele teritoriale de muncă, în cazul evenimentelor care au produs invaliditate evidentă sau confirmată, deces, accidente colective, incidente periculoase, în cazul evenimentelor care au produs incapacitate temporară de muncă lucrătorilor la angajatorii persoane fizice, precum şi în situaţiile cu persoane date dispărute;
c) de către Inspecţia Muncii, în cazul accidentelor colective, generate de unele evenimente deosebite, precum avariile sau exploziile;
d) de către autorităţile de sănătate publică teritoriale, respectiv a municipiului Bucureşti, în cazul suspiciunilor de boală profesională şi a bolilor legate de profesiune.

Rezultatul cercetării evenimentului se va consemna într-un proces-verbal.

În caz de deces al persoanei accidentate ca urmare a unui eveniment, instituţia medico-legală competentă este obligată să înainteze inspectoratului teritorial de muncă, în termen de 7 zile de la data decesului, o copie a raportului de constatare medico-legală.

ACCIDENTE DE MUNCĂ

Prin accident de muncă se intelege vătămarea violentă a organismului, precum şi intoxicaţia acută profesională, care au loc în timpul procesului de muncă sau în îndeplinirea îndatoririlor de serviciu şi care provoacă incapacitate temporară de muncă de cel puţin 3 zile calendaristice, invaliditate ori deces.

Este, de asemenea, accident de muncă:

a) accidentul suferit de persoane aflate în vizită în întreprindere şi/sau unitate, cu permisiunea angajatorului;
b) accidentul suferit de persoanele care îndeplinesc sarcini de stat sau de interes public, inclusiv în cadrul unor activităţi culturale, sportive, în ţară sau în afara graniţelor ţării, în timpul şi din cauza îndeplinirii acestor sarcini;
c) accidentul survenit în cadrul activităţilor cultural-sportive organizate, în timpul şi din cauza îndeplinirii acestor activităţi;
d) accidentul suferit de orice persoană, ca urmare a unei acţiuni întreprinse din proprie iniţiativă pentru salvarea de vieţi omeneşti;
e) accidentul suferit de orice persoană, ca urmare a unei acţiuni întreprinse din proprie iniţiativă pentru prevenirea ori înlăturarea unui pericol care ameninţă avutul public şi privat;
f) accidentul cauzat de activităţi care nu au legătură cu procesul muncii, dacă se produce la sediul

persoanei juridice sau la adresa persoanei fizice, în calitate de angajator, ori în alt loc de muncă organizat de aceştia, în timpul programului de muncă, şi nu se datorează culpei exclusive a accidentatului;

g) accidentul de traseu, dacă deplasarea s-a făcut în timpul şi pe traseul normal de la domiciliul lucrătorului la locul de muncă organizat de angajator şi invers;
h) accidentul suferit în timpul deplasării de la sediul persoanei juridice sau de la adresa persoanei fizice la locul de muncă sau de la un loc de muncă la altul, pentru îndeplinirea unei sarcini de muncă;
i) accidentul suferit în timpul deplasării de la sediul persoanei juridice sau de la adresa persoanei fizice la care este încadrată victima, ori de la orice alt loc de muncă organizat de acestea, la o altă persoană juridică sau fizică, pentru îndeplinirea sarcinilor de muncă, pe durata normală de deplasare;
j) accidentul suferit înainte sau după încetarea lucrului, dacă victima prelua sau preda uneltele de lucru, locul de muncă, utilajul ori materialele, dacă schimba îmbrăcămintea personală, echipamentul individual de protecţie sau orice alt echipament pus la dispoziţie de angajator, dacă se afla în baie ori în spălător sau dacă se deplasa de la locul de muncă la ieşirea din întreprindere sau unitate şi invers;
k) accidentul suferit în timpul pauzelor regulamentare, dacă acesta a avut loc în locuri organizate de angajator, precum şi în timpul şi pe traseul normal spre şi de la aceste locuri;
l) accidentul suferit de lucrători ai angajatorilor români sau de persoane fizice române, delegaţi pentru îndeplinirea îndatoririlor de serviciu în afara graniţelor ţării, pe durata şi traseul prevăzute în documentul de deplasare;
m) accidentul suferit de personalul român care efectuează lucrări şi servicii pe teritoriul altor ţări, în baza unor contracte, convenţii sau în alte condiţii prevăzute de lege, încheiate de persoane juridice române cu parteneri străini, în timpul şi din cauza îndeplinirii îndatoririlor de serviciu;
n) accidentul suferit de cei care urmează cursuri de calificare, recalificare sau perfecţionare a pregătirii profesionale, în timpul şi din cauza efectuării activităţilor aferente stagiului de practică;
o) accidentul determinat de fenomene sau calamităţi naturale, cum ar fi furtună, viscol, cutremur, inundaţie, alunecări de teren, trăsnet (electrocutare), dacă victima se afla în timpul procesului de muncă sau în îndeplinirea îndatoririlor de serviciu;
p) dispariţia unei persoane, în condiţiile unui accident de muncă şi în împrejurări care îndreptăţesc presupunerea decesului acesteia;
q) accidentul suferit de o persoană aflată în îndeplinirea atribuţiilor de serviciu, ca urmare a unei agresiuni.

ATENTIE.

În situaţiile menţionate la lit. g), h), i) şi l), deplasarea trebuie să se facă fără abateri nejustificate de la traseul normal şi, de asemenea, transportul să se facă în condiţiile prevăzute de reglementările de securitate şi sănătate în muncă sau de circulaţie în vigoare.

Clasificarea accidentelor de munca

Accidentele de muncă se clasifică, în raport cu urmările produse şi cu numărul persoanelor accidentate, în:

a) accidente care produc incapacitate temporară de muncă de cel puţin 3 zile calendaristice;
b) accidente care produc invaliditate;
c) accidente mortale;
d) accidente colective, când sunt accidentate cel puţin 3 persoane în acelaşi timp şi din aceeaşi cauză.

Cercetarea accidentelor de munca

Cercetarea evenimentelor are ca scop stabilirea împrejurărilor şi a cauzelor care au condus la producerea acestora, a reglementărilor legale încălcate, a răspunderilor şi a măsurilor ce se impun a fi luate pentru prevenirea producerii altor cazuri similare şi, respectiv, pentru determinarea caracterului accidentului.

Cercetarea se face imediat după comunicare, în conformitate cu prevederile art. 29 alin. (1) din lege.

Cercetarea evenimentelor care produc incapacitate temporară de muncă se efectuează de către angajatorul la care s-a produs evenimentul.

Angajatorul are obligaţia să numească de îndată, prin decizie scrisă, comisia de cercetare a evenimentului.

Comisia de cercetare a evenimentului va fi compusă din cel puţin 3 persoane; una dintre acestea trebuie să fie lucrător desemnat, reprezentant al serviciului intern sau reprezentant al serviciului extern, cu pregătire de nivel superior.

Persoanele numite de către angajator în comisia de cercetare a evenimentului trebuie să aibă pregătire tehnică corespunzătoare şi să nu fie implicate în organizarea şi conducerea locului de muncă unde a avut loc evenimentul şi să nu fi avut o responsabilitate în producerea evenimentului.

Angajatorul care şi-a asumat atribuţiile în domeniul securităţii şi sănătăţii în muncă nu poate face parte din comisia de cercetare a evenimentului, în acest caz urmând să apeleze la servicii externe.

Dacă în eveniment sunt implicate victime cu angajatori diferiţi, în comisia de cercetare numită de angajatorul la care s-a produs evenimentul vor fi nominalizate şi persoane numite prin decizie scrisă de către ceilalţi angajatori.

Angajatorul care a organizat transportul răspunde pentru cercetarea accidentului de circulaţie produs pe drumurile publice, urmat de incapacitate temporară de muncă, cu respectarea, atunci când este cazul.

Cercetarea evenimentului,dacă acesta a avut loc în afara întreprinderii şi/sau unităţii angajatorului şi nu a avut nicio legătură cu aceasta, se efectuează în condiţiile legii.

Angajatorul care nu dispune de personal competent sau nu are personal suficient trebuie să asigure cercetarea apelând la servicii externe de prevenire şi protecţie.

Persoanele împuternicite, potrivit legii, să efectueze cercetarea evenimentelor au dreptul să ia declaraţii scrise, să preleveze sau să solicite prelevarea de probe necesare cercetării, să solicite sau să consulte orice acte ori documente ale angajatorului, iar acesta este obligat să le pună la dispoziţie în condiţiile legii.

Pentru cercetarea evenimentelor se pot solicita experţi sau specialişti cum ar fi cei din cadrul unor operatori economici cu competenţe potrivit legii să efectueze expertize tehnice, iar aceştia trebuie să răspundă solicitării.

Specialiştii şi experţii întocmesc expertize tehnice care vor face parte integrantă din dosarul de cercetare a evenimentului.

Cheltuielile aferente efectuării expertizelor se suportă de către angajatorul la care a avut loc evenimentul sau care se face răspunzător de organizarea activităţii în urma căreia s-a produs evenimentul.

Cercetarea evenimentului urmat de incapacitate temporară de muncă se va încheia în cel mult 5 zile lucrătoare de la data producerii.

Fac excepţie de la prevederile paragrafului anterior situaţii cum ar fi cele în care este necesară prelevarea de probe ori efectuarea de expertize, pentru care se poate solicita în scris, argumentat şi în termen, la inspectoratul teritorial de muncă pe raza căruia s-a produs evenimentul, prelungirea termenului de cercetare.

Cercetarea evenimentelor care au antrenat deces, invaliditate evidentă, accident colectiv sau situaţie de persoană dată dispărută, precum şi cercetarea incidentelor periculoase se vor încheia în cel mult 10 zile lucrătoare de la data producerii acestora.

Fac excepție de la prevederile paragrafului anterior situații cum ar fi cele în care este necesară eliberarea certificatului medico-legal, prelevarea de probe sau efectuarea de expertize, pentru care inspectoratul teritorial de muncă care cercetează evenimentele poate solicita în scris, argumentat și în termen, la Inspecția Muncii, prelungirea termenului de cercetare.

În cazul accidentului cu incapacitate termporară de muncă, în urma căruia a intervenit invaliditate confirmată prin decizie sau decesul victimei, inspectoratul teritorial de muncă va completa dosarul de cercetare întocmit la data producerii evenimentului și va întocmi un nou proces-verbal de cercetare bazat pe dosarul astfel completat.

Întocmirea noului proces-verbal de cercetare a accidentului, prevăzut la paragraful anterior se face în cel mult 5 zile lucrătoare de la data primirii de către inspectoratul teritorial de muncă a deciziei de încadrare într-un grad de invaliditate sau a certificatului de constatare medico-legal.

În cazul evenimentului a cărui consecință este invaliditate evidentă, evenimentul va fi cercetat de inspectoratul teritorial de muncă ca eveniment care a produs incapacitate temporară de muncă

D**osarul de cercetare** va cuprinde:

a) opisul actelor aflate în dosar;

b) procesul-verbal de cercetare;

c) nota de constatare la fața locului, încheiată imediat după producerea evenimentului de către inspectorul de muncă, în cazul evenimentelor care se cercetează de către inspectoratul teritorial de muncă/Inspecția Muncii, conform competențelor, sau de către lucrătorul desemnat/serviciile de prevenire și protecție, în cazul evenimentelor a căror cercetare intră în competența angajatorului, și semnată de către angajator/reprezentantul său legal, care va cuprinde precizări cum ar fi poziția victimei, existența sau inexistența echipamentului individual de protecție, starea echipamentelor de muncă, modul în care funcționau dispozitivele de protecție, închiderea fișei individuale de instructaj prin barare și semnătură, ridicarea de documente sau prelevarea de probe;

d) schițe și fotografii referitoare la eveniment;

e)declarațiile accidentaților, în cazul evenimentului urmat de incapacitate temporară de muncă sau de invaliditate;

f) declarațiile martorilor și ale oricăror persoane care pot contribui la elucidarea împrejurărilor și a cauzelor reale ale producerii evenimentului;

g) copii ale actelor și documentelor necesare pentru elucidarea împrejurărilor și a cauzelor reale ale evenimentului;

h) copii ale certificatului constatator sau oricăror alte autorizații în baza cărora angajatorul își desfășoară activitatea;

i) copii ale fișei de expunere la riscuri profesionale și ale fișei de aptitudine, întocmite conform legii;

j) copii ale contractelor individuale de muncă ale victimelor;

k)copii ale fișelor de instruire individuală în domeniul securității și sănătății în muncă ale victimelor; în caz de deces aceste fișe se vor anexa în original;

l) concluziile raportului de constatare medico-legală, în cazul accidentului mortal;

m) copie a hotărârii judecătorești prin care se declară decesul, în cazul persoanelor date dispărute;

n) copie a certificatelor de concediu medical, în cazul accidentului urmat de incapacitate temporară de muncă;

o) copie a deciziei de încadrare într-un grad de invaliditate, în cazul accidentului urmat de invaliditate;

p) actul emis de unitatea sanitară care a acordat asistența medicală de urgență, din care să rezulte data, ora când accidentatul s-a prezentat pentru consultație și diagnosticul, în cazul accidentelor de traseu;

q) copie a procesului-verbal de cercetare la fața locului, încheiat de serviciile poliției rutiere, în cazul accidentelor de circulație pe drumurile publice.

Dosarul va mai cuprinde, după caz, orice alte acte şi documente necesare pentru a determina caracterul accidentului, cum ar fi:

a) copie a autorizației, în cazul în care victima desfăşura o activitate care necesita autorizare;

b) copie a diplomei, adeverinței sau certificatului de calificare a victimei;

c) acte de expertiză tehnică, întocmite cu ocazia cercetării evenimentului;

d) acte doveditoare, emise de organe autorizate, din care să se poată stabili locul, data şi ora producerii evenimentului sau să se poată justifica prezența victimei la locul, ora şi data producerii evenimentului;

e) documente din care să rezulte că accidentatul îndeplinea îndatoriri de serviciu;

f) corespondența cu alte instituții/unități în vederea obținerii actelor solicitate;

g) adresele de prelungire a termenelor de cercetare, în conformitate cu art. 120 alin. (2) şi (4);

h) actul medical emis de unitatea sanitară care a acordat asistență medicală de urgență, din care să rezulte diagnosticul la internare şi/sau externare;

i) procesul-verbal încheiat după producerea evenimentului, în condițiile prevăzute la art. 111;

j) formularul pentru înregistrarea accidentului de muncă, denumit în continuare FIAM, aprobat prin ordin al ministrului muncii, solidarității sociale şi familiei.

Dosarul de cercetare a evenimentului trebuie să îndeplinească următoarele condiții:

a) filele dosarului să fie numerotate, semnate de inspectorul care a efectuat cercetarea sau de membrii comisiei de cercetare, numită de angajator, şi ştampilate cu ştampila inspectoratului sau a angajatorului;

b) numărul total de file conținut de dosarul de cercetare şi numărul de file pentru fiecare document anexat la dosar să fie menționate în opis;

c) fiecare document, cu excepția procesului-verbal de cercetare, să fie identificat în dosarul de cercetare ca anexă;

d) paginile şi spațiile albe să fie barate;

e) schițele referitoare la eveniment, anexate la dosar, să fie însoțite de explicații;

f) fotografiile referitoare la eveniment să fie clare şi însoțite de explicații;

g) formularul pentru declarație să fie conform modelului prevăzut în anexa nr. 14;

h) declarațiile aflate la dosar să fie tehnoredactate, pentru a se evita eventualele confuzii datorate scrisului ilizibil, certificate ca fiind conforme cu originalul şi semnate de către inspectorul care a efectuat cercetarea sau de către unul dintre membrii comisiei de cercetare.

Dosarul de cercetare a evenimentelor se va întocmi astfel:

a) într-un exemplar, pentru evenimentele care au produs incapacitate temporară de muncă; dosarul se păstrează în arhiva angajatorului care înregistrează accidentul;

b) într-un exemplar, pentru incidentele periculoase; dosarul se păstrează la inspectoratul teritorial de muncă care a efectuat cercetarea;

c) în două exemplare, pentru evenimentele care au produs invaliditate confirmată prin decizie, deces, accidente colective; originalul se înaintează organelor de urmărire penală şi un exemplar se păstrează la inspectoratul teritorial de muncă care a efectuat cercetarea;

d) în două exemplare, pentru evenimentele care au antrenat invaliditate evidentă; originalul se păstrează la inspectoratul teritorial de muncă care a efectuat cercetarea şi un exemplar se transmite angajatorului care înregistrează accidentul;

e) în trei exemplare, pentru evenimentele cercetate de Inspecția Muncii; originalul se înaintează organelor de urmărire penală, un exemplar se păstrează la Inspecția Muncii şi un exemplar la inspectoratul teritorial de muncă pe raza căruia s-a produs evenimentul;

f) în mai multe exemplare, pentru evenimentele care au produs incapacitatea temporară de muncă pentru victime cu angajatori diferiți; originalul se păstrează în arhiva angajatorului care înregistrează accidentul şi celelalte exemplare se păstrează de către ceilalți angajatori.

În cazul evenimentelor care au generat accidente urmate de incapacitate temporară de muncă sau al incidentelor periculoase în care faptele comise pot fi considerate infracțiuni, potrivit legii, dosarul de cercetare se încheie în două exemplare, originalul fiind înaintat organului de urmărire penală.

Dosarul de cercetare, întocmit de comisia numită de către angajator, se înaintează pentru verificare şi avizare la inspectoratul teritorial de muncă pe raza căruia s-a produs evenimentul, în termen de 5 zile lucrătoare de la finalizarea cercetării.

Inspectoratul teritorial de muncă va analiza dosarul, va aviza şi va restitui dosarul în cel mult 7 zile lucrătoare de la data primirii.

Dosarul va fi însoţit de avizul inspectoratului teritorial de muncă.

În cazul în care inspectoratul teritorial de muncă constată că cercetarea nu a fost efectuată corespunzător, poate dispune completarea dosarului şi/sau refacerea procesului-verbal de cercetare, după caz.

Comisia de cercetare va completa dosarul şi va întocmi procesul-verbal de cercetare în termen de 5 zile lucrătoare de la data primirii dosarului.

Dosarul de cercetare întocmit de inspectoratul teritorial de muncă va fi înaintat în vederea avizării la Inspecția Muncii, în cel mult 5 zile lucrătoare de la finalizarea cercetării.

Dosarul de cercetare pentru cazul dispariţiei de persoane, ca urmare a unui eveniment şi în împrejurări care îndreptățesc presupunerea decesului acestora, va fi păstrat la inspectoratul teritorial de muncă care a efectuat cercetarea, până la emiterea hotărârii judecătoreşti prin care se declară decesul persoanelor dispărute, conform prevederilor legale în vigoare; după completarea dosarului, acesta va fi înaintat în vederea avizării la Inspecția Muncii.

Inspecția Muncii avizează şi restituie dosarele în cel mult 10 zile lucrătoare de la data primirii.

În cazul în care Inspecția Muncii constată că cercetarea nu a fost efectuată corespunzător, poate dispune completarea dosarului şi întocmirea unui nou proces-verbal de cercetare.

Inspectoratul teritorial de muncă va completa dosarul şi va întocmi noul proces-verbal de cercetare în termen de 5 zile lucrătoare de la data primirii dosarului.

Inspectoratul teritorial de muncă transmite dosarele de cercetare organelor de urmărire penală,dupa caz, numai după ce au fost avizate de către Inspecția Muncii.

Dosarul de cercetare al accidentului de muncă cu invaliditate, înaintat organelor de urmărire penală, se restituie la inspectoratul teritorial de muncă care a efectuat cercetarea, pentru completare şi întocmirea unui nou proces-verbal de cercetare, în cazul în care se produce decesul accidentatului ca urmare a accidentului suferit, confirmat în baza unui act medico-legal.

Dosarul mentionat la paragraful anterior se restituie la inspectoratul teritorial de muncă în termen de 10 zile lucrătoare de la data solicitării acestuia.

Completarea dosarului mentionat la paragraful anterior şi întocmirea noului proces-verbal de cercetare a evenimentului se fac în cel mult 5 zile lucrătoare de la primirea dosarului la inspectoratul teritorial de muncă.

Dosarul completat şi noul proces-verbal de cercetare vor fi înaintate în vederea avizării la Inspecția Muncii, care le va restitui inspectoratului teritorial de muncă în termen de 10 zile lucrătoare de la data primirii.

După avizarea de către Inspecția Muncii, dosarul va fi înaintat organelor de urmărire penală de către inspectoratul teritorial de muncă.

Procesul-verbal de cercetare a evenimentului trebuie să conțină următoarele capitole:

a) data încheierii procesului-verbal;
b) numele persoanelor şi în ce calitate efectuează cercetarea evenimentului;
c) perioada de timp şi locul în care s-a efectuat cercetarea;
d) obiectul cercetării;
e) data şi ora producerii evenimentului;
f) locul producerii evenimentului;
g) datele de identificare a angajatorului la care s-a produs evenimentul, numele reprezentantului său legal;
h) datele de identificare a accidentatului/accidentaților;
i) descrierea detaliată a locului, echipamentului de muncă, a împrejurărilor şi modului în care s-a produs evenimentul;
j) urmările evenimentului şi/sau urmările suferite de persoanele accidentate;
k) cauza producerii evenimentului;
l) alte cauze care au concurat la producerea evenimentului;
m) alte constatări făcute cu ocazia cercetării evenimentului;
n) persoanele răspunzătoare de încălcarea reglementărilor legale, din capitolele de la lit. k), l) şi m);
o) sancțiunile contravenționale aplicate;
p) propuneri pentru cercetare penală;
q) caracterul accidentului;
r) angajatorul care înregistrează accidentul de muncă sau incidentul periculos;
s) măsuri dispuse pentru prevenirea altor evenimente similare şi persoanele responsabile pentru realizarea acestora;
t) termenul de raportare la inspectoratul teritorial de muncă privind realizarea măsurilor prevăzute la lit. s);
u) numărul de exemplare în care s-a încheiat procesul-verbal de cercetare şi repartizarea acestora;
v) numele şi semnătura persoanei/persoanelor care a/au efectuat cercetarea;
w) avizul inspectorului-şef adjunct securitate şi sănătate în muncă;
x) viza inspectorului-şef/inspectorului general de stat.

- În capitolul prevăzut la lit. b) se vor indica, de asemenea, prevederile legale potrivit cărora persoanele sunt îndreptățite să efectueze cercetarea, precum şi numele angajatorului şi ale persoanelor care au participat din partea organelor competente la primele cercetări.
- În capitolul prevăzut la lit. c) se vor indica, de asemenea, motivele pentru care s-a solicitat prelungirea termenului de cercetare.
- În capitolul prevăzut la lit. e) se va indica, de asemenea, data decesului, pentru cazul în care s-a produs un eveniment şi ulterior a survenit decesul victimelor implicate în acest eveniment.
- În capitolul prevăzut la lit. g) se vor indica, de asemenea, datele de identificare ale angajatorilor la care sunt/au fost angajate victimele, numele reprezentanților legali ai angajatorilor, numărul documentului prin care s-a certificat autorizarea de funcționare din punct de vedere al securității şi sănătății în muncă, adresa punctului de lucru.
- În capitolul prevăzut la lit. h) se vor indica, de asemenea, următoarele: numele, prenumele, cetățenia, vârsta, starea civilă, numărul de copii minori, domiciliul, locul de muncă la care este încadrat, profesia de bază, ocupația în momentul accidentării, vechimea în muncă, în funcție sau în meserie şi la locul de muncă, data efectuării ultimului instructaj în domeniul securității şi sănătății în muncă, iar pentru persoanele care, în momentul accidentării, desfăşurau o activitate pentru care este necesară autorizare, se va face referire şi la aceasta.
- Capitolul prevăzut la lit. i) va conține următoarele subcapitole:
  - **a)** descrierea detaliată a locului producerii evenimentului;
  - **b)** descrierea detaliată a echipamentului de muncă;
  - **c)** descrierea detaliată a împrejurărilor;
  - **d)** descrierea detaliată a modului în care s-a produs evenimentul.

- În capitolele prevăzute la lit. k)-m) se va face trimitere la reglementările legale în vigoare încălcate, cu redarea integrală a textului acestora.
- Denumirea capitolului prevăzut la lit. o) se va schimba în "Propuneri pentru sancțiuni administrative şi disciplinare", în cazul accidentelor cercetate de către comisia numită de angajator.
- Capitolele prevăzute la lit. w) şi x) se vor regăsi în procesul-verbal de cercetare numai pentru evenimentele cercetate de către inspectoratul teritorial de muncă sau Inspecția Muncii, conform competențelor.
- În cazul accidentelor cu ITM, procesul-verbal de cercetare se va încheia cu capitolul prevăzut la lit. w), care va fi numit "Viza angajatorului".

ATENTIE

În situațiile în care din cercetare rezultă că accidentul nu întruneşte condițiile pentru a fi încadrat ca accident de muncă, se va face această menţiune la capitolele procesului-verbal de cercetare prevăzute la lit. q) şi r) şi se vor dispune măsurile care trebuie luate de angajator pentru prevenirea unor cazuri asemănătoare.

Comisia de cercetare a unui eveniment numită de angajator poate face propuneri de sancțiuni disciplinare şi/sau administrative, pe care le va menționa în procesul-verbal de cercetare.

Procesul-verbal de cercetare a unui eveniment se întocmeşte în:

a) 3 exemplare, în cazul accidentului de muncă urmat de incapacitate temporară de muncă, pentru angajatorul care înregistrează accidentul, inspectoratul teritorial de muncă care a avizat dosarul şi asigurător;

b) mai multe exemplare, în cazul accidentului de muncă urmat de incapacitate temporară de muncă pentru lucrători cu angajatori diferiți, pentru fiecare angajator, inspectoratul teritorial de muncă care a avizat dosarul şi asigurător;

c) 5 exemplare, în cazul accidentului de muncă urmat de invaliditate, pentru angajatorul care înregistrează accidentul, organul de urmărire penală, inspectoratul teritorial de muncă care a efectuat cercetarea, Inspecția Muncii şi asigurător;

d) 5 exemplare, în cazul accidentului de muncă mortal sau al celui colectiv, precum şi în cazul accidentului mortal în afara muncii, pentru angajatorul care înregistrează accidentul, organul de urmărire penală, inspectoratul teritorial de muncă care a efectuat cercetarea, Inspecția Muncii şi asigurător;

e) exemplare, în cazul incidentului periculos, pentru angajatorul care înregistrează incidentul, organele de urmărire penală, inspectoratul teritorial de muncă care a efectuat cercetarea, Inspecția Muncii şi asigurător.

ATENTIONARI

(1) În cazul în care accidentul de muncă s-a produs la un angajator, altul decât cel care îl înregistrează, un exemplar din procesul-verbal de cercetare va fi trimis şi acestuia.

(2) În cazul în care angajatorul la care se înregistrează accidentul de muncă îşi are sediul, domiciliul sau reşedința pe teritoriul altui județ decât cel pe raza căruia s-a produs accidentul, se va trimite un exemplar din procesul-verbal de cercetare inspectoratului teritorial de muncă pe raza căruia are sediul, domiciliul sau reşedința angajatorul.

(3) În cazul evenimentelor care nu au fost comunicate şi cercetate, dar persoana vătămată prezintă un certificat medical cu cod "accident de muncă", angajatorul care şi-a asumat atribuțiile în domeniul securității şi sănătății în muncă/lucrătorul desemnat/serviciul intern de prevenire şi protecție/serviciul extern de prevenire şi protecție va solicita acesteia o declarație scrisă privind modul şi împrejurările în care s-a produs evenimentul.

Înregistrarea şi evidenţa accidentelor de muncă şi a incidentelor periculoase

a) Inregistrarea

Înregistrarea accidentelor de muncă şi a incidentelor periculoase se face în baza procesului-verbal de cercetare.

Accidentul de muncă produs în timpul prestării unor servicii pe bază de contract, comandă sau alte forme legale încheiate în întreprinderea şi/sau unitatea unui angajator, alta decât cea la care este încadrată victima, se înregistrează potrivit clauzelor prevăzute în acest sens în documentele încheiate.

În situaţia în care documentul încheiat nu prevede clauze în acest sens, clauzele nu sunt suficient de acoperitoare pentru toate situaţiile sau clauzele sunt contrare prevederilor prezentelor norme metodologice, accidentul de muncă se înregistrează de către angajatorul răspunzător de conducerea şi/sau de organizarea activităţii care a avut ca urmare producerea accidentului.

Accidentul de muncă produs în timpul prestării unor servicii pe bază de comandă, la domiciliul clientului, se înregistrează de către angajatorul la care este/a fost angajată victima.

Accidentul de muncă suferit de o persoană aflată în îndeplinirea îndatoririlor de serviciu în întreprinderea şi/sau unitatea altui angajator se înregistrează de către angajatorul răspunzător de conducerea şi/sau de organizarea activităţii care a avut ca urmare producerea accidentului.

Accidentele suferite în timpul stagiului de practică profesională de către elevi, studenţi, ucenici şi şomeri în perioada de reconversie profesională se înregistrează de către angajatorul la care se efectuează practica/reconversia profesională.

Accidentul de muncă suferit de o persoană în cadrul activităţilor cultural-sportive, în timpul şi din cauza îndeplinirii acestor activităţi, se înregistrează de către instituţia sau angajatorul care a organizat acţiunea respectivă.

Accidentul de muncă produs ca urmare a unei acţiuni întreprinse de o persoană, din proprie iniţiativă, pentru salvarea de vieţi omeneşti sau pentru prevenirea ori înlăturarea unui pericol grav şi iminent ce ameninţă avutul public sau privat din întreprinderea şi/sau unitatea unui angajator, se înregistrează de către angajatorul la care s-a produs accidentul.

În cazul accidentului produs ca urmare a unei acţiuni întreprinse de o persoană, din proprie iniţiativă, pentru salvarea de vieţi omeneşti sau pentru prevenirea ori înlăturarea unui pericol grav şi iminent ce ameninţă avutul public sau privat, produs în afara întreprinderii şi/sau unităţii unui angajator şi care nu are nicio legătură cu acesta, înregistrarea se face conform legii.

Accidentul de muncă de traseu se înregistrează de către angajatorul la care este angajată victima sau, după caz, de angajatorul răspunzător de conducerea şi/sau de organizarea activităţii care a avut ca urmare producerea accidentului, conform concluziilor cercetării.

Accidentul de muncă de circulaţie se înregistrează de către angajatorul la care este angajată victima sau, după caz, de angajatorul răspunzător de conducerea şi/sau de organizarea activităţii care a avut ca urmare producerea accidentului, conform concluziilor cercetării.

Accidentul produs în afara întreprinderii şi/sau unităţii, ca urmare a neluării unor măsuri de securitate de către un alt angajator, se înregistrează de către angajatorul din vina căruia s-a produs accidentul.

Accidentul de muncă suferit de însoţitorii de încărcături, personalul de poştă de la vagoanele C.F.R., angajaţi ai unor angajatori care, potrivit legii, sunt obligaţi să delege însoţitori pentru astfel de încărcături, pe mijloace de transport ce nu le aparţin, se va înregistra de către angajatorul răspunzător de organizarea activităţii care a avut ca urmare producerea accidentului sau, după caz, în condiţiile clauzelor prevăzute în documentele încheiate.

Observatie.

Pentru unele situaţii neprevăzute în prezentele reglementări, cu privire la înregistrarea accidentelor de muncă, inspectoratul teritorial de muncă sau Inspecţia Muncii va stabili modul de înregistrare a accidentului în cauză.

Dispariția unei persoane în condițiile unui accident de muncă şi în împrejurări care îndreptățesc presupunerea decesului acesteia se înregistrează ca accident mortal, după rămânerea definitivă şi irevocabilă a hotărârii judecătoreşti, conform prevederilor legale, prin care este declarat decesul.

Data producerii accidentului de muncă mortal, prevăzut la alin. precedent, este data înscrisă în hotărârea judecătorească ca fiind data decesului.

Angajatorul la care a fost angajată persoana dispărută va comunica, imediat, numărul şi data hotărârii judecătoreşti la inspectoratul teritorial de muncă.

Accidentul de muncă cu invaliditate se va înregistra pe baza procesului-verbal de cercetare întocmit de inspectoratul teritorial de muncă.

În baza procesului-verbal de cercetare întocmit de persoanele împuternicite prin lege, angajatorul la care se înregistrează accidentul va completa FIAM.

FIAM se completează pentru fiecare persoană accidentată în câte 4 exemplare care se înaintează spre avizare după cum urmează:

a) inspectoratului teritorial de muncă care a avizat dosarul de cercetare întocmit de comisia angajatorului, în termen de 3 zile lucrătoare de la primirea avizului;

b) inspectoratului teritorial de muncă care a efectuat cercetarea, în termen de 3 zile lucrătoare de la primirea procesului-verbal de cercetare.

Verificarea şi avizarea FIAM de către inspectoratul teritorial de muncă se fac în termen de 5 zile lucrătoare de la primirea formularului.

Angajatorul la care se înregistrează accidentul anexează FIAM la dosarul sau la procesul-verbal de cercetare şi distribuie celelalte exemplare la persoana accidentată, inspectoratul teritorial de muncă şi asigurătorul pe raza căruia îşi are sediul social, domiciliul sau reşedința.

În cazul în care victima unui accident de muncă a fost propusă pentru pensionare odată cu emiterea deciziei de încadrare într-o grupă de invaliditate, se va completa un exemplar FIAM care se va anexa la dosarul de pensionare ce va fi înaintat unității de expertiză medicală şi recuperare a capacității de muncă.

b)Evidenta

Angajatorul va ține evidența evenimentelor în:

a) Registrul unic de evidență a accidentaților în muncă, conform modelului prevăzut în anexa nr. 15 la Normele Metodologice;

b) Registrul unic de evidență a incidentelor periculoase, conform modelului prevăzut în anexa nr. 16 la Normele Metodologice;

c) Registrul unic de evidență a accidentelor uşoare, conform modelului prevăzut în anexa nr. 17 la Normele Metodologice;

d) Registrul unic de evidență a accidentaților în muncă ce au ca urmare incapacitate de muncă mai mare de 3 zile de lucru, conform modelului prevăzut în anexa nr. 18 la Normele Metodologice.

În registrul prevăzut la lit. d) se va ține evidența accidentaților în muncă pentru care perioada de incapacitate temporară de muncă este de minimum 4 zile de lucru, fără a lua în calcul ziua producerii accidentului.

Registrele de evidență trebuie să fie actualizate.

În baza FIAM şi a proceselor-verbale de cercetare a incidentelor periculoase, inspectoratul teritorial de muncă va ține evidența tuturor accidentelor de muncă şi a incidentelor periculoase înregistrate de angajatorii care au sediul, domiciliul sau reşedința pe teritoriul județului respectiv.

Inspectoratul teritorial de muncă va ține evidența în:

a) Registrul unic de evidență a accidentaților în muncă;

b) Registrul unic de evidență a incidentelor periculoase;

c) Registrul unic de evidență a accidentaților în muncă ce au ca urmare incapacitate de muncă mai mare de 3 zile de lucru.

RASPUNDEREA JURIDICA

Infracţiuni

Sunt prevazute de Legea 319/2006, la art.37 si art.38.

7.1.1. (1) Neluarea vreuneia dintre măsurile legale de securitate şi sănătate în muncă de către persoana care avea îndatorirea de a lua aceste măsuri, dacă se creează un pericol grav şi iminent de producere a unui accident de muncă sau de îmbolnăvire profesională, constituie infracţiune şi se pedepseşte cu închisoare de la un an la 2 ani sau cu amendă.

(2) Dacă fapta prevăzută la alin. (1) a produs consecinţe deosebite, pedeapsa este închisoarea de la un an la 3 ani sau amendă.

(3) Fapta prevăzută la alin. (1) săvârşită din culpă se pedepseşte cu închisoare de la 3 luni la un an sau cu amendă, iar fapta prevăzută la alin. (2) săvârşită din culpă se pedepseşte cu închisoare de la 6 luni la un an sau cu amendă.

7.1.2.(1) Nerespectarea de către orice persoană a obligaţiilor şi a măsurilor stabilite cu privire la securitatea şi sănătatea în muncă, dacă prin aceasta se creează un pericol grav şi iminent de producere a unui accident de muncă sau de îmbolnăvire profesională, constituie infracţiune şi se pedepseşte cu închisoare de la un an la 2 ani sau cu amendă.

(2) Dacă fapta prevăzută în alin. (1) a produs consecinţe deosebite, pedeapsa este închisoarea de la un an la 3 ani sau amendă.

(3) Dacă nerespectarea constă în repunerea în funcţiune a instalaţiilor, maşinilor şi utilajelor, anterior eliminării tuturor deficienţelor pentru care s-a luat măsura opririi lor, pedeapsa este închisoarea de la un an la 2 ani sau amendă.

(4) Faptele prevăzute la alin. (1) şi (3) săvârşite din culpă se pedepsesc cu închisoare de la 3 luni la un an sau cu amendă, iar fapta prevăzută la alin. (2) săvârşită din culpă se pedepseşte cu închisoare de la 6 luni la un an sau cu amendă.

Contravenţii

Sunt prevazute de Legea 319/2006, la art.39.

(1) Constituie contravenţii faptele săvârşite de angajatorii aflaţi în una dintre situaţiile prevăzute de prezenta lege.

(2) Constituie contravenţie şi se sancţionează cu amendă de la 5.000 lei la 10.000 lei încălcarea dispoziţiilor art. 13 lit. b), c), p) şi r), din Legea 319/2006.

(3) Constituie contravenţie şi se sancţionează cu amendă de la 3.000 lei la 10.000 lei încălcarea dispoziţiilor art. 13 lit. n) din Legea 319/2006.

(4) Constituie contravenţie şi se sancţionează cu amendă de la 4.000 lei la 8.000 lei încălcarea dispoziţiilor art. 12 alin. (1) lit. a) şi b), art. 13 lit. a), d) - f), h) - m) şi o), art. 20, art. 29 alin. (1) lit. a) şi ale art. 32 alin. (2) din Legea 319/2006.

(5) Constituie contravenţie şi se sancţionează cu amendă de la 3.500 lei la 7.000 lei încălcarea dispoziţiilor art. 7 alin. (4) - (6), art. 8, art. 11 alin. (1) şi (3), art. 13 lit. q) şi s) şi ale art. 27 alin. (1) lit. a) şi b) din Legea 319/2006.

(6) Constituie contravenţii şi se sancţionează cu amendă de la 3.000 lei la 6.000 lei următoarele fapte:

a) încălcarea dispoziţiilor art. 9 alin. (1), ale art. 10 şi 16 din Legea 319/2006;

b) încălcarea dispoziţiilor art. 14, 15 şi ale art. 34 alin. (1) din Legea 319/2006.

(7) Constituie contravenţie şi se sancţionează cu amendă de la 2.500 lei la 5.000 lei încălcarea dispoziţiilor art. 11 alin. (2) şi (4), ale art. 17, 19 şi 21 din Legea 319/2006.

(8) Constituie contravenţii şi se sancţionează cu amendă de la 2.000 lei la 4.000 lei următoarele fapte:

a) încălcarea dispoziţiilor art. 12 alin. (1) lit. c) şi d), art. 13 lit. g), art. 18 alin. (5) şi (6) şi ale art. 36 din Legea 319/2006;
b) încălcarea dispoziţiilor art. 34 alin. (5) din Legea 319/2006.

(9) Constituie contravenţie şi se sancţionează cu amendă de la 5.000 lei la 10.000 lei nerespectarea reglementărilor de securitate şi sănătate în muncă privind:

a) fabricarea, transportul, depozitarea, manipularea sau utilizarea substanţelor ori preparatelor chimice periculoase şi a deşeurilor rezultate;
b) prevenirea prezenţei peste limitele maxime admise a agenţilor chimici, fizici sau biologici, precum şi suprasolicitarea diferitelor organe sau sisteme ale organismului uman;
c) darea în exploatare sau repunerea în funcţiune, parţială ori totală, a construcţiilor, echipamentelor de muncă noi sau reparate, precum şi pentru aplicarea proceselor tehnologice;
d) întocmirea şi respectarea documentaţiilor tehnice pentru executarea lucrărilor care necesită măsuri speciale de siguranţă;
e) folosirea surselor de foc deschis şi fumatul la locurile de muncă unde acestea sunt interzise;
f) prevenirea accidentelor prin electrocutare la executarea, exploatarea, întreţinerea şi repararea instalaţiilor şi a echipamentelor electrice, precum şi pentru prevenirea efectelor electricităţii statice şi ale descărcărilor atmosferice;
g) asigurarea şi folosirea instalaţiilor electrice de construcţie adecvate la locurile de muncă unde există pericole de incendiu sau de explozie;
h) asigurarea celei de-a doua surse de alimentare cu energie electrică a echipamentelor de muncă;
i) transportul, manipularea şi depozitarea echipamentelor de muncă, materialelor şi produselor;
j) delimitarea, îngrădirea şi semnalizarea zonelor periculoase;
k) semnalizarea de securitate şi/sau de sănătate la locul de muncă;
l) asigurarea exploatării fără pericole a recipientelor-butelii cu gaze comprimate sau lichefiate, a instalaţiilor mecanice sub presiune şi a celor de ridicat, a conductelor prin care circulă fluide sub presiune şi a altor asemenea echipamente de muncă;
m) utilizarea, întreţinerea, revizia şi repararea periodică a echipamentelor de muncă;
n) asigurarea, marcarea şi întreţinerea căilor de acces şi de circulaţie;
o) asigurarea iluminatului de siguranţă;
p) organizarea activităţii de păstrare, întreţinere şi denocivizare a echipamentului individual de protecţie;
q) întocmirea documentelor de urmărire a parametrilor funcţionali ai echipamentelor de muncă şi a rapoartelor de serviciu pentru instalaţiile cu regim special de exploatare;
r) aplicarea metodelor de exploatare minieră, execuţia, exploatarea şi întreţinerea lucrărilor miniere, realizarea şi funcţionarea sistemului de aeraj, corespunzător clasificării minelor din punctul de vedere al emanaţiilor de gaze;
s) amenajarea locurilor de muncă pentru lucrul la înălţime, în spaţii închise şi în condiţii de izolare.

Constituie contravenţie şi se sancţionează cu amendă de la 5.000 lei la 10.000 lei neprezentarea de către serviciile externe a raportului semestrial de activitate.

Sancţiunile contravenţionale prevăzute la art. 39 alin. (2) - (9) şi la art. 40 din Legea 319/2006se aplică angajatorilor.

Constatarea contravenţiilor

(1) Constatarea contravenţiilor şi aplicarea amenzilor prevăzute la art. 39 alin. (2) - (9) şi la art. 40 din Legea 319/2006 se fac de către inspectorii de muncă.

(2) Constatarea contravenţiilor şi aplicarea amenzilor prevăzute la art. 39 alin. (6) lit. b) alin. (8) lit. b) din Legea 319/2006 se fac şi de către inspectorii sanitari din cadrul Ministerului Sănătăţii Publice şi al unităţilor subordonate.

(3) În caz de constatare a unei situaţii care se încadrează în prevederile art. 37 şi 38 din Legea 319/2006, inspectorii prevăzuţi la alin. (1) şi (2) vor sesiza de îndată organele de urmărire penală competente, potrivit legii.

Observatii.

1. Prevederile art. 39 alin. (2) - (9) şi ale art. 40din Legea 319/2006, se completează cu dispoziţiile Ordonanţei Guvernului nr. 2/2001 privind regimul juridic al contravenţiilor, aprobată cu dificări şi completări prin Legea nr. 180/2002, cu modificările şi completările ulterioare.
2. Contravenientul poate achita pe loc sau în termen de cel mult 48 de ore de la data încheierii procesului-verbal ori, după caz, de la data comunicării acestuia jumătate din minimul amenzii prevăzute de lege, corespunzător faptei pentru care a fost sancţionat, inspectorul de muncă făcând menţiune despre această posibilitate în procesul-verbal.
3. Angajatorii răspund patrimonial, potrivit legii civile, pentru prejudiciile cauzate victimelor accidentelor de muncă sau bolilor profesionale, în măsura în care daunele nu sunt acoperite integral prin prestaţiile asigurărilor sociale de stat.

Întocmit

Jr. Constantin BUJOR

REGLEMENTAREA DOMENIULUI SISTEMELOR DE ALARMARE ÎMPOTRIVA EFRACȚIEI ÎN LEGEA NR.333/2003

BIBLIOGRAFIE:

- Legea nr.333/2003 privind paza obiectivelor, bunurilor, valorilor şi protecția persoanelor;
- Norme metodologice de aplicare a prevederilor proiectului legii.
- Standardele S.R.C.E.I. seria 839
- Normele tehnice privind proiectarea, instalarea, întreținerea şi utilizarea sistemelor de alarmă împotriva efracției.

În cadrul legii privind paza obiectivelor, bunurilor, valorilor şi protecția persoanei se reglementează domeniul sistemelor de alarmare împotriva efracției.

Astfel, la CAPITOLUL IV – "Sisteme tehnice de protecție şi de alarmare împotriva efracției", prin cele trei secțiuni, respectiv 9 articole se reglementează domeniul sistemelor de alarmare, licențierea societăților specializate în instalarea sistemelor şi dispeceratele de monitorizare.

Secțiunea I	–	Mijloace de protecție şi alarmare împotriva efracției
Secțiunea a - II a	-	Licențierea societăților specializate în sisteme de alarmare împotriva efracției
Secțiunea a - III – a	-	Dispeceratele de monitorizare a sistemelor de alarmare

În Secțiunea I, la art. 28 alin. (1), este stipulată obligația conducătorilor de unități care dețin bunuri, valori şi suporturi de stocare a documentelor de a-şi asigura paza, mijloacele de protecție mecano-fizice şi sistemele de alarmare împotriva efracției.

În alin. (2), este stabilită competența de avizare a proiectelor de instalare a sistemelor de protecție şi alarmare împotriva efracției, potrivit actelor normative ce privesc protecția informațiilor clasificate.

Alin. (3) precizează condițiile pe care trebuie să le îndeplinească elementele de protecție mecano-fizice, respectiv să fie certificate că rezistă la efracție, corespunzător gradului de siguranță impus de caracteristicile obiectivului păzit.

La alin. (4) sunt definite elementele de protecție mecano-fizică şi anume: ziduri, plase, blindaje, case de fier, seifuri, dulapuri metalice, tezaur, geamuri şi folie de protecție, grilaje, uşi şi încuietori.

În alin. (5) se defineşte sistemul de alarmare împotriva efracției.

"Prin sistem de alarmă împotriva efracției se înțelege ansamblul de echipamente electronice compus din centrală de comandă şi semnalizare optică şi acustică, detectoare de prezență, antişoc şi acustice, butoane şi pedale de panică, control acces şi televiziune cu circuit închis, cu posibilități de înregistrare şi stocare a imaginilor şi datelor de natură să asigure o protecție corespunzătoare obiectivelor şi persoanelor"

Alin. (6) stabileşte condițiile de instalare a sistemelor de alarmare după avizarea proiectelor şi controlul poliției în executarea instalațiilor şi punerea în funcțiune.

Ultimul alineat, respectiv alin. (7) precizează că "proiectele sistemelor de alarmă împotriva efracției se întocmesc în conformitate cu normele tehnice stabilite prin hotărâre de guvern".

În art. 29, este stabilită obligația firmei prestatoare şi a beneficiarului în folosirea de mijloace de protecție mecano-fizice şi sisteme de alarmare certificate.

Certificarea calității mijloacelor de protecție mecano-fizice se face de către un laborator de încercări din țară, autorizat şi acreditat.

La art. 30, se stabileşte obligația de prevedere a mijloacelor de protecție mecano-fizice şi sistemelor de alarmare împotriva efracției în faza de proiect de execuție a clădirilor.

Art. 31 stabileşte condițiile de comercializare a mijloacelor de protecție mecano-fizice şi de alarmare împotriva efracției după încadrarea într-o clasă de siguranță (rezistență), în conformitate cu normele europene.

În art. 32 este stabilită obligația beneficiarilor, a personalului firmelor prestatoare în păstrarea confidențialității informației referitoare la sistemele instalate sau aflate în întreținere.

În ultimul articol din secțiune, respectiv art. 33, sunt precizate condițiile de clasificare a sistemelor de alarmare în raport cu importanța bunurilor şi a valorilor ce urmează a fi apărate şi categoria de importanță a construcției, competența de clasificare fiind acordată societăților de asigurări.

Secțiunea a – II –a - Licențierea societăților specializate în sisteme de alarmare împotriva efracției

În art. 34 alin. (1) se reglementează condițiile de a desfăşura activități de proiectare, instalare şi întreținere a sistemelor de alarmare împotriva efracției numai în baza licenței Inspectoratului General al Poliției Române şi avizului prealabil al Serviciului Român de Informații.

În alin. (2), se stabileşte obligația conducerii firmelor licențiate de a face cunoscute organului de poliție modificările survenite în structura şi organizarea activității.

În alin. (3), se stabileşte necesitatea avizării conducătorilor şi personalului tehnic din cadrul societăților licențiate.

Prin art. 35 alin. (1), este stabilită interdicția de culegere a informațiilor, înregistrărilor audio sau video care exced obiectului de activitate pentru care li s-a acordat licență, precum şi instalarea de echipamente care să le permită executarea acestor activități.

În alin. (2) este stabilită obligația conducerii societăților specializate în sisteme de alarmare în asigurarea respectării prevederilor legale şi a regulamentelor proprii de organizare şi funcționare aprobate cu ocazia licențierii.

La alin. (3), se reglementează asocierea societăților specializate cu firme străine de profil.

Secțiunea a – III - a - Dispeceratele de monitorizare a sistemelor de alarmare

Art. 36 stabileşte cine poate organiza dispecerate de zonă.

Astfel, unitățile de jandarmi, corpul gardienilor publici, societățile specializate de pază şi cele din domeniul sistemelor tehnice de alarmă pot înființa dispecerate de monitorizare.

Alin. (2) "Înființarea dispeceratelor de zonă se face numai după avizarea regulamentului de organizare şi funcționare de către Inspectoratul General al Poliției Române. Fac excepție unitățile de jandarmi, pentru dispeceratele proprii".

La alin. (3), se stabileşte obligația existenței contractelor încheiate cu beneficiarii conectați la dispecerat.

Alin. (4) stabileşte persoanele care pot efectua intervenții la obiectivele alarmate, fiind competent numai personalul calificat din jandarmerie, corpurile gardienilor publici şi societățile specializate de pază.

La alin. (5) se reglementează procedura de intervenție şi măsurile ce se impun, în funcție de situație.

În ultimul alineat – (6), este stipulată obligativitatea menționării în planul de pază a faptului că obiectivul respectiv este conectat la un dispecerat de monitorizare.

Prin standardele CEI seria 839 sunt definiți termenii, facilități ale echipamentelor componente ale sistemelor de alarmare.

Răspunderi şi sancțiuni:

Potrivit art. 57: "Nerespectarea dispozițiilor prezentei legi atrage, după caz, răspunderea civilă, materială, disciplinară, contravențională sau penală.

Astfel, art. 58: "Desfăşurarea de activități de pază sau protecție, de proiectare, producere, instalare şi întreținere a sistemelor de alarmă împotriva efracției sau a componentelor acestora fără atestat sau fără licența de funcționare prevăzută de lege constituie infracțiune şi **se pedepseşte cu închisoare de la 6 luni la 3 ani."**

Sancțiuni contravenționale:

Art.60 lit.g: "nerespectarea prevederilor art. 24, art. 34 alin. (2), art. 41 alin. (7) şi (9) şi ale art. 42 se sancționează cu amendă de la **5-10 milioane lei;**
Art.34 alin (2) "Persoanele fizice sau juridice prevăzute la alin. (1) sunt obligate ca, în termen de 15 zile, să comunice în scris unității de poliție competente orice modificare intervenită în structura şi organizarea activității pentru care a fost eliberată licența".
Art.60 lit. h) "instalarea de sisteme tehnice de alarmă împotriva efracției sau de componente ale acestora cu încălcarea prevederilor art. 28 alin. (6) şi (7), precum şi nerespectarea prevederilor art. 30 şi 31;" se sancționează cu amendă de la **5- 10 milioane lei."**
"(6) Instalarea, modificarea, inclusiv punerea în funcțiune a sistemelor de alarmare împotriva efracției, se avizează şi se controlează potrivit prevederilor alin. (2).
(7) Proiectele sistemelor de alarmare împotriva efracției se întocmesc în conformitate cu normele tehnice stabilite prin hotărâre a Guvernului.
ART. 31 -Se interzice comercializarea, în orice mod, a mijloacelor de alarmare împotriva efracției, a mijloacelor de protecție mecano-fizice sau a componentelor acestora fără prezentarea certificatului de calitate, eliberat de un laborator autorizat din țară, a standardului național sau internațional şi fără precizarea clasei de siguranță în care se încadrează, conform normelor europene."

Săvârşirea într-un interval de 3 luni a cel puțin două dintre contravențiile menționate, atrage suspendarea, pe o perioadă de la o lună la 3 luni, a dreptului societății sancționate de a încheia noi contracte şi de a angaja personal.

Depăşirea limitelor obiectului de activitate al societății specializate se sancționează cu amendă de la ***5-10 milioane lei şi anularea autorizației.***
ART. 35- (1) "Societăților specializate în domeniul sistemelor de alarmare le sunt interzise culegerea de informații, înregistrările audio sau video care excedează obiectului de activitate pentru care li s-a acordat licență, precum şi instalarea de echipamente disimulate care să le permită executarea acestor activități."
În conformitate cu art. 62, licența de funcționare a societăților se anulează în următoarele cazuri:
a) la săvârşirea uneia dintre contravențiile prevăzute la art. 60 lit. i) - k), dacă făptuitorul are calitatea de conducător al societății care are ca obiect de activitate paza şi/sau protecția, precum şi a contravențiilor prevăzute la art. 60 lit. l) şi m);

"i) refuzul de a asigura accesul reprezentanților autorităților publice aflați în exercițiul funcțiunii, al personalului poliției sau al jandarmeriei, special desemnat pentru exercitarea atribuțiilor legale de control, pentru luarea măsurilor de prevenire în obiectivele păzite sau asistate prin mijloace tehnice antiefracție şi în organizarea activității de gardă de corp;

j) depăşirea limitelor obiectului de activitate al societății specializate sau al corpurilor gardienilor publici;

k) refuzul de a furniza datele, informațiile sau documentele solicitate de către reprezentanții autorităților publice competente, potrivit legii, aflați în exercițiul funcțiunii;

l) executarea, în fapt, a atribuțiilor de organizare şi funcționare a activității societăților specializate de către persoane care au suferit condamnări pentru infracțiuni săvârşite cu intenție;

m) nerespectarea condițiilor care au stat la baza eliberării licenței de funcționare."

b) la repetarea, în interval de un an, a faptelor care atrag măsura suspendării;
c) la săvârşirea uneia dintre infracțiunile prevăzute la art. 59;
d) la săvârşirea de către conducătorii societăților specializate de pază şi protecție, ai celor licențiate în domeniul sistemelor de alarmare împotriva efracției ori al componentelor acestora sau al celor de monitorizare a sistemelor de alarmare a unor infracțiuni în legătură cu activitatea acestor societăți.

(2) Anularea licenței de funcționare se dispune de către Inspectoratul General al Poliției Române sau, după caz, de către instanța de judecată şi se comunică oficiului registrului comerțului

pe raza căruia funcţionează societatea specializată de pază şi protecţie, în termen de 10 zile de la data rămânerii definitive a procesului-verbal de contravenție sau a hotărârii judecătoreşti prin care s-a respins plângerea împotriva procesului-verbal de contravenție.

De asemenea, potrivit art. 32: "Beneficiarii, conducătorii şi personalul societăților specializate în domeniul sistemelor de alarmare şi al mijloacelor de protecție mecano-fizice sunt obligați să păstreze confidențialitatea informațiilor referitoare la sistemele instalate sau avute în întreținere."

Intocmit,
Comisar Sef Catrinoiu Aurel

CAZUISTICĂ PE LINIA SISTEMELOR DE ALARMARE ÎMPOTRIVA EFRACȚIEI

Eficiența sistemelor de alarmare este dată de modul de proiectare şi executare a instalațiilor, lipsa unor componente crează puncte vulnerabile care măreşte gradul de risc al producerii de evenimente negative.

Cele mai multe spargeri înregistrate în obiective protejate cu sistem au fost produse cu anihilarea (distrugerea) echipamentelor componente, dislocarea sirenelor exterioare şi scufundarea în apă, umplerea cu spumă poliuretanică ori distrugerea unităților centrale.

Concepția sistemelor de alarmă reprezintă segmentul care poate prevede în bună măsură asigurarea unei protecții eficiente, însă în cadrul acestei activități se constată greşeli din partea personalului firmelor specializate, respectiv, alegerea de soluții neadecvate (echipamente subdimensionate ca zone şi partiții, principii de funcționare etc.), lipsuri în structura sistemului, nesupravegherea căilor de acces şi a tuturor zonelor vulnerabile.

De asemenea, în cadrul activităților de instalare a echipamentelor se comit o mulțime de greşeli. Cele mai frecvente sunt de montare necorespunzătoare prin amplasare neadecvată ori cu nerespectarea caracteristicilor tehnice ale echipamentelor - centrala de alarmă în zona de intrare în obiectiv, detectori la înălțime mare, sirena de exterior la mică înălțime ori în zone uşor accesibile, neorientarea detectorilor.

Alte greşeli sunt cele de programare a centralei prin stabilirea unor timpi de temporizare la intrare mari, ceea ce facilitează acțiunile de anihilare a sistemului în această perioadă de timp.

Nemascarea traseelor cablurilor de conexiuni între echipamente la lucrările executate aparent permite descoperirea cu uşurință a elementelor sistemului, reuşindu-se obținerea de date despre sistem ceea ce poate ajuta persoanele interesate care pregătesc un atac asupra obiectivului să-l anihileze

Activitatea de mentenanță a echipamentelor cu toate că în multe cazuri este neglijată, prezintă importanță în depistarea componentelor defecte, acoperite, deplasate, murdare (zugrăvite), lovite etc., ceea ce presupune o revizie periodică a sistemului şi o testare a bunei funcționări.

Şi în utilizarea sistemelor sunt întâlnite o serie de greşeli, datorate în special lipsei de instruire a beneficiarului. În mod frecvent au fost constatate cazuri de nefolosire a sistemului prin nearmarea acestuia la plecarea din unitate, cazuri în care codurile nu erau personalizate, fiind folosit acelaşi cod de către tot personalul utilizator, coduri formate din datele de naştere ori numerele de telefon ale posesorilor, neschimbarea codurilor periodic sau ori de către ori s-a întâmplat spionarea codului de către alte persoane.

Sistemul nu se testează periodic, mergându-se pe premiza că acesta este funcțional şi nu se analizează periodic memoria jurnal a evenimentelor din centrala de alarmă pentru a se verifica modul de efectuare a serviciului de către personalul de pază.

Pentru eliminarea acestor neajunsuri organele de poliție prin maiştrii militari electronişti din serviciile de ordine publică trebuie să coordoneze şi controleze permanent toate segmentele de activități menționate.

Astfel, începând cu activitatea de proiectare prin verificările efectuate cu ocazia avizării trebuie să analizeze structura sistemului din aplicația ce urmează a fi executată pentru a se vedea modul de supraveghere a obiectivului și acoperirea punctelor vulnerabile.

În timpul activității de instalare a echipamentelor verificările în teren sunt necesare pentru a se urmări respectarea proiectului și în mod special locul de amplasare a componentelor sistemului.

De asemenea, modul de utilizare al sistemului trebuie controlat periodic pentru a se verifica dacă acesta este exploatat în mod corespunzător și este în perfectă stare de funcționare.

Trebuie remarcat că numai în aceste condiții sistemul de alarmă poate prezenta o eficiență sporită și poate aduce un aport substanțial sistemului de pază al obiectivului protejat.

Toate acestea conducând la înregistrări de fapte cu anihilări de sisteme ori eludarea acestora.

Exemplificăm, cazul de la Brașov, unde la Banca Românească în seara zilei de 08.04.2001, paznicul JINGA CONSTANTIN, de 21 ani, salariatul SC APS VALAHIA SRL Bucureşti, ce efectua serviciul de pază la sediul băncii a dispărut cu armamentul din dotare, sustrăgând din bancă suma de 7.600 dolari USA, 400 DM și 2.000.000 lei.

Verificările au reliefat că cel în cauză, după prezentarea la serviciu, la ora $19^{22,}$ a scos caseta video de la sistemul de televiziune cu circuit închis, după care, cunoscând codul, a dezarmat sistemul de alarmă, a pătruns în antetezaurul băncii și a deschis o casă de bani, cu cheile găsite într-un sertar, de unde a sustras sumele menționate.

Evenimentul s-a produs pe fondul lipsei de control asupra sistemului de pază și a gravelor neglijențe manifestate de personalul băncii, care l-a folosit anterior pe agentul de pază la transportul unor saci de bani, în acest fel observând codul de acces ce se folosea.

Pentru evitarea unor asemenea evenimente este necesar ca echipamentul de înregistrare să fie protejat și asigurat într-un spațiu cu acces numai pentru factorii de conducere.

De asemenea, în noaptea de 23/24.04.2000 autori necunoscuți au pătruns în sediul societății Liberty Oradea – punct de lucru Cluj Napoca după tăierea firelor telefonice ale întregii clădiri, aceștia au reușit să sustragă cca. 500 milioane lei păstrați într-un dulap. Sistemul de alarmă cu toate că era monitorizat pe linie telefonică, dispeceratul nu a recepționat semnalul de alarmă, iar din componența acestuia lipsea sirena de exterior care ar fi avertizat locatarii despre spargere.

Montarea necorespunzătoare a unității centrale a creat posibilitatea ca multe spargeri să nu fie semnalate în timp util, autorii reușind cu rapiditate să anihileze unitatea centrală și respectiv sistemul de alarmare.

La data de 16.08.2002, autori necunoscuți, prin tăierea încuietorii de la ușa de acces și la folosirea de chei potrivite au pătruns în două puncte de schimb valutar din București aparținând SC ADRIATICA EXCANGE SRL, de unde au sustras suma de 160 milioane lei.

Cu ocazia verificărilor în teren s-au constatat următoarele:

Punctele de schimb valutar sunt în spații separate, primul funcționează la parterul unui imobil de locuințe, în incinta unui spațiu comercial cu destinație de curățătorie chimică cu intrarea principală din stradă, iar cea secundară prin spatele imobilului, iar cel de-al doilea într-un spațiu propriu la o distanță de 10 metrii de primul, cu acces din stradă.

Spațiul aferent primului punct de schimb este compartimentat față de restul unității și față de clienți cu material din carton presat pe o înălțime de 2 metrii, fără a avea parte superioară și tavan. Accesul se realizează printr-o ușă confecționată din același material asigurată cu o încuietoare tip yală. Cel de-al doilea are compartimentare din sticlă normală vopsită, iar către exterior (stradă) vitrină din tâmplărie metalică cu geam termopan. Ușa de acces este din același material fiind asigurată cu două încuietori tip yală.

Valorile primului punct de schimb erau păstrate într-o casă de bani, de mărime 50 x 50 x 60 cm, încastrată în pardoseală și zidită de pereții laterali, respectiv casă tip HESPER de aproximativ 800 kg.

Pătrunderea în unitate s-a realizat pe ușa de acces principală prin tăierea inelului de asigurare cu lacăt, cu toate că exista clopot de protecție a încuietorii, a escaladat peretele punctului de schimb valutar și cu ajutorul unor chei potrivite a deschis casa de bani, de unde au sustras valorile existente, părăsind zona pe ușa din spatele clădirii.

Punctul de schimb valutar era prevăzută cu sistem de alarmă, care se compunea dintr-o centrală, doi senzori de prezență, un buton de panică, tastatură de comandă şi sirenă de exterior, echipamentele fiind instalate la deschiderea casei de schimb de o firmă specializată. Sistemul de alarmă supraveghează numai spațiul punctului de schimb, restul încăperii nefiind protejat, acesta fiind monitorizat pe linie telefonică la un dispecerat de zonă.

La orele 7^{00} şi 7^{02} la centrul de monitorizare s-au primit semnale de efracție de la cele două puncte de schimb, dispecerul de serviciu trimițând echipa de intervenție care însă a ajuns după ce autorii spargerii au părăsit zona. Din documentele existente echipa de intervenție a sosit la obiectivul alarmat în aproximativ 5 minute.

La nivelul biroului de ordine publică al Secției 8 poliție, urmează a se verifica activitățile desfăşurate de polițişti pe această linie.

În perioada 21-22 decembrie 2002, autori necunoscuți, prin tăierea încuietorii de la uşa de acces al magazinului UNISEM şi decuparea peretelui despărțitor, au pătruns în spațiul punctului de schimb valutar din Bucureşti aparținând SC THE BEST EXCHANGE SRL, de unde au sustras suma de 720 milioane lei şi 300 euro.

Cu ocazia verificărilor în teren s-au constatat următoarele:

Punctul de schimb valutar funcționează la parterul unui imobil de locuințe, într-un spațiu închiriat de la SC UNISEM SRL. Compartimentarea spațiului față de magazinul de semințe este totală şi realizată cu PAL melaminat de 2 cm, accesul în punctul de schimb făcându-se direct din Calea Moşilor printr-un spațiu în care funcționează un magazin de telefoane GSM.

Valorile punctului de schimb sunt păstrate într-o casă de bani cu două uşi, de mărime 90 x 50 x 60 cm, încastrată în zid.

Sistemul de alarmă este comun cu cel al magazinului de telefoane GSM, fiind compus dintr-o centrală, doi detectori de prezență, unul montat în spațiul casei de schimb şi celălalt la intrare în spațiul magazinului de telefoane şi o sirenă de exterior. Acesta este monitorizat prin sistem radio de o firma specializată

Pătrunderea în spațiul punctului s-a realizat prin tăierea lacătului şi forțarea încuietorii de la uşa magazinului UNISEM, care nu este protejat cu sistem de alarmă şi decuparea peretelui despărțitor realizat din pal melaminat de 2,5 cm pe o porțiune de 1m x 45 cm. Decuparea s-a realizat în zona de amplasare a casei de bani, permițând accesul necesar deschiderii uşilor casei de bani prin tăiere cu scule aşchietoare.

Detectorul de prezentă care supraveghează spațiul punctului de schimb este orientat spre uşa de acces, fără să acopere zona de amplasare a casei de bani, fapt ce a favorizat pătrunderea şi forțarea seifului fără ca sistemul de alarmă să sesizeze aceasta.

Nu a putut fi contactat administratorul casei de schimb pentru a se stabili cine a instalat sistemul de alarmă fără să existe avizul poliției pe proiectul sistemului.

Conform listingului de evenimente în perioada 21-23.12.ac. la dispeceratul societății nu s-a recepționat semnal de alarmă de la punctul de schimb, fiind efectuate două teste de probă în zilele de 21 şi 22 în jurul orelor 18^{50}, la care s-a confirmat funcționarea sistemului local, iar la verificare efectuată de polițiștii aflați la cercetarea la fața locului (orele 13^{06}) s-a stabilit că sistemul funcționează.

În noaptea 09/10 ianuarie 2003, autori necunoscuți, au pătruns în casa de schimb amplasată în incinta magazinului AUTO CROS SRL din Bucureşti, prin forțarea casei de bani, au furat din interiorul acesteia lei şi valută în valoare totală de circa 2.000 dolari USA.

Cu ocazia verificărilor în teren s-au constatat următoarele:

Punctul de schimb valutar funcționează la parterul unui imobil de locuințe, în incinta magazinului de covoare al SC AUTO CROS SRL, într-o compartimentare tip cabină realizată din tâmplărie de aluminiu cu geam normal.

Valorile punctului de schimb sunt păstrate într-o casă de bani cu o uşă tip Salamandra, de mărime 500 x 50 x 50 cm, încastrată în pardoseală.

Spațiul magazinului de covoare şi cel al punctului de schimb valutar au fost protejate prin sisteme de alarmă independente, care au fost distruse prin lovire cu corpuri contondente, cu toate că

centrala de alarmă a magazinului era montată la o înălțime foarte mare, folosindu-se pentru aceasta de un stativ de covoare. Nici un dintre sisteme nu avea prevăzută sirenă de exterior ori comunicator de transmitere la distanță a semnalului de alarmă și nu erau avizate de poliție.

Pătrunderea în spațiul punctului s-a realizat prin tăierea lacătelor de la ușa magazinului de covoare și descuierea yalei ușii cabinei punctului de schimb. Prin decupare cu ajutorul unor scule tăietoare au fost practicate două orificii de aproximativ 7x7 cm în ușa casei de bani, reușind deschiderea ușii și devalizarea valorilor monetare, autorii părăsind încăperea pe ușa din spatele imobilului.

Cu ocazia verificărilor nu a putut fi contactat administratorul casei de schimb pentru a se stabili cine a instalat sistemul de alarmă fără să existe avizul poliției pe proiectul sistemului.

La data de 16.01.2003, ofițerul de serviciul al Secției 15 poliție a fost sesizat de dispeceratul IDM cu privire la faptul că în jurul orelor 20[15], un individ necunoscut a furat din incinta punctului de schimb valutar 8.860.163 lei, 2350 dolari USA și 150 euro.

Cu ocazia verificărilor în teren s-au constatat următoarele:

Punctul de schimb valutar funcționează la parterul unui imobil de locuințe, având intrarea direct din bulevard, cu vecini, magazin de mobilă la stânga și agenție Loto Prono la dreapta.

Spațiul punctului de schimb a fost realizat prin compartimentare din magazinul de mobilă, având pereții comuni realizați din material tip PAL, protejați cu tablă de fier de aproximativ 5 mm și grilaj metalic la plafon (pe exterior), fiind creat spațiu separat pentru lucrător și clienți. Delimitarea spațiului este totală fiind realizată din același material, având ghișeul de tranzacții monetare din sticlă securizată și ușă de acces care poate fi blocată din interior cu ajutorul a două zăvoare.

Valorile punctului de schimb sunt păstrate într-o casă de bani cu două compartimente de mărime 1200 x 60 x 60 cm, încastrată în pardoseală.

Punctul de schimb valutar este protejat cu sistem de alarmă compus dintr-o centrală tip DSC, doi senzori PIR, în hol clienți și lucrător, contact magnetic la ușa exterioară și două sirene, interioară și exterioară.

De asemenea, punctul este supravegheat de o cameră video cu înregistrare pe casetă video, cu pornire la apariția mișcării în zona gestionarului, instalație realizată artizanal care asigura o înregistrare secvențială. Camera video este amplasată în spațiul lucrătorului și supraveghea în mod special activitatea acestuia, cuprinzând și puțin zona clientului de la ghișeu, limitarea fiind determinată de afișele lipite pe sticla ghișeului.

În jurul orelor, 20 [15], după ora de închidere a unității, în momentul în care gestionarul de serviciu HAGIU GABRIELA de 32 de ani a vrut să iasă din punctul valutar, un individ de aproximativ 1,70 m, slab, îmbrăcat cu o geacă de culoare de culoare închisă, cu fes pe cap și pulover cu gât ridicat la nivelul bărbiei, a împins-o în interior și prin amenințare verbală a determinat-o să se așeze cu fața la pardoseală, i-a luat cheile și a descuiat casa de bani de unde a luat 8.860.163 lei, 2350 dolari USA și 150 euro, deși în casa de bani se mai aflau 70.254.00 lei, 172 dolari, 16 euro și 5 lire englezești.

Înainte de a pleca autorul a legat-o pe Hagiu Gabriela la gură, mâini și picioare cu bandă de scoch pentru ambalaj, a scos caseta din videorecorder prin forțarea cutiei unde acesta este asigurat, însă a aceasta a fost găsită pe casa de bani.

După vizionarea casetei video a rezultat că momentul producerii evenimentului nu a fost surprins de camera video.

Cu ocazia cercetării efectuate la fața locului au fost ridicate mai multe urme papilare, cercetările fiind continuate de polițiștii Secției 15.

Un caz în care autorii au acționat cu mult profesionalism, îl constituie cel comis la 01.11.2002, în București la casa de schimb valutar aparținând SC PARIS EXCHANGE SRL, când autori necunoscuți au pătruns în spațiul punctului de schimb prin subsolul imobilului, secționând și înlăturând o țeavă de plastic destinată scurgerii apei menajere, apoi realizând spargerea peretelui despărțitor al încăperii unde se afla seiful cu valori. Acesta avea o grosime de circa 3 cm, fiind confecționat din beton cu plasă de sârmă. S-a reușit forțarea casei de bani și sustragerea a 12.500 dolari USA, 760 Euro și 500.000 lei. Spațiul punctului de schimb era prevăzut cu sistem de alarmare, însă în încăperea unde era casa de bani nu exista detector de prezență.

În acest caz, rezultă clar că autorii au făcut în prealabil o documentare amănunțită cu privire la spațiul, vecinătățile şi dotările punctului de schimb.

Poliția Secției 19 a fost sesizată telefonic că în noaptea de 17-18 octombrie a.c. în jurul orelor 2^{45}, autori necunoscuți prin amenințare cu o armă au solicitat vânzătoarei de la barul aflat în incinta stației de benzină OMV situată pe şoseaua Alexandriei, banii proveniți din încasări.

În urma negocierilor cu aceştia şi arătându-le că au fost filmați de camerele de supraveghere, autorii au renunțat la acțiune, fiind identificați în persoana numiților Ioniță George de 26 ani, Costache George Ştefan, 21 ani, ambii din Bucureşti şi Hodoroagă Cristian Alexandru, 18 ani din comuna Botoroagă, jud.Teleorman.

Cu ocazia verificărilor în teren s-au constatat următoarele:

În incinta stației de benzină este amenajat un bar şi un magazin de produse, pentru deservirea acestora fiind prevăzut un lucrător în afara celui care deserveşte stația de benzină.

Pentru asigurarea securității stației există prevăzut un post de pază pe trei schimburi, neînarmat, încadrat cu personal de la o societate specializată, conform planului de pază aprobat.

De asemenea, firma menționată a instalat un sistem electronic de securitate format din instalația de supraveghere video şi antiefracție, care este monitorizat pe linie telefonică la dispeceratul aceleaşi societăți.

Instalația de televiziune cu circuit închis este compusă din 10 camere de luat vederi care supraveghează zonele celor 4 pompe de benzină, cele două case de marcat ale încasărilor, zona barului şi exteriorul magazinului (partea din spate), spălătoriei. Imaginile preluate sunt prelucrate şi înregistrate cu sistemul digital Matrix pe un computer cu o autonomie la înregistrare de 72 ore. Sistemul antiefracție cuprinde unitatea centrală şi 3 butoane de panică, montate la casele de marcat şi în biroul şefului de stație.

Valorile monetare sunt păstrate într-un seif tip Hesper cu trapă, fixat în perete, cu acces pentru depunerea banilor din magazin. Valorile din seif pot fi ridicate numai din biroul şefului de stație unde sunt situate şi uşile seifului.

În noaptea de 17/18 oct. a.c. în serviciu se aflau două persoane, una la bar şi casiera de la stația de benzină.

În timpul atacului, casiera de serviciu a avut prezența de spirit de a atrage atenția agresorilor asupra camerelor de luat vederi spunându-le că sunt filmați şi astfel vor fi foarte uşor identificați de poliție, fără a acționa butonul de panică, motiv pentru care aceştia au renunțat la intenția lor, fiind identificați ulterior pe baza înregistrărilor sistemului de TVCI.

În urma percheziției efectuate la locuința numitului Costache George Ştefan a fost găsită o puşcă cu aer comprimat tip "Gamo" cal.4,5 mm, două pistoale cu aer comprimat, două lunete pentru armă, o bâtă de base-ball, un lanț, mai multe cuțite de vânătoare şi alice de plumb pentru puşcă şi pistoale, precum şi un binoclu marca "Practica- 10x25S".

Cercetările sunt continuate cu primii doi în stare de reținere, luându-se măsuri de depistare şi prindere a celui de-al treilea autor care este dispărut de la domiciliu, pentru tentativă la infracțiunea de tâlhărie şi complicitate la tentativă de tâlhărie.

Deşi stația de benzină este asigurată cu un post de pază permanent, în timpul atacului, agentul de pază aflat în serviciu nu era de față întrucât se afla în vestiar unde dormea.

Verificându-se documentele aflate în obiectiv s-a constatat că nu s-a consemnat evenimentul în registrul special destinat, nu s-a întocmit de fiecare dată proces verbal de predare primire a serviciului şi nu s-au efectuat controale de noapte din partea conducerii societății de pază.

Imaginile cu evenimentul au fost copiate pe un CD şi predate Secției 19 poliție pentru continuarea cercetărilor.

Au mai fost cazuri de nepăstrare a confidențialității codurilor de acces, neglijență a personalului propriu care a mascat zona de supraveghere a detectorului ori a acoperit obiectivul camerei video.

Cu ocazia analizelor de caz efectuate au rezultat următoarele aspecte:

- echipamentele sistemelor de alarmare nu sunt instalate profesional ori sunt incomplete, neprezentând astfel, eficiența scontată în detectarea pătrunderilor în spațiile supravegheate și alarmarea personalului abilitat ori a autorităților;
- nu sunt protejate spațiile prin alegerea mai multor soluții tehnice;
- nu sunt respectate condițiile de fixare mecanică a echipamentelor;
- utilizatorii nu folosesc toate facilitățile sistemelor și nu respectă regulile tehnic privind testarea periodică a funcționării.

Intocmit,
Comisar Sef Catrinoiu Aurel

REGULI DE PROIECTARE A SISTEMELOR DE ALARMARE ÎMPOTRIVA EFRACȚIEI.

Conținutul proiectelor de execuție a aplicațiilor

În conformitate cu prevederile normelor metodologice de aplicare a Legii nr.333/2003 privind paza obiectivelor, bunurilor, valorilor și protecția persoanelor, instalarea sistemelor de alarmare se face în baza proiectului de execuție avizate de poliție.

Proiectele sistemelor de alarmare vor fi întocmite de personalul tehnic avizat al societăților licențiate în acest sens, cu respectarea prezentelor norme tehnice.

Proiectarea aplicațiilor cu sisteme de alarmare împotriva efracției se realizează cu respectarea normelor în domeniu și a celor proprii unităților, ținându-se seama de gradul de protecție stabilit de conducerea unităților în funcție de valorile ce trebuie protejate (umane și materiale), existența și situarea zonelor vitale, căile de acces, circulația personalului propriu și al clienților, amenajările mecano-fizice realizate, tipul pazei, amplasarea dispozitivului de pază și depărtarea față de echipajul specializat de intervenție cu care unitatea are contract de prestări servicii.

Proiectele de execuție ce urmează a fi avizate se vor prezenta la Serviciul poliției de ordine publică al inspectoratului județean pe a cărui rază teritorială se află obiectivul sau la Direcția Generală de Poliției a Municipiului București, după caz, și vor cuprinde următoarele documente:

a) cererea de avizare a beneficiarului, care va conține: adresa beneficiarului și a obiectivului ce urmează a fi protejat, numărul de telefon/fax, obiectul proiectului și termenul de realizare, societatea care execută lucrarea și numărul licenței emise de Inspectoratul General al Poliției Române, personalul care a întocmit, verificat și aprobat proiectul și șeful de lucrare cu numerele avizelor eliberate de poliție;
b) planul cuprinzând amplasamentul și împrejurimile obiectivului la care urmează să se execute lucrarea de instalare a sistemului de alarmare împotriva efracției, cu denumirea străzilor și a clădirilor cu care se învecinează (schiță);se precizează și căile de acces și dedicațiile acestora.
c) elemente privind construcția: tipul construcției (veche, nouă, reamenajată, în construcție), dimensiunile încăperilor (înălțime, lungime, lățime), cât și destinația acestora, toate fiind realizate la o scară convenabilă. La clădirile vechi sau la cele care se reamenajează, în mod obligatoriu, trebuie să se facă referire la materialele de construcție, grosimea pereților exteriori, a plafoanelor și pardoselilor, cât și pereților camerelor unde se păstrează valori. Pentru suprafețele vitrate, ferestre și ușile de acces se va preciza modul de protejare cu mijloace mecano-fizice și clasa de siguranță a acestora.
d) prezentarea tabelară a structurii sistemului de alarmare împotriva efracției pe categorii de instalații (efracție, control acces, TVCI) propus pentru instalare: denumirea și tipul elementelor (componentelor), numărul acestora, denumirea firmei producătoare, furnizorul, avize de calitate

e) descrierea zonelor protejate prin sistemul de alarmare împotriva efracției, elementul de detecție alocat, modul de programare al zonei şi partiția din care face parte (prezentare tabelară), iar notarea elementelor de detecție din structura sistemului de alarmare împotriva efracției se va regăsi în desenele proiectului. Aceleaşi descrieri şi pentru celelalte subsisteme:
   - pentru TVCI se vor preciza camerele video şi zonele supravegheate, menționându-se imaginea care se doreşte a fi preluată
   (imagine de ansamblu ori de detaliu) şi țintele care se doresc a fi supravegheate (clienți, personal propriu etc). În situația camerelor mobile se precizează zonele de interes acoperite şi procedura de localizare a acesteia.

Se va întocmi memoriu tehnic situațiile proiectate pentru fiecare instalație, precizându-se ce funcțiuni realizează fiecare componentă şi modul de utilizare al întregului sistem.

f) specificarea locului de amplasare al centralei de alarmare împotriva efracției şi a tastaturilor de comandă precum şi al echipamentelor de control acces şi TVCI;
g) calculul energetic al sistemului din care să rezulte autonomia acestuia în cazul scoaterii din funcțiune a rețelei de tensiune (pe instalații);
h) datele tehnice de catalog ale elementelor sistemului de alarmare împotriva efracției, performanțe, domenii de utilizare, descrierea funcțională, posibilități de programare şi alte facilități cu anexarea prospectelor producătorului;
i) modul de asigurare a garanției, service-lui şi intervenției în cazul defectării sistemului de alarmare împotriva efracției. Termenul maxim de remediere a defecțiunilor sistemelor de alarmare împotriva efracției instalate în obiectivele de importanță va fi de maxim 12 ore în localitatea firmei instalatoare, respectiv 24 ore în alte localități;
j) jurnalul de cabluri în care se precizează conexiunile(de la doza, până la…), codul cablului, tipul de cablu folosit şi secțiunea;
k) documentele de certificare pentru echipamentele utilizate, emise de un laborator acreditat conform legii;
l) desenele obiectivului cu amplasarea elementelor componente sistemului, care vor fi întocmite la o scară convenabilă, folosindu-se simboluri standardizate şi formate standardizate cu includerea cartuşului. Desenele se realizează separat pe tipuri de instalații, executându-se şi scheme bloc pentru fiecare instalație.

(1) Proiectele vor fi întocmite cu respectarea următoarelor cerințe:

a) întocmirea în două exemplare, unul se va preda beneficiarului pe bază de proces verbal, celălalt se va păstra de proiectant în regimul documentelor secrete de serviciu, cu respectarea legii.

b) înregistrarea proiectelor de proiectant, atribuirea unui cod şi numerotarea filelor, cu specificarea numărului total de file, în antetul sau subsolul cărora se vor trece codul şi denumirea firmei proiectante;

c) realizarea paginii de titlu, cu menționarea obiectivului şi a personalului care a întocmit documentația;

(2) Accesul la proiectele sistemelor de alarmare împotriva efracției este permis numai personalului autorizat, care are atribuții profesionale în legătură cu acesta.

Aspecte care se vor urmării cu ocazia întocmirii proiectelor:

- semnarea paginilor care necesită aceasta (pagina de titlu, desene);
- corelarea între notarea (identificarea) elementelor de detecție din tabelul de zonare şi indicativele din desenele obiectivului, precum şi cu specificația de aparatură (nr. bucăți);
- existența tuturor capitolelor şi datelor precizate;
- concordanța cu realitatea a desenelor cu compartimentările obiectivului;

Intocmit,
Comisar Sef Catrinoiu Aurel

**SISTEME DE SECURITATE ANTIEFRATIE
SI PROTECTIE PERIMETRALA**.

Modulul VII: Sisteme de securitate antiefratie si protectie perimetrala.

***Tema nr 4**: Principii de detectie, tipuri de detectoare*

1. Ce este un sistem de securitate electronic: Definitie, exemplificari.
2. Detectie / detectoare: tipuri de detectie, principiul de detectie, cum se instaleaza, care sunt cauzele de alarme false sau modalitati de sabotare.

***Tema nr 5**: Arhitectura unui sistem. Concepte si terminologie. Comunicatia intre componentele sistemului si centrala.*
***Tema nr 6**: Programarea sistemelor de securitate: principii de baza.*
***Tema nr 7:** Testarea periodica si mentenanta.*

Modulul VIII: Executia si mentenanta sistemelor de securitate antiefractie si protectie perimetrala

***Tema nr 1** - Caracteristicile sistemului instalat*
***Tema nr 2** - Echipamentele de protectie*
***Tema nr 3** - Starea de functionare a sistemului*
***Tema nr 4** - Mentenanta sistemului*
***Tema nr 5** - Alimentarea cu energie electric a sistemului*
***Tema nr 6** - Setarile programelor configurare a echipamentelor/ sistemelor tehnice de detecție, efracție și control acces*

Modulul VII: Sisteme de securitate antiefratie si protectie perimetrala.

Introducere: Mecanismul de asigurare a securitatii unui obiectiv

Realizarea securitatii unui obiectiv este un proces structurat pe urmatoarele 4 componente:

1. *Detectia evenimentului*
2. *Transmiterea evenimentului catre dispeceratul de monitorizare si interventie si /sau evaluarea alarmei*
3. *Asigurarea intirzierii evenimentului prin mijloace de securitate mecanica*
4. *Asigurarea interventiei*

Detectia evenimentului se realizeaza cu ajutorul sistemelor de securitate antiefractie si protectie perimetrala, utilizind senzori adecvati metodelor de intruziune ce se doreste a fi detectata, specifice obiectivului. Desi sunt folosite principii si tehnologii comune, exista o diferenta semnificativa intre detectia antiefractie la interior si detectia la exterior necesara in cazul sistemelor de protectie perimetrala. Aceasta diferenta este generata de factorii de mediu externi, mult mai “agresivi” in cazul protectiei perimetrale.

Transmiterea evenimentului catre dispeceratul de monitorizare este specifica sistemelor de securitate antiefractie si este tratata intr-un modul separat in acest curs. In cazul protectiei perimetrale, pentru a asigura o interventie eficienta (localizare precisa a evenimentului si eliminarea alarmelor specifice

mediului) este necesara evaluarea evenimentului (operatiune care se efectueaza cu ajutorul sistemelor CCTV. Timpul de reactie este extrem de important, evaluarea alarmei si asigurarea interventiei fiind asigurate de "factorul uman".

Acest modul de curs prezinta conceptele ce stau la baza realizarii primei componente a mecanismului de asigurare a securitatii.

***Tema nr 4**: Principii de detectie, tipuri de detectoare*

1. Ce este un sistem de securitate electronic: Definitie, exemplificari.

Ca functionalitate primara, un sistem de securitate poate fi definit ca un ansamblu de dispozitive ce detecteaza si semnalizeaza o intruziune sau o stare de pericol asociata intrarii neautorizate in spatiul protejat. Dezvoltarea capacitatii de prelucrare a informatiilor precum si a tehnologiilor de comunicatie au extins functiunile primare ale sistemului de securitate astfel incit, in prezent, pot fi monitorizate mai multe tipuri de evenimente ce descriu o situatie potentiala de pericol cum ar fi alarmele de tip tehnic sau medical.

Domeniul de aplicatie este extrem de vast: de la aplicatii rezidentiale la sisteme de inalta securitate. In functie de particularitatile obiectivului protejat (cu referire deosebita la valorile ce trebuiesc protejate) gradul de complexitate al unui sistem poate varia foarte mult, insa principiile care stau la baza unui sistem electronic de securitate sunt aproape intotdeauna aceleasi.

FF IMPORTANT: orice sistem de securitate are si rolul de a se autoproteja la interventii neautorizate. Pentru realizarea acestei functii, toate dispozitivele sistemului sunt prevazute cu un contact antisabotaj (tamper). Rolul acestuia este de a genera o alarma speciala, de sabotaj, atunci cind se incearca interventia in sistem. De asemenea, cutiile de jonctiuni pentru sistemele de securitate sunt special construite si protejate cu un contact anti-sabotaj.

Exista doua categorii de detectie: detectia pasiva si cea activa.

Detectia pasiva este cea care utilizeaza un parametru existent in mediu asociat evenimentului ce se doreste a fi detectat. Detectorul este un "observator tacut" al mediului.

Detectia activa presupune generarea unui parametru in mediul supravegheat a carui modificare este asociata cu evenimentul care se doreste a fi detectat.

2. Detectie / detectoare: tipuri de detectie, principiul de detectie, cum se instaleaza, care sunt cauzele de alarme false sau modalitati de sabotare

a. Contactul magnetic

Cel mai "vechi" senzor utilizat de la inceputurile sistemelor de securitate este contactul mecanic. Acesta a fost utilizat pentru sesizarea pozitiei elementelor de acces in spatiile protejate: usi si ferestre. Conform definitiei, contactul mecanic este un senzor pasiv, starea sa fiind dictata de elementele din mediu supravegheate. Ca dispozitiv de securitate, contactul mecanic este usor sabotabil iar montarea si reglajul sunt dificile in cele mai multe cazuri. El este in continuare intilnit in dispozitive electromecanice de control al accesului, fiind incorporat in dispozitiv in faza de productie al acestuia.

Contactul mecanic a fost inlocuit de contactul magnetic, un ansamblu format dintr-un releu reed si un magnet (fig. 1)

- Magnet
- Contact magnetic propriu-zis (releu reed)
- Elemente distantiere si protectoare a terminalelor

Fig. 1 Ansamblu contact magnetic

Ca ansamblu, contactul magnetic este un senzor activ; magnetul genereaza cimpul supravegheat. Prin modificarea pozitiei acestuia, cimpul magnetic care actioneaza releul reed si il "tine" in pozitia inchis (N.C.) scade in intensitate pina cind contactul se deschide, semnalizind o stare de alarma.
Exista o varietate mare de tipuri constructive, toate avind acelasi principiu de functionare. Pentru aplicatii destinate usilor metalice se poate utiliza varianta constructiva numita "heavy duty" care prin modalitatea de instalare creaza un intrefier intre dispozitiv si usa metalica, permitind functionarea corecta a contactului magnetic. De asemenea se pot utiliza versiuni incastrate in tocul usii sau ferestrei precum si contacte magnetice pentru usi sectionale a caror pozitie de inchidere poate prezenta abateri de ordinul milimetrilor.

Contactul magnetic poate fi sabotat relativ usor, prin utilizarea unui magnet exterior puternic in cazul in care este cunoscuta pozitia in care acesta este instalat. Exista tipuri constructive care au o imunitate ridicata la sabotarea cu magnet extern, la care magnetul se pozitioneaza intr-o plaja limitata a distantelor (prea aproape sau prea departe de contact genereaza alarma).

De asemenea, contactul magnetic nu poate fi utilizat in aplicatii de inalta securitate pe instalatii de control al accesului pentru activarea intrarilor de tip usa deschisa, dar este util ca element suplimentar de control.

b. Senzorul pasiv in infra-rosu (PIR)

Senzorul pasiv in IR este un dispozitiv destinat detectiei deplasarii cu minim 10-15 cm/s a unui corp cu diferenta de temperatura fata de mediu de minim 3-5^{0}C.
Senzorul PIR utilizeaza un dispozitiv sensibil la radiatia infrarosie din spectrul termic (8-14 μm) numit piroelement (fig2).

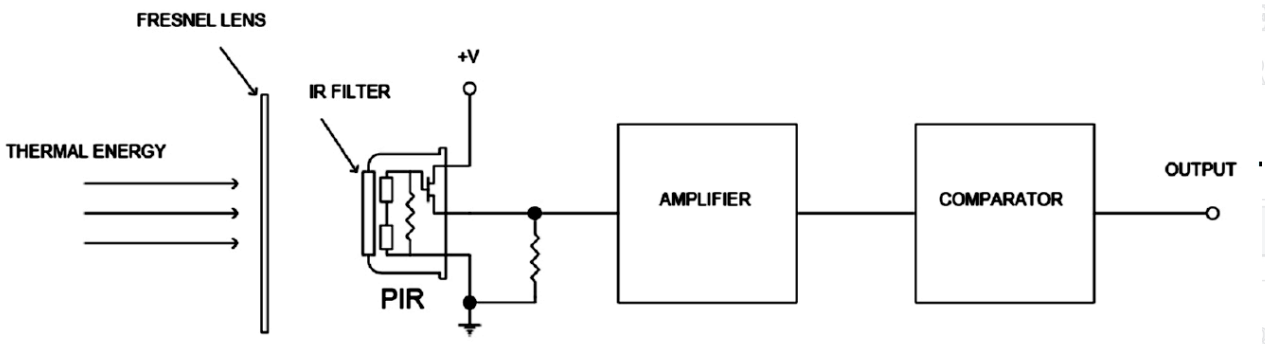


Fig 2. Schema de principiu a unui sensor pasiv in infrarosu

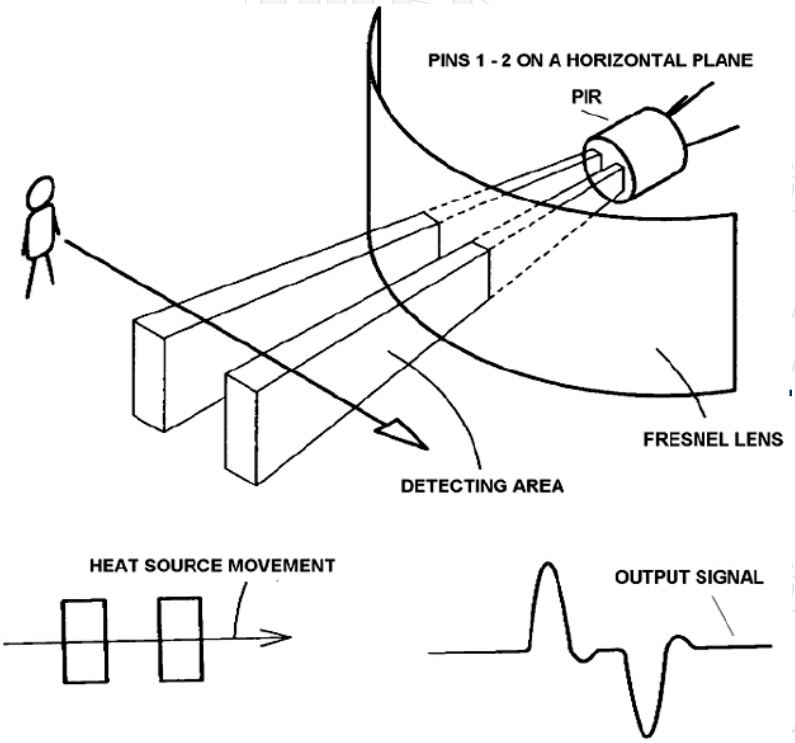


Fig. 3 Principiul de functionare al senzorului PIR

Pentru concentrarea radiatiei infrarosii se utilizeaza un ansamblu special de lentile Fresnell. Modul de amplasare si dimensiunile acestora determina caracteristica de detectie a senzorului. Exista senzori volumetrici, senzori cortina, senzori cu spot lung, senzori de tavan.

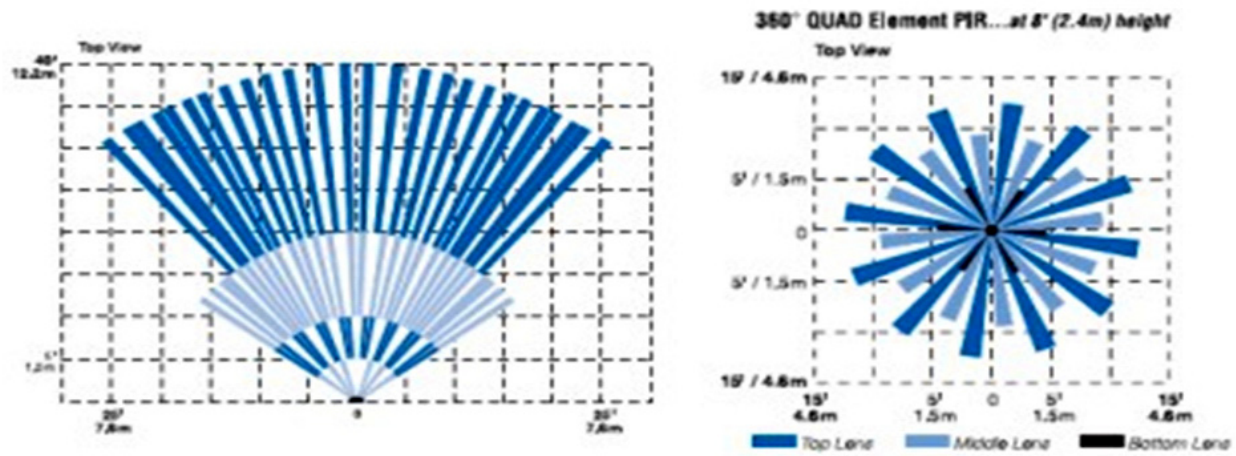


Fig 4 Exemple de caracteristici de detectie:
Pentru senzor cu mai multe nivele a spoturilor si pentru senzori de tavan



Regleta de jonctiuni | Contact antisabotaj | Piroelement | Switch-uri pentru selectarea sensibilitatii

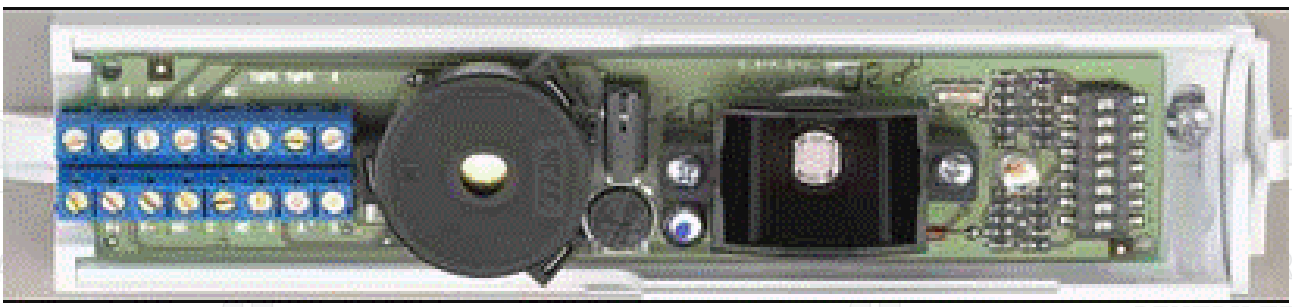


Fig. 5 Tipuri de senzori IR

O alta modalitate de concentrare a radiatiei este data de utilizarea unei oglinzi concentratoare de forma parabolica, piroelementul situandu-se in focarul parabolei. PIR-urile cu oglinda sunt senzori volumetrici in adevaratul inteles al cuvantului.

Senzorul PIR prezinta doua avantaje:
i. Elementele de delimitare a spatiilor (pereti, geamuri, usi) sunt opace la radiatia IR, astfel incit senzorul nu detecteaza miscare in exteriorul spatiului protejat.
ii. Datorita flexibilitatii in constructia lentilelor Fresnell exista tipuri constructive pentru o varietate larga de aplicatii.

Detectoarele obisnuite se instaleaza in general la 2 – 2,3 m de la poadeaua incaperii si au un unghi de detectie de 90 – 105^0. Se instaleaza de regula in colturile incaperii pentru a asigura o protectie completa. Raza de detectie pe spoturile centrale este in general de 12m, ceea ce face suficienta instalarea unui singur senzor intr-o incapere obisnuita.

Dezvoltarea tipurilor constructive de piroelemente (dual element, quad element) au permis fabricarea de senzori PIR imuni la corpuri de dimensiune redusa (pet imune) precum si la senzori cu procesare digitala avansata pentru cresterea imunitatii la alarme false.

Pentru protectie perimetrala exista senzori special construiti sa functioneze atit in conditii speciale de mediu cit si cu performante ridicate (distanta supravegheata). In acest scop se produc senzori cu lob ingust, cu lentila mare, care au o acoperire de max. 120m, vezi fig. 6.

Fig. 6 Senzor IR de exterior

Senzorul PIR este un senzor mascabil – el functioneaza numai in raza de vizibilitate. Vopselurile, hirtia, sticla obisnuita sunt opace la radiatia IR, ceea ce face ca senzorul sa fie relativ usor sabotabil in cazul in care potentialul infractor are acces la senzor atunci cind zona supravegreata de acesta cand sistemul de securitate nu este activat.
Pentru evitarea alarmelor false sunt necesare anumite masuri de prevenire a miscarii accidentale a corpurilor din incaperi (ex. hirtia termica de fax) precum si a curentilor de aer calzi sau reci (ferestre deschise, amplasare necorespunzatoare a senzorilor fata de instalatiile de climatizare sau convectoare de caldura.
Cu toate aceste limitari, senzorul PIR este cel mai popular element utilizat in sistemele de securitate datorita flexibilitatii ridicate si a costului scazut al dispozitivului.

c. Senzorul activ cu microunde

Detectoarele cu microunde sunt senzori activi care genereaza un cimp electromagnetic in spatiul protejat. Orice miscare a unui corp care reflecta radiatia electromagnetica este sesizata si genereaza alarma. Principiul de detectie se bazeaza pe efectul Doppler. Senzorii transmit semnale in banda X de regula (10,5 Ghz) dar exista si produse fabrcate in benzile S (2,54 Ghz) sau K (24 Ghz) generate de o dioda Gunn care nu are efecte nocive asupra oamenilor sau echipamentelor sensibile (pacemakere etc.).

Puterea semnalului este de asemenea extrem de redusa, semnalul avind o bataie de maximum 100m in linie dreapta. Deviatia de frecventa masurata prin efect Doppler este de ordinul herzilor (20 – 100Hz). Aceasta gama este corelata cu miscarea unui corp uman; orice alte frecvente fiind excluse.
Emitatorul si receptorul sunt amplasate in aceeasi carcasa. Aria de acoperire este reglabila in funcite de sensibilitatea receptorului. Acest reglaj este deosebit de important intrucit microundele trec de regula prin pereti, char si cei din beton armat.

Detectoarele cu microunde se pot utiliza atit la interior cit si la exterior, nefiind sensibile la variatii termice sau curenti de aer. Sunt detectoare sensibile, greu sau imposibil de mascat dar au ca problema principala imposibilitatea delimitarii spatiului protejat.
In conditiile in care exista surse electromagnetice de frecvente apropiate (banda X) apar limitari de utilizare. Zonele iluminate cu tuburi fluorescente pot genera alarme false; ciclul de ionizare creat de astfel de lampi putind fi interpretat de detector ca o alarma falsa.
Senzorul poate fi mascat cu obiecte metalice mari, care reflecta radiatia electromagnetica in spectrul mentionat.

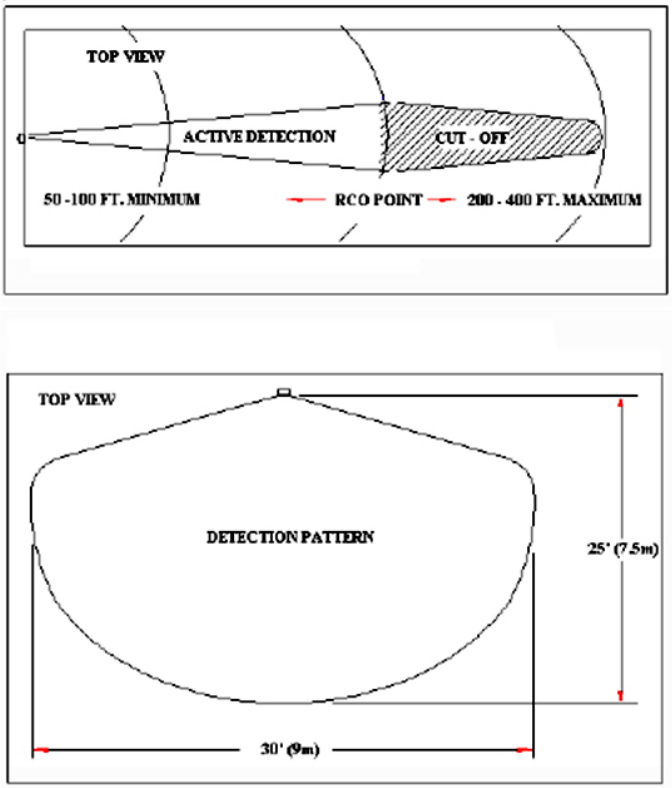


Fig. 7. Carcteristici de directivitate a detectoarelor cu microunde: zona de detectie activa funcite de distanta si zona de acoperire

Pentru delimitarea stricta a zonei supravegheate peretii trebuiesc ecranati. Acest lucru se poate realiza relativ usor in cazul peretilor armati cu plasa metalica, tinind cont ca plasa metalica este un ecran in cazul in care dimensiunile ochiurilor plasei sunt mai mici decit lungimea de unda a semnalului detectorului.
Pentru detectoarele care functioneaza in banda X, lungimea de unda este de 3 cm.

Pentru protectia perimetrala exista dispozitive active monostatice (emitator si receptor incorporate), in aceleasi benzi K si X. Ca o regula generala de amplasare, dispozitivele trebuie sa se protejeze intre ele.

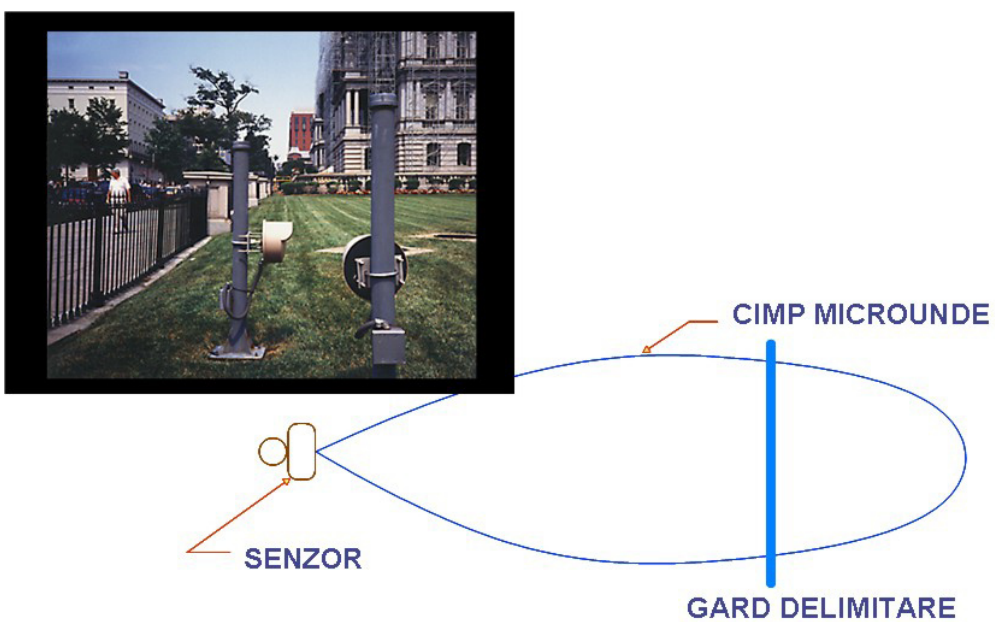


Fig. 8 Amplasarea detectoarelor monostatice cu MW

Si in cazul detectoarelor monostatice de exterior se impune controlul distantei pe care se face detectia.

d. Senzorul de vibratii

Detectoarele de vibratii sau socuri sunt destinate in general unor aplicatii speciale, cum ar fi protectia peretilor tezaurelor dar si a unor suprafete vitrate. Detectoarele de socuri contin un traductor care transforma semnale de tip acustic in semnale electrice. In general, traductorul este de tip piezo dar exista si alte tipuri de traductoare.

Fig. 9 Senzor de soc/vibratie

Raza de detectie este variabila, functie de natura materialului din care este construit peretele protejat. Majoritatea producatorilor asigura o raza de acoperire de aproximativ 6m pentru pereti de beton. Aceste detectoare sunt sensibile la alarme false cum ar fi ciocanituri in pereti sau zgomote de reparatii din restul cladirii ceea ce face ca utilizarea lor sa fie limitata din cauza acestor factori.

La instalarea acestor detectoare trebuie analizata structura peretilor protejati: atit materialul de baza (beton, caramida, lemn etc.) cit si materialul de acoperire sau izolatie. Spre exemplu, instalarea unui senzor de soc pe un perete de beton armat acoperit cu un strat izolator antifonic de polistiren expandat trebuie realizata prin aplicarea senzorului de soc pe strucrtura de baza a peretelui, inainte de acoperirea acestuia cu polistiren. De asemenea, trebuie luat in calcul un coeficient mult mai mare de absorbtie a sunetelor.

Reglarea sensibilitatii este de asemenea o operatiune importanta. Senzorul nu trebuie sa fie extrem de sensibil pentru a elimina pe cit posibil alarmele datorate zgomotului de mediu.

e. Senzorul de geam spart

Detectoarele de geam spart functioneaza pe principiul analizei spectrale sunetului produs de spargerea unei suprafete vitrate (spectrul intre 1 si 5 Khz). Acest sunet are in componenta sa armonici superioare la o anumita intensitate sonora ceea ce face ca sunetul sa poata fi distins de alte zgomote din mediu. Acest tip de senzori este mult mai indicat pentru protejarea suprafetelor vitrate decit senzorii de vibratii intrucit nu sunt sensibili la zgomotele exterioare (de regula de joasa frecventa). Senzorul se monteaza la o distanta de pina la 5m de suprafata vitrata si are a acoperire de aprox. 6 metri.

Datorita diversitatii materialelor din care se fac in prezent suprafete vitrate anumiti producatori de echipament calibreaza senzorii in functie de tipul de material al zonei protejate.

Testarea si reglajul se fac cu dispozitive speciale (testere simulatoare). Implicit, producatorii care au o gama mai larga de detectoare de geam spart pun la dispozitie si testerele specifice fiecarui tip de detector.

Principala limitare consta in faptul ca un geam poate fi taiat fara a genera zgomotul specific de spargere. Se recomanda ca atit detectoarele de socuri cit si detectoarele de geam spart sa fie utilizate in conjunctie cu elemente de detectie volumetrica.

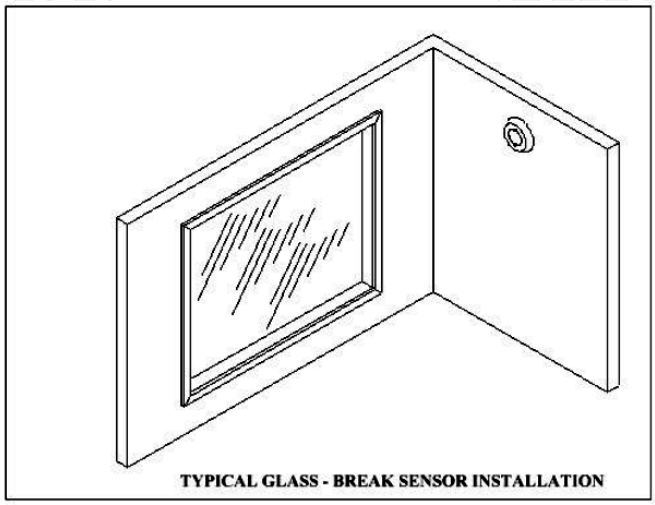


Fig. 10 Instalare tipica a unui detector de geam spart

Fig. 11 Detector de geam spar

f. Senzorul geofonic (seismic)

Senzorii seismici sunt utilizati in aplicatii de inalta securitate avind o functie similara senzorilor de vibratii. Diferenta majora dintre cele doua tipuri de detectoare consta in spectrul de frecventa analizat. Asa cum aratam in paragraful principii de detectie, detectoarele seismice analizeaza spectrul subsonic cuprins intre 4 si 6 Hz.

Acest tip de senzor este foarte indicat pentru detectarea tentativelor de gaurire a seifurilor, ATM-urilor, camerelor blindate cu orice model de dispozitiv mecanic de gaurire.
Raza de acoperire este similara cu cea a detectoarelor de vibratii.

Fig. 12 Detector seismic perimetrala

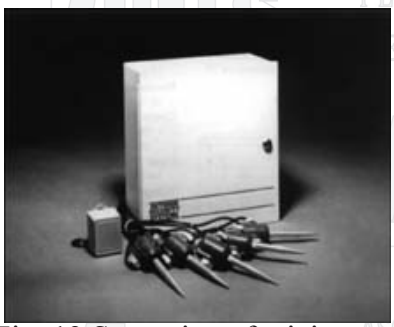


Fig .13 Senzori geofonici pentru protectie

Aceste tipuri de detectoare pot fi instalate cu succes in zone zgomotoase, in special in cazul in care trebuie protejati pereti exteriori aflati in zone cu trafic greu.

g. Detectoare dubla tehnologie

Necesitatea crestierii imunitatii la alarme false a dus la aparitia unor dispozitive de detectie ce incorporeaza de fapt doua module independente ce utilizeaza tehnologii de detectie diferite, cum ar fi:

- Detectorul dual PIR + MW
- Detectorul dual PIR + Geam spart
- Detectorul dual PIR + Ultrasonic

Unele dispozitive permit configurarea contactului de alarma atit in logica SI cit si in logica SAU, ceea ce permite, in functie de necesitati, maximizarea sensibilitatii senzorului sau a imunitatii la zgomot a acestuia.

De exemplu, utilizind in logica SI un detector dual PIR + MW dispunem de toate avantajele cumulate ale celor doua tehnologii in optinerea unui senzor cu o rata redusa a alarmelor false deoarece in cazul sectiunii PIR zona de detectie este bine delimitata de elementele constructive ale incaperii iar partea de MW asigura imunitatea la curenti de aer.

Ca aplicatie, detectorul ultrasonic este utilizat in special in alarmele auto, deoarece poate functiona intr-o gama extinsa de temperatura. Este un detector activ, ce functioneaza pe principiul detectie modulatiei de amplitudine a semnalului receptionat (ecou) in cazul in care in aria protejata exista corpuri in miscare.

Ca aplicatie de securitate in conjunctie cu un detector PIR se poate utiliza in spatii in care se desfasoara in mod curent activitate (hipermarket-uri, cladiri de birouri, spatii industriale) si mai putin ca aplicatie rezidentiala.

Fig. 14 Senzor dual PIR + MW

Fig. 15 Detector dual PIR + Ultrasonic

h. Detectoare antimasking

Detectoarele anti-masking sunt detectoare speciale, de regula cu dubla tehnologie, cae sesizeaza obturarea zonei supravegheate cu un obiect plasat in proximitatea senzorului, si care semnalizeaza obturarea utilizind un contact separat.

Aceste detectoare se utilizeaza in aplicatii de inalta securitate, atit pentru rata redusa de alarme false cit si pentru siguranta in exploatare oferita de functia anti-mascare.

In fig. 16 sunt detaliate citeva tipuri de caracteristici de acoperire pentru senzori duali antimasking:

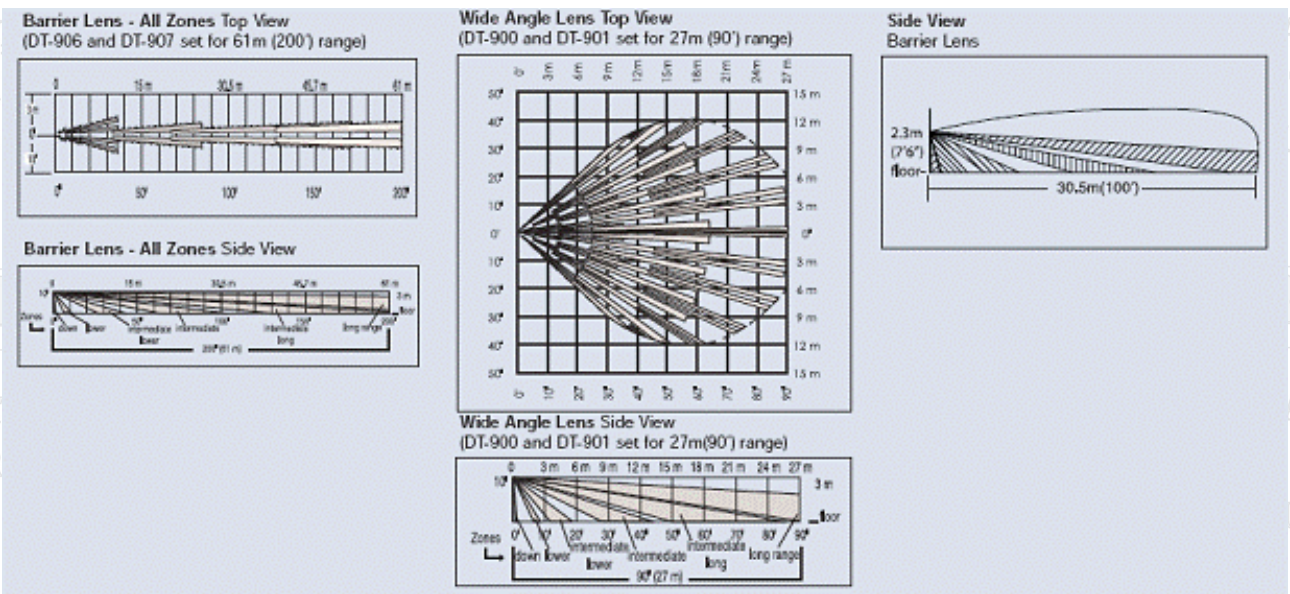


Fig. 16 Caracteristici de acoperire pentru senzori duali AM

i Senzori in linia de vizibilitate

Acesti tip de senzori pot fi utilizati cu suscces in cazul in care terenul este plat ceea ce nu permite aparitia unor zone mascate. Exista doua tehnologii: IR sau microunde. Tehnologia IR poate fi atit activa cit si pasiva, bariere si senzori. Tehnologia MW este activa, exista si bariere si senzori.

Bariere IR. Barierele IR sunt o solutie de detectie relativ scazuta ca pret. Barierele pot fi atit de interior cit si de exterior. Detectia se face in linia de vizibilitate. Bariera contine un ansamblu de emitatoare si receptoare de semnal modulat pentru a nu putea fi usor sabotate.

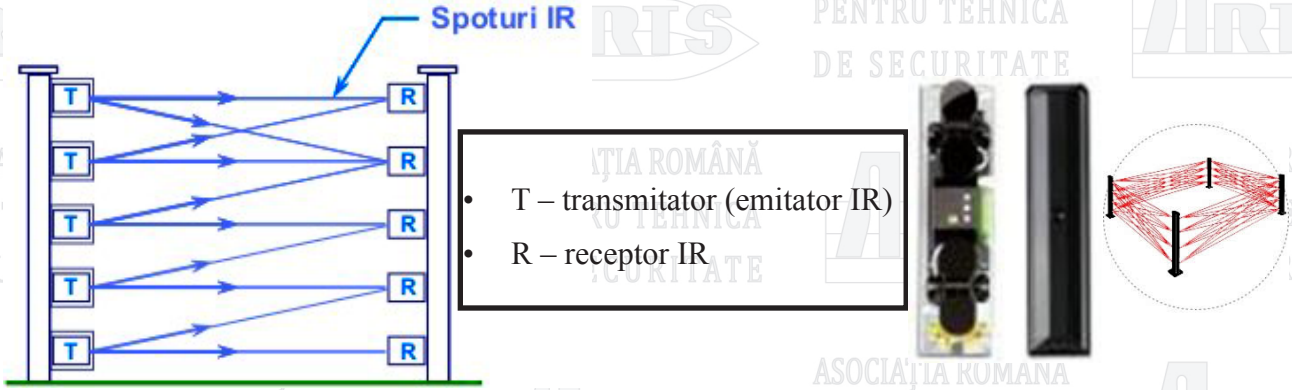


Fig. 17. Sistem de bariere active cu IR

Zona protejata este cea de viziblitate intre emitator si receptor. Barierele IR se gasesc in multe variante constructive, de la 1 la 8 spoturi, numarul ridicat de spoturi fiind necesar pentru cresterea inaltimii de detectie a barierei. Spoturile pot fi paralele sau incrucisate.
Principala caracteristica a unei bariere IR este distanta de detectie. Pentru aplicatiile de exterior, distanta maxima trebuie redusa la jumatate fata de datele de catalog.
O deosebita atentie trebuie acordata alimentarii, unele dispozitiva avind un element de incalzire intern, care creste mult consumul barierei in conditii de temperatura scazuta.
Barierele IR necesita o atentie deosebita la aliniere. Alinierea se face urmarind maximizarea nivelului semnalului receptionat cu ajutorul unui instrument de masura.
Amplasarea barierelor este extrem de importanta. La exterior treabuie avuta in vedere eliminarea si controlul permanent al vegetatiei pentru a nu genera alarme false. De asemenea, in cazuri extreme de mediu (ploaie, ceata, ninsoare) functionarea barierelor va fi temporar intrerupta.

Barierele cu microunde sunt mai sigure decit barierele IR datorita principiului de functionare. Semnalul in cazul microundelor ajunge la receptor pe mai multe cai, direct sau prin reflexie, ceea ce face ca forma zonei de detectie sa fie un elipsoid de rotatie.

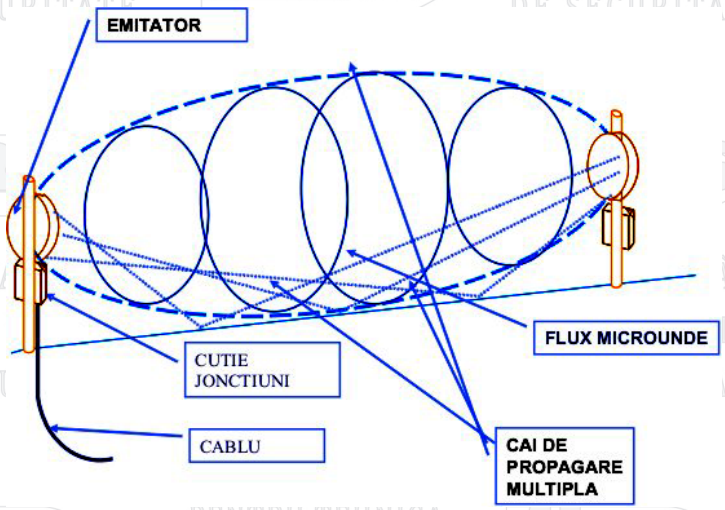


Fig. 18. Bariera MW

i. Tehnologii de protectie a gardurilor

Protectia gardurilor se poate realiza cu:

- Senzori discreti de vibratii
- Cablu electic senzitiv
- Fibra optica
- Sisteme “taut wire”
- Sisteme de detectie in camp electrostatic.
- Sisteme de detectie cu localizare cu puls RF

Senzorii discreti de vibratii pot fi de tip geofonici, sensibili la vibratiile mecanice. Lungimea zonei se seteaza din modul de grupare al detectoarelor pe intrari.

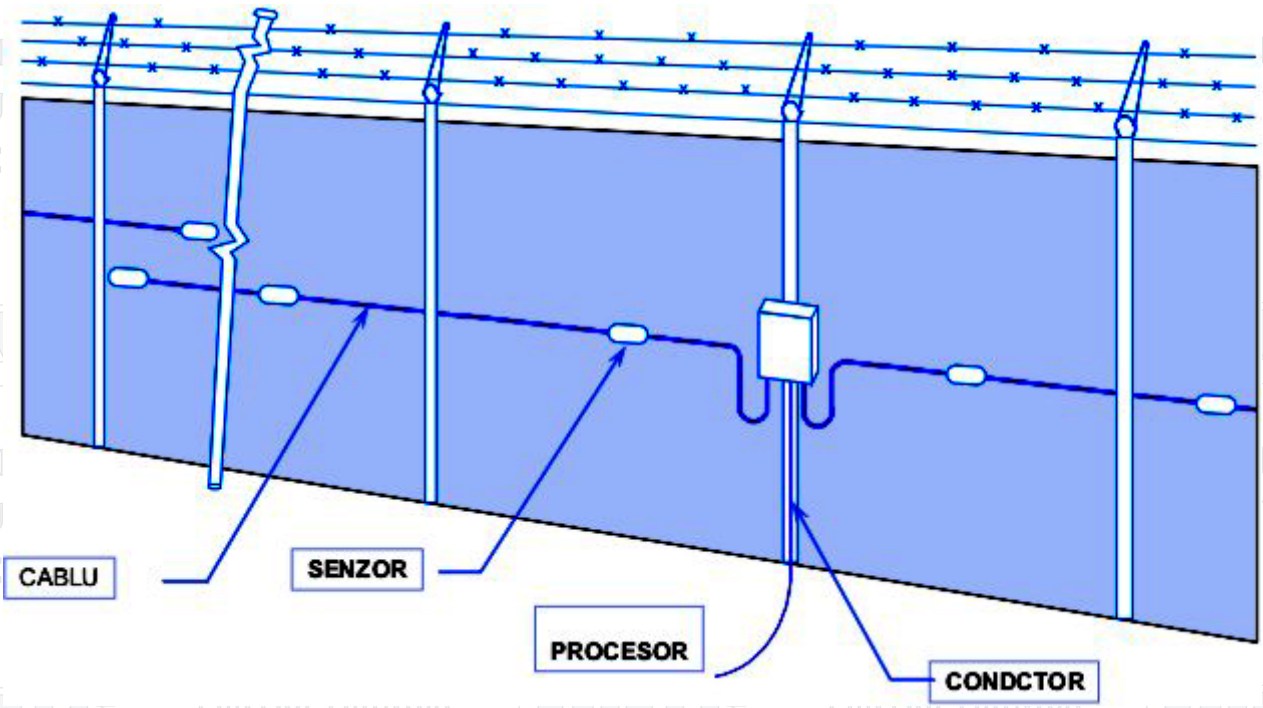


Fig. 19 Amplasarea senzorilor de vibratii mecanice

Cablul senzitiv este un traductor care transforma vibratiile in semnal electromagnetic.
Este utilizat pentru protejarea gardurilor la tentativa de escaladare si presupune contact fizic intre infractor si gardul protejat. Pentru cresterea sensibilitatii este recomandabila montarea in forma de S a cablului senzitiv.

Fig. 20. Cablu senzitiv amplasat pe gard

Fig. 21. Amplasarea in forma de S (serpuita)
pentru cresterea sensibilitatii de detectie.

Fibra optica poate fi de asemenea folosita pentru detectia vibratiilor unui gard. Detectia se realizeaza prin schimbarea modului de propagare al luminii transmise pe fibra optica. Acest sistem poate acoperi distante de pina la 2000m si necesita procesare la ambele capete ale cablului.

Fig. 22 Gard protejat cu fibra optica.

SISTEMELE “taut wire” (sirma tensionata, intinsa): se bazeaza pe modificarea echilibrului unei sirme intinse de resorturi. Firele de sirma mentin senzorii in echilibru, escaladarea unui gard protejat cu un asemenea sistem modifica echilibrul si genereaza alarma.
Lungimea zonelor este data de amplasarea senzorilor. Acestia pot fi simple contacte sau senzori piezo.

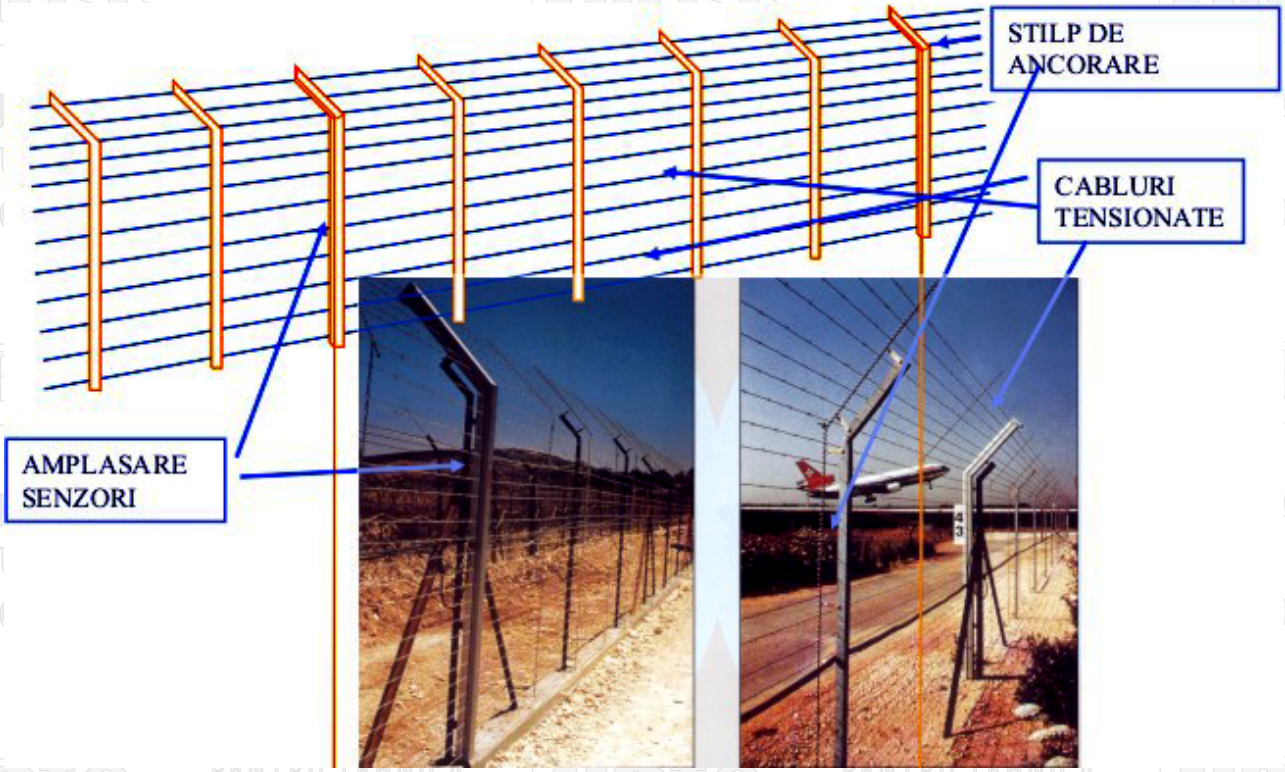


Fig. 23. Amplasarea sistemului "taut wire"

Sistemul taut wire prezinta avantajul imunitatii relativ mari la factorii de mediu perturbatori, inclusiv curenti puternici de aer.

Sistemele de detectie in camp electrostatic sesizeaza prezenta unui intrus in zona supravegheata. Este un sistem de detectie de tip capacitiv, zonarea se face pe tronsoane.

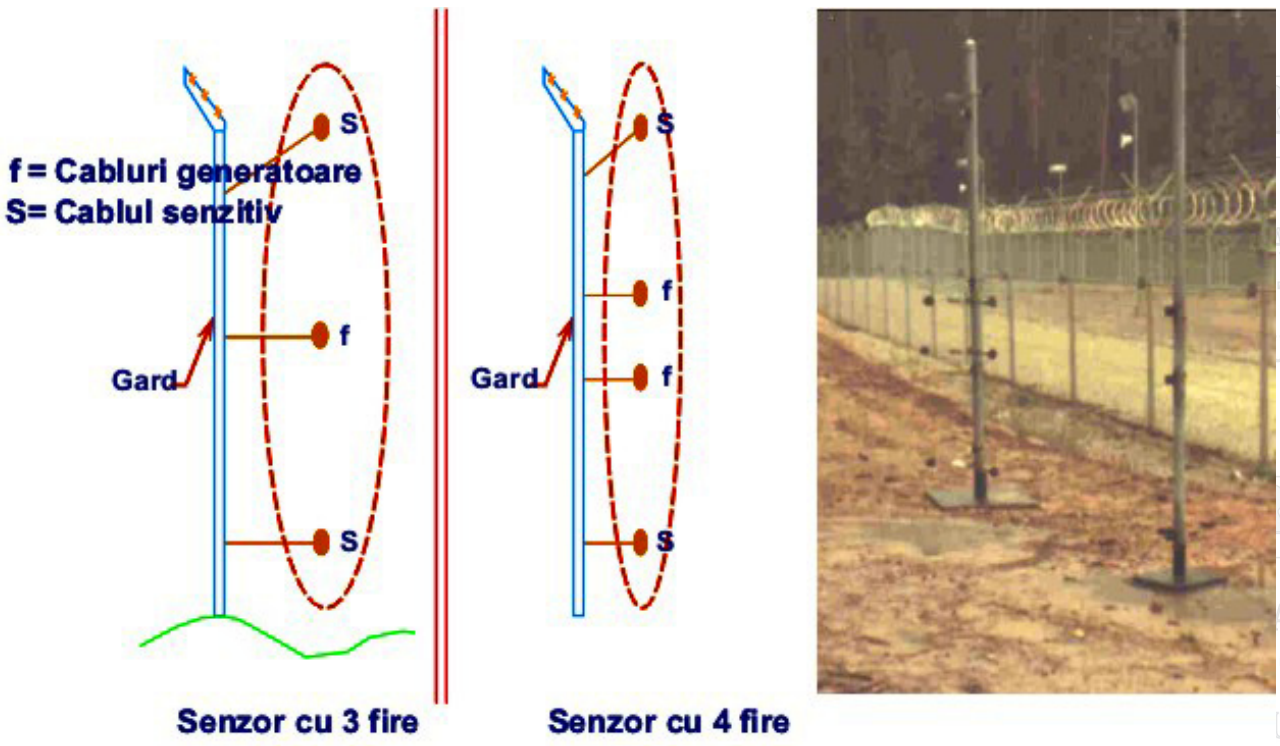


Fig. 24. Modalitatea de amplasare a unui sistem de detectie in camp electrostatic.

Sistemele de detectie a vibratiei cu localizare utilizind un puls RF sunt printre cele mai performante sisteme de protectie perimetrale, datorita urmatoarelor avantaje:

a. precizia de detectie este foarte ridicata (3m).

b. zonele se seteaza software, oriunde pe cablul de detectie.

c. toate semnalele se transmit pe acelasi cablu: semnalul de detectie, comunicatia si alimentarea.

d. zonele se pot omite software sau pe baza unui program orar.

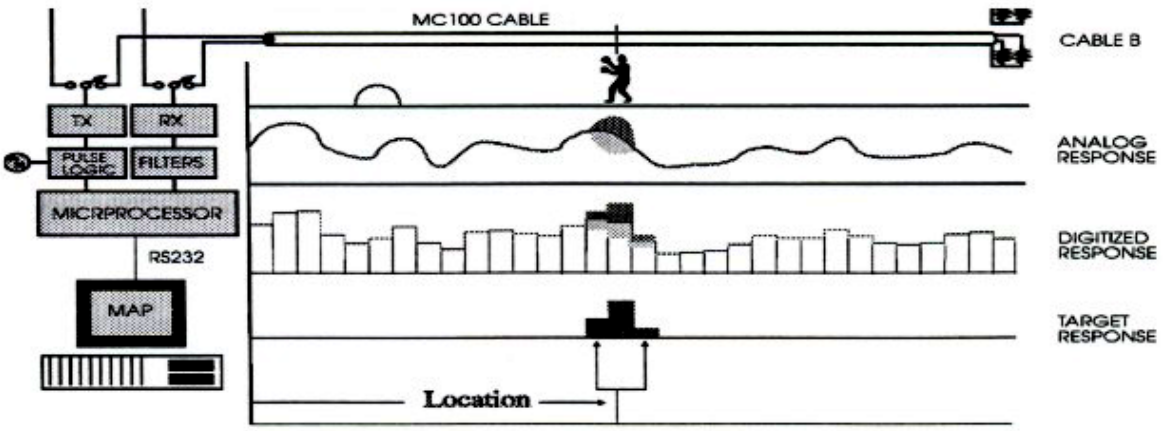


Fig. 25 Sistem de protectie perimetrala
ce utilizeaza un puls RF.

***Tema nr 5**: Arhitectura unui sistem. Concepte si terminologie. Comunicatia intre componentele sistemului si centrala.*

Elementele constitutive ale unui sistem de securitate sunt: senzorii, centrala, echipamentele periferice ale centralei, dispozitivele de avertizare locala si dispozitivele de comunicare la distanta.

Senzorii sunt dispozitive ce preiau o informatie de tip stare de alarma.

Centrala este o unitate de automatizare ce proceseaza informatiile preluate de la senzori in functie de starea sistemului (activat, dezactivat etc). Rolul principal al oricarei centrale de efractie este de a semnaliza (optic, acustic si/sau la distanta) detectarea unei intruziuni in spatiul protejat.
Centrala este un automat programabil: starea iesirilor depinde de starea intrarilor + starea sistemului. Iesirile pot fi comenzi pentru dispozitivele de semnalizare locala, porturi de comunicatie sau iesiri pentru interconectarea cu alte dispozitive.

Echipamentele periferice ale centralei sunt modulele de expandare si interfetele de comanda.
Modulele de expandare au rolul de a extinde numarul de intrari si/sau de iesiri ale centralei pentru configurarea unor sisteme de capacitate sporita.
Interfetele de comanda (MMI – men machine interface), numite in literatura de specialitate interfete om-masina au rolul de a permite utilizatorilor sa comande diferite functiuni ale sistemului. Aceste interfete pot
fi contacte cu cheie speciala de securitate, tastaturi sau cititoare de tag-uri de acces, cititoare biometrice etc.

Dispozitivele de de avertizare locala pot fi optice, acustice sau opto-acustice (mixte). Rolul acestor dispozitive este de a semnaliza o stare de alarma.

Dispozitivele de avertizare la distanta sint comunicatoare care utilizeaza diferite canale de comunicatie pentru a semnaliza o alarma la un dispecerat de monitorizare si interventie. Multe din echipamentele existente pe piata includ in centrala un port de comunicatie, de regula pe linie telefonca. Un alt tip de suport poate fi cel radio sau, mai nou, un port TCP/IP pentru transmisia pe suport internet.

Terminologie de specialitate.

a). Conceptul de **zona**.
Conceptul de zona prezinta doua semnificatii distincte: din punct de vedere electric si d.p.d.v al arhitecturii sistemului de securitate.
Din punct de vedere electric, zona reprezinta o intrare a centralei de alarma semnalata ca entitate pe dispozitivele de afisare.
Din punc de vedere sistemic, zona reprezina un spatiu bine delimitat care este protejat impotriva efractiei.
Comportamentul sistemului in cazul detectarii pe o zona (intrare) a unui semnal de alarma este diferit, functie de tipul logic al zonei. Centralele existente pe piata au fie tipuri de zona predefinite fie permit configurarea de catre programator a comportamentului sistemului in functie de necesitati. Citeva tipuri de zone sunt foarte uzuale in sistemele de securitate:

- Zona instantanee – este o zona care declanseaza instantaneu o alarma. Zonele de 24 de ore declanseaza alarma indiferent de faptul ca partitia din care fac parte este activata sau nu, in timp ce zonele de 12 ore genereaza alarma numai in cazul in care partitia ce le contine este armata.

- Zona temporizata – este o zona a carei activare genereaza o temporizare interna a sistemului dupa care, in cazul in care acesta nu este dezactivat, declanseaza automat o alarma. Din zonele temporizate fac parte zonele de intrare/iesire (Entry/Exit zone) care declanseaza temporizarea si zonele de urmarire (EE Follower) care pastreaza temporizarea in cazul in care aceasta a fost initiata de o zona de intrare/iesire sau genereaza instantaneu o alarma daca zona este activata inainte de a se activa temporizarea de intrare de catre o zona de intrare/iesire. Aceste doua tipuri de zone temporizate se gasesc amplasate pe caile de acces catre MMI-urile sistemului.
- Zone de panica-atac sunt zone instantanee de 24 de ore. De regula in sistemele de securitate monitorizate, aceste zone declanseaza o alarma silentioasa.
- Zona de sabotaj / defectiune tehnica – sunt zone de 24 de ore utilizate pentru monitorizarea securitatii sistemului (contactele antisabotaj ale dispozitivului, zonele anti-masking etc).

b). Conceptul de **partitie** (**arie**). Partitia reprezinta o multime de zone care sunt activate si dezactivate simultan, de catre acelasi utilizator.
Evident, si conceptul de arie/partitie prezinta aceeasi dualitate ca si conceptul de zona: din punct de vedere electric o arie reprezinta o multime de zone fizice conectate electric la centrala (intrari) care sunt operate simultan de aceiasi utilizatori, iar din punct de vedere sistemic o partitie este o suprafata mai mare protejata de sistemul de securitate a carei functionare/utilizare are caracteristici comune pentru toate zonele.

c). **Coduri**
Codurile sunt “cheile” sistemului. Codurile permit identificare utilizatorului in sistem si efectuarea de catre acesta de functii cum ar fi:

- Activare/dezactivare partitii (functia de baza a sistemului de securitate)
- Omitere de zone. In anumite conditii este necesara omiterea (bypass) unei zone in mod exceptional.
- Recunoastere / resetare alarme.
- Programare coduri utilizatori – Programarea codurilor utilizatorilor este o operatiune ce trebuie executata de personalul care exploateaza sistemul de securitate.

Un sistem are mai multe tipuri de coduri, de exemplu:

Codul de instalator - are rolul de a permite accesul la functiile de programare ale sistemului. In majoritatea cazurilor, codul de instalator permite de asemenea analiza jurnalului de evenimente din memoria centralei.

Codul master – utilizator principal - activare, dezactivare, programare coduri, omitere zone etc…

Cod user (utilizator simplu) – armare, dezarmare, eventual omitere zone.

Cod constringere: este un tip special de cod user ce transmite la dispecerat un mesaj de constringere (atac) si este folosit in cazul in care utilizatorul este fortat de agresori sa dezactiveze sistemul de securitate.

Cod cu drepturi limitate (numai activare sistem) – codul persoanelor care fac mentenanta si trebuie sa activeze sistemul de securitate la terminarea activitatii.

2.2. Comunicatie

Un sistem de securitate are in general urmatoarea arhitectura:

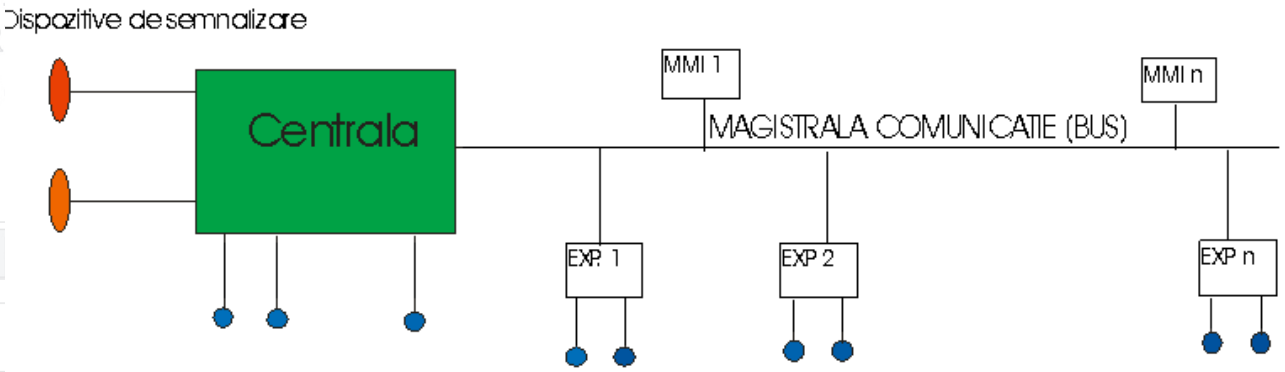


Fig. 26 Arhitectura unui sistem de secruritate

Exista mai multe tipuri de comunicatie in interiorul sistemului:

a. comunicatia intre senzori si centrala sau unitatile de expandare. Dupa cum am aratat, decizia referitoare la starea de alarma se ia la nivel de detector, ceea ce presupune o informatie pe 1 bit.

Exista urmatoarele tipuri de conexiuni a zonei:

- contact normal deschis (NO)
- contact normal inchis (NC)
- contact normal inchis cu rezistenta de cap de linie (EOL)
- contact normal inchis cu doua rezistente de cap de linie (DEOL)

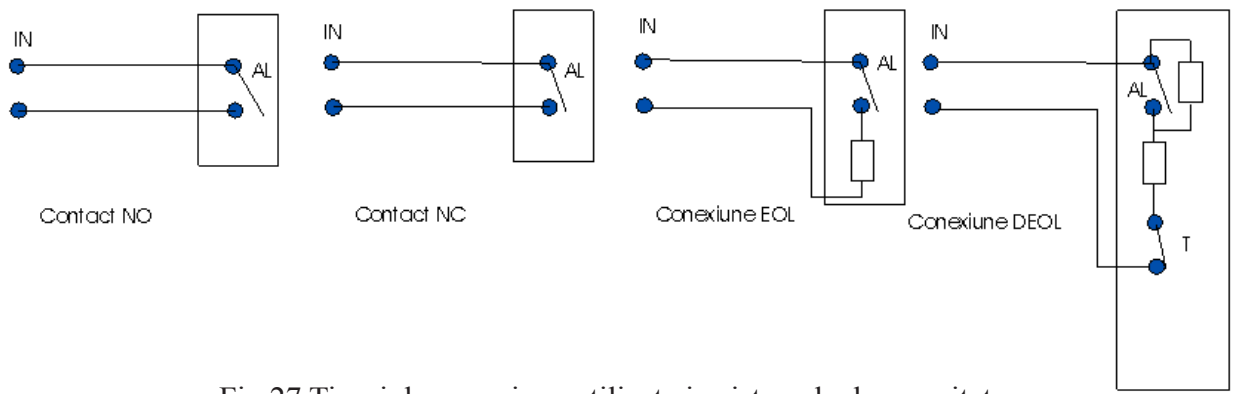


Fig 27 Tipuri de conexiune utilizate in sistemele de securitate

Din punct de vedere al securitatii conexiunii, in sistemele de securitate nu se utilizeaza contacte normal deschise intrucit acestea sunt cele mai usor de sabotat prin taierea unui singur conductor.

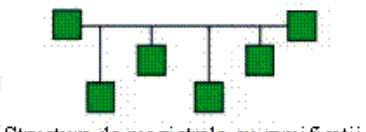
Pentru asigurarea unei securitati sporite antisabotaj se utilizeaza conexiunea cu rezistenta de cap de linie: **REZISTENTA SE MONTEAZA FIZIC IN SENZOR!!!**

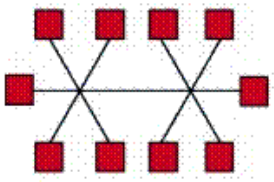
Pentru utilizarea ergonomica a intrarilor in centrala, se utilizeaza conexiunea cu doua rezistente de cap de linie. Aceasta conexiune permite monitorizarea simultana atit a cuntactului de alarma (AL) cit si a contactului antisabotaj (T = tamper) existent in carcasa senzorului.

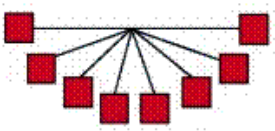
- Comunicatia intre centrala si expandoare sau MMI-uri este realizata prin intermediul unei magistrale de date (BUS). Aceasta comunicatie presupune transmiterea unei cantitati mai mare de informatie. Centrala interogheaza ciclic dispozitivele aflate pe magistrala (expandoare sau tastaturi) printr-un protocol de comunicatie seriala. Exista mai multe tipuri de comunicatie

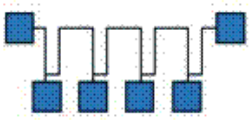
folosite in sistemele de securitate. Unele dintre ele nu prezinta solicitari speciale referitoare la arhitectura magistralei si permit conexiuni de tip STAR sau ramificate, altele prezinta anumite cerinte specifice. Un protocol extrem de utilizat, nu numai in cazul sistemelor de securitate dar si in cazul sistemelor de control al accesului si pentru actionarile si comenzile utilizate in sistemele CCTV este protocolul RS 485. Acest protocol de comunicatie seriala necesita:

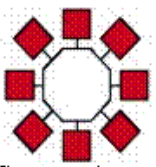
a. Utilizarea unui mediu de comunicatie uniform (cablu pentru comunicatie de date, cum ar fi o pereche torsadata din cablul UTP sau STP)
b. Arhitectura PIPE-LINE, in care dispozitivele sunt conectate pe BUS ca margelele pe ata; ramificatiile, conexiunile in stea nu sunt permise deoarece introduc dezadaptari pe canalul de comunicatie.
c. Terminatoare (adaptoare de impedanta) la capetele magistralei de comunicatie.


Structura de magistrala cu ramificatii


Structura de magistrala ramificat stelata


Structura de magistrala stelata


Structura de magistrala daisy chain (obligatorie pentru RS 485)


Structura de magistrala in bucla

Porturile de comunicatie externa.

Porturile de comunicatie externa sunt fie porturi seriale pentru comunicatie locala (RS232 max 30m, RS485 maxim 1200m fara repetor), fie portul telefonic pentru avertizarea la distanta pe linie telefonica, fie mai nou porturi TCP/IP utilizate in monitorizarea centralizata a unor sisteme distribuite utilizind retele LAN sau WAN.

Dispecerizarea sistemelor poate fi facuta utilizind oricare din porturile de comunicatie disponibile, in cazul in care exista un protocol comun intre echipamentul monitorizat si cel de monitorizare. Foarte utilizat in anii ‘90 este portul telefonic pentru care au fost dezvoltate o serie de protocoale de comunicatie, cum ar fi Contact ID ce permite transmiterea de mesaje complete de alarma ce includ: codul de abonat, partitia, zona si tipul de alarma.

Alta modalitate de dispecerizare este utilizarea de iesiri programate pentru anumite tipuri de alarma conectate la intrarile unui emitator radio dedicat pentru sisteme de securitate. Odata cu dezvoltarea retelelor GSM, comunicatorul radio clasic a fost inlocuit de comunicatorul GPRS.

***Tema nr 6**: Programarea sistemelor de securitate: principii de baza.*

Programarea sistemelor de securitate antiefractie este o procedura a carui nivel de dificultate depinde mai putin de marimea sistemului si mai mult de nivelul de complexitate a interdependentelor dintre subsisteme si automatizarile ce se doresc a fi implementate.

Programarea sistemului reprezinta selectarea acelor functiuni utile pentru o aplicatie specifica. Instalarea sistemelor de securitate este o activitate de productie in urma careia rezulta de cele mai multe ori “unicate” sau, in cel mai fericit caz, produse de serie mica. De aceea, fiecare sistem in parte va avea particularitatile sale in ceea ce priveste programarea.

Exista doua etape distincte in activitatea complexa de programare a unui sistem:

a. elaborarea procedurilor de functionare si utilizare
b. programarea propriu-zisa a sistemului

Elaborarea procedurilor de functionare presupune armonizarea intre informatiile cuprinse in proiectul tehnic de executie, solicitarile specifice ale beneficiarului si eventualele cerinte legale pentru obiectiv. Aceasta activitate se face, de regula, impreuna cu persoana desemnata de beneficiar sa receptioneze si sa supervizeze exploatarea sistemului de securitate. Aceasta este de regula o atributie a Managerului de securitate sau a Administratorului obiectivului daca functia de Manager de securitate nu exista in structura organizatiei.

Programatorul sistemului de securitate trebuie sa obtina informatiile specifice referitoare la modul de utilizare a spatiului (program de lucru) precum si la drepturile de accesare (utilizatori). In practica, adeseori programatorul se afla in situatia de a genera solutii referitoare la utilizarea sistemului pentru maximizarea rezultatelor in ceeea ce priveste asigurarea securitatii pe baza normelor in vigoare si a functiilor specifice asigurate de echipamentul utilizat. In cazul in care exista un plan de paza pentru obiectivul protejat, trebuie realizata corelarea procedurilor de operare a sistemului de securitate cu masurile prevazute in planul de paza.

Dintre informatiile specifice care trebuie sa rezulte in urma acestei analize se numara:

- timpii de intrare, iesire, durata semnalizarilor
- numarul de utilizatori si drepturile specifice ale fiecaruia.
- Eventualele modificari referitoare la partitionarea sistemului si la traseele principale de acces catre tastaturi. Daca sunt necesare astfel de modificari fata de proiectul avizat, acesta trebuie modificat si reavizat in consecinta. Modificarile pot fi avizate cu ocazia inspectiei obligatorii care se efectueaza la finalul lucrarilor.

Programarea propriu-zisa este etapa de introducere a parametrilor de programare in memoria centralei. Programatorul trebuie sa fie familiarizat cu functiile de programare specifice ale echipamentului utilizat, cu accesarea modului de programare a echipamentelor si cu tehnica de programare a fiecarei informatii in parte.

In timpul operatiunilor de programare, programatorul de sisteme de securitate va avea in vedere urmatoarele informatii ce trebuesc programate:

- Optiunile generale de functionare a centralei (daca este cazul), cum ar fi: afisarea orei, modul de semnalizare a anumitor evenimente (cum ar fi sabotajele) etc.
- Tipul de zona specific fiecarei intrari si descriptorii de zona. In cazul in care comportamentul unui anumit tip de zona este programabil, se vor programa intii tipurile de zona.
- Timpii de intrare, iesire, durata de actionare a iesirilor de alarma.
- Partitionarea (alocarea zonelor la partitii).
- Programarea utilizatorilor – doar partea de drepturi de utilizare (daca este cazul, functie de echipamentul utilizat) **EXCLUS PROGRAMAREA PROPRIU-ZISA A CODURILOR DE UTILIZATOR!!!**
- Programarea tastaturilor (alocarea acestora la partitii, functii specifice tastaturilor cum ar fi blocarea in cazul introducerii repetate de coduri false de acces etc.)
- Programarea iesirilor sistemului: iesirile utilizate pentru semnalizarile de alarma si celelalte iesiri utilizate ale sistemului.
- Programarea comunicatorului digital al centralei (daca este cazul). Aceasta sectiune de programare presupune utilizarea de date obtinute de la firma ce efectueaza monitorizarea sistemului cum ar fi: codul de abonat, numerele de telefon ale dispeceratului, prtocolul de comunicatie utilizat, codurile de alarma.

La finalizarea programarii se vor testa toate intrarile sistemului si toate functiile de alarma, inclusiv comunicatia cu dispeceratul de interventie.

Tema nr 7: *Testarea periodica si mentenanta.*

Functionarea corecta a sistemelor de securitate este asigurata prin testarea periodica a sistemului si prin procedurile de mentenanta preventiva.
Testarea periodica este recomandata a fi facuta la cel putin doua saptamani. Prin testare se verifica functionarea fiecarei zone a sistemului de securitate. Scopul testului este de a verifica functionarea completa a sistemului: armare, generare alarma, verificare comunicatie cu dispeceratul de interventie. Multe echipamente au incluse in meniul de utilizator o functie speciala de testare (walk test), prin care se poate verifica fiecare zona fara a fi necesara armarea sistemului si generarea de alarme. Aceasta functie se utilizeaza obligatoriu in conjunctie cu un test de alarma pentru a verifica atit semnalizarea locala cit si la dispecerat. Aceste teste sunt specifice utilizatorului si este necesar sa fie efectuate de catre acesta. Trebuie facuta distinctie intre testarea periodica si verificarea electrica a sistemului / mentenanta acestuia. Aceste din urma operatiuni sunt specifice echipei tehnice care a instalat sistemul de securitate. Operatiunile de mentenanta vor fi tratate in urmatorul modul.

Modulul VIII: Executia si mentenanta sistemelor de securitate antiefractie si protectie perimetrala

Tema nr 1 *- Caracteristicile sistemului instalat*

Prin caracteristicile sistemului instalat intelegem totalitatea functiilor de detectie si semnalizare precum si comenzile de la si spre sistemul de securitate. Aceste atribute se gasesc in proiectul tehnic de executie, dar modalitatea lor de implementare nu este specificata in proiect. Modul de programare precum si atributele de programare fiind specifice fiecarui producator, informatiile din proiectul tehnic trebuiesc interpretate de tehnicianul de sisteme de securitate relativ la specificatiile tehnice ale echipamentui instalat. De regula in proiectare se utilizeaza o terminologie standard (vezi tipul de zona intrare/iesire) in timp ce producatorii utilizeaza un limbaj personalizat, uneori numai din motive de marketing (se utilizeaza nu numai entry / exit zone ci si alte denumiri cum ar fi entry zone, door etc).
Atit pentru executie cit si pentru mentenanta, trebuie cunoscute urmatoarele detalii despre sistemul de securitate:

1. tipul de echipament utilizat, pe fiecare categorie: centrala, detectoare, sisteme de semnalizare, dispozitive de comunicatie etc.
2. Caracteristicile acestora si modul de instalare.
3. Modalitatea de realizare a cablarii si traseele de cablare.
4. Perioada de mentenanta precum si modalitatile/procedurile de asigurare a acesteia.

NOTA: Vor fi respectate cu strictete toate specificatiile producatorului referitoare la arhitecturile de magistrale, tipul de cablu si lungimile maxime de cablare. Alegerea traseului va fi facuta respectind normele de realizare a instalatiilor de curenti slabi. De asemenea, se vor respecta cu strictete specificatiile referitoare la realizarea alimentarii dispozitivelor. Astfel de detalii nu sunt prezentate in proiectul tehnic de executie si fac obiectul pregatirii lucrarii de catre inginerul de sisteme de securitate. Este de datoria acestuia sa specifice modalitatea de realizare a alimentarii sistemului, a regulilor de utilizare a cablului ecranat (daca este cazul etc).

Tema nr 2 *- Echipamentele de protectie*

In procesul de instalare este necesara respectarea normelor de protectie a muncii. Instalarea anumitor echipamente presupune lucru la inaltime, utilizind utilaje speciale (scari inalte, platforma, schela etc). Organizarea de santier presupune alocarea numarului de persoane necesar atit desfasurarii procesului de instalare cit si pentru asigurarea securitatii muncii.

Atunci cind nu exista planuri detaliate ale cladirilor si nu se cunosc trasele de alimentare cu energie electrica sau instalatii sanitare, perforarea peretilor trebuie efectuata doar dupa o analiza amanuntita a acestora. Exista dispozitive care identifica pozitia aproximativa a insertiilor metalice in pereti (utilizate pentru a descoperi traseele de dar nu este suficient, instalatiile sanitare moderne utilizeaza materiale plastice care nu pot fi detectate cu aceasta metoda.

Tema nr 3 *- Starea de functionare a sistemului*

Prin functionarea sistemului se intelege posibilitatea sistemului de a efectua integral toate functiile pentru care acesta a fost proiectat, in conditii de exploatare normale, precizate de catre instalator. Sistemul trebuie re-adus in stare de functionare mai intii la punerea in functiune si ulterior dupa aparitia oricarei defectiuni sau modificari aduse sistemului de securitate.
In cadrul procesului de punere in functiune (PIF), tehnicianul de sisteme de securitate va verifica daca fiecare dispozitiv este alimentat corect, daca functioneaza local si daca functionarea acestuia este receptionata corect la centrala de alarma. O categorie separata de probleme ce pot apare la punerea in functiune sunt problemele de comunicatie pe magistrala. Diagnoza problemelor de comunicatie este complexa si, pentru sisteme mari, trebuie executata sub coordonarea directa a unui inginer de sisteme de securitate.
Tehnicile de diagnoza sunt specifice fiecarui echipament. In general, la sistemele proiectate pina in prima jumatate a anilor 90 diagnoza se efectua prin operatiuni direct pe echipament, din aproape in aproape. Dupa aceasta data, atit programarea cit si operatiunile de testare au fost automatizate cu ajutorul calculatorului. In prezent, multe echipamente vin insotite de pachete software complexe de programare si testare, ceea ce permite diagnosticarea rapida a potentialelor probleme aparute la PIF.

Pentru fiecare familie de echipamente, tehnicienii si inginerii de sisteme de securitate trebuie sa urmeze programe de training dedicate, sustinute de distribuitorii de echipamente. Programul de training este specific competentelor ce se urmaresc a fi acumulate de cursanti (program dedicat instalarii, program de training specific programarii etc).

Tema nr 4 *- Mentenanta sistemului*

Mentenanta sistemului este reprezentata de totalitatea operatiunilor ce trebuiesc executate pentru a mentine un sistem de securitate in perfecta stare de functionare.
Specific sistemelor de securitate antiefractie, procedurile de mentenanta periodica includ:

a. curatarea detectoarelor
b. verificarea orientarii si fixarii acestora
c. testarea zonelor
d. verificarea incarcarii acumulatoarelor daca aceasta functie nu este realizata automat de sistemul de securitate
e. vizualizarea jurnalului de evenimente al centralei (in special pentru echipamentele la care accesul la jurnalul de evenimente este permis numai instalatorului
f. test de comunicatie cu dispeceratul de monitorizare si interventie (daca este cazul)

Singura solicitare legala legata direct de activitatea de mentenanta se refera la inlocuirea periodica a acumulatoarelor de back-up la un interval de 3 ani. Conform diagramelor oferite de producatori, acesta este intervalul de timp dupa care, pentru acumulatoarele cu plumb de tipul celor utilizate in sistemele de securitate, capacitatea acestora scade la 30% din capacitatea nominala.

Tema nr 5 *- Alimentarea cu energie electrica a sistemului*

O atentie deosebita trebuie acordata alimentarii cu energie electrica a sistemelor de securitate. Cele mai multe probleme de functionare a sistemelor de securitate sunt generate de probleme de alimentare, din care putem nominaliza:

a. lipsa pe o perioada mai indelungata a alimentarii cu energie electrica
b. supratensiuni aparute pe circuitul de alimentare iar in caz extrem deconectarea punctului de nul ceea ce duce la spuratensiuni de pina la 380 Vca.
c. Caderi repetate si reporniri bruste a retelei.

De multe ori aceste pulsuri de tensiune duc la blocarea unitatilor centrale (atit la efractie cit si la celelalte subsisteme). De aceea, pentru sistemele de securitate mari este recomandat ca alimentarea sa se faca prin UPS-uri pentru aplicatii profesionale care sa protejeze sistemul de securitate.
Pentru realizarea alimentarii o serie de reguli in plus fata de normele de realizare a instalatiilor de curenti tari trebuiesc respectate:
1. pentru alimentarea sistemelor de securitate se prevede un circuit electric separat
2. in cazul sistemelor complexe, alimentarea cu energie electrica se realizeaza dintr-o singura faza
3. in cazul sistemelor la care dispozitivele sunt amplasate pe distante mari si nu se poate realiza un sistem de alimentare unitar, dispozitivele vor trebui izolate din punct de vedere galvanic.
4. impamantarea ca si ecranarea cablurilor de semnal (daca se utilizeaza) se efectueaza arborescent, pornind dintr-un singur punct.

Tema nr 6 *- Setarile programelor de configurare a echipamentelor/ sistemelor tehnice de detectie, efractie si control acces*

Atunci cind echipamentele instalate sunt insotite de programe de configurare si monitorizare, acestea trebuiesc setate pentru a permite comunicatia cu echipamentul instalat. De regula, aceste setari sunt relativ simple:

a. daca configurarea se efectueaza de la distanta, va trebui setat modul de comunicare (linie telefonica utilizand de regula un modem dedicat sau adresa IP)
b. daca operatia de configurare se efectueaza local, atunci va trebui setat portul de comunicatie sau adresa de IP.

O problema apare deseori cind se utilizeaza echipamente care sunt construite pentru a fi programate pe port serial clasic deoarece toate computerele moderne nu mai au in constructie acest port. In aceasta situatie se instaleaza pe un anumit port USB o interfata USB - seriala si se configureaza portul COM aferent corespunzator specificatiilor programului de programare (de multe ori nu sunt acceptate decit COM 1-4). O data ce aceasta setare a fost efectuata, interfata USB nu trebuie introdusa in alt port USB ci numai in acel port in care ea a fost configurata.

Întocmit: Ing.Laurențiu Popescu

SISTEME DE MONITORIZARE A ECHIPAMENTELOR DE DETECȚIE A ALARMELOR

ing. Silviu Clep

Cuprins

Cap 1. Noțiuni introductive privind sistemele de monitorizare a alarmelor

Prin acest curs, autorul, dorește inițierea şi familiarizarea Tehnicianului specialist în sisteme de securitate cu noțiunile de bază ce stau la baza conceperii, funcționării, exploatării şi întreținerii unui sistem de monitorizare a alarmelor.

Teoria Sistemului de Management a Securității definește multidimensionalitatea conceptului de securitate (fizică, tehnologică, informațională, inteligent – umană), diversitatea amenințărilor interne şi externe asupra obiectivului protejat, dinamica riscurilor, a prevenției şi a acțiunii atât în timpul

producerii unor evenimente, cât şi pentru limitarea efectelor acestora după producere. Acest lucru determină conceperea şi realizarea unei structuri de securitate multifuncțională care să asigure integrarea funcțională a tuturor subsistemelor care o compun.

În principiu, un Sistem Integrat de Securitate (SIS) este compus din următoarele subsisteme:

- subsistemul de detecție şi alarmare perimetrală
- subsistemul de control acces
- subsistemul de televiziune cu circuit închis
- subsistemul de detecție şi alarmare la efracție
- subsistemul de detecție şi alarmare/stingere la incendii, inundații şi alte pericole
- subsistemul comunicații şi transmisii de date
- subsistemul dispecerat (de monitorizare)
- subsistemul electroalimentare

În subsistemul dispecerat (de monitorizare) se realizează:

- corelarea şi intercondiționarea automată a funcționării elementelor subsistemelor componente în scopul realizării funcțiilor sistemului integrat de securitate
- evaluarea gradului de amenințare în cazul unui atac extern
- punerea la dispoziția operatorilor a informațiilor complete privind situația creată
- precizarea contramăsurilor ce trebuie întreprinse de către operatori în fiecare situație
- alarmarea personalului şi a forțelor de intervenție fie automat, fie prin intermediul operatorilor, funcție de procedura prestabilită în fiecare situație;
- înregistrarea şi arhivarea datelor furnizate de subsistemele componente în vederea analizării ulterioare a acestora

Teoretic Subsistemul dispecerat poate asigura monitorizarea oricărui subsistem al Sistemului Integrat de Securitate, în realitate însă acest lucru este posibil doar pentru o monitorizare locală a subsistemelor SIS. Pentru monitorizarea la distanță apar probleme tehnice de comunicație şi procesare a informațiilor care limitează implementarea unui sistem funcțional pentru oricare din subsistemele SIS. Prezentul curs se wwreferă doar la monitorizarea echipamentelor de detecție a alarmelor la efracție şi incendiu, cu unele referiri şi la sistemele de control al accesului şi la sistemele de supraveghere video în măsura în care acestea funcționează intr-un sistem integrat cu sistemul de detecție si alarma la efracție sau şi cu sistemul de detecție şi alarmare la incendiu.

1.1. Definiții şi abrevieri

Uzual în practică se folosesc doi termeni **monitorizare** şi **dispecerizare.** Pentru a înțelege care este terminologia corectă ce trebuie utilizată din punct de vedere tehnic, dar şi lexical, vom apela la Dicționarul Explicativ al Limbii Române.

Monitorizare: - a supraveghea prin intermediul monitorului sau al altui aparat specializat

Monitor: - (inform) program de control care permite supravegherea mai multor programe fără legătură între ele, într-un ordinator; (tehn.) aparat care dirijează, coordonează sau supraveghează;…..

Dispecerizare: - acțiunea de control şi reglementare operativă şi permanentă a unui proces

Dispecerat: - încăpere în care funcționează serviciul de dispeceri

Dispecer: - tehnician sau sistem automat care urmăreşte, coordonează şi reglementează operativ mersul producției dintr-o întreprindere, care supraveghează mişcarea trenurilor pe o anumită porțiune a liniei etc

Din punctul de vedere al legislației românești Legea 333/2003 şi HG 1010/2004 utilizează termenul de **Dispecerate de Monitorizare,** cu observația că se referă doar la monitorizarea sistemelor de alarmă la efracție.

În cele ce urmează vom definii termeni specifici sistemelor de monitorizare:

Acces: Acțiunea de intrare sau ieşire dintr-o suprafață securizată.
Condiția de alarmă: Funcția unui sistem de alarmă sau parte din el, de a reacționa în prezența unui pericol.
Centrul de monitorizare şi recepționare al alarmei (CMRA): un centru continuu către care informația privind situația unuia sau mai multor sisteme de alarmă, este raportat.
Sistemul de alarmă: o instalație electrică care răspunde unui detector manual sau automat la prezența unei situații de risc.
Echipament de transmisie alarme: Echipament care este folosit în mod special pentru transmiterea mesajelor de alarma de la sistemul de alarma, către MARC.
Sistemul de transmitere alarme: echipamentul şi rețeaua folosite pentru a transfera informații cu privire la starea unui sistem de alarmă sau a mai multor sisteme către unul sau mai multe dispecerate.
Autentificare: schimbarea unui cod ptr. a identifica faptul că premisele supravegheate ale emițător-receptorului nu au fost substituite de un echipament similar fără acest cod, sau că informația mesajului transmis nu a fost modificată.
Criptare: codarea, traducerea sau altă modificare a informației prin care metoda în care este modificată informația variază în funcție de timp într-o manieră pseudo-haotică.
Mesaj: serii de semnale parcurse de o rețea care include identificarea, funcția şi diferite înțelesuri pentru furnizarea propriei integrități, imunități şi recepții potrivite.
Formatele mesajului: definițiile cuprinsului detaliat al tipurilor individuale de mesaje (cu structura completă a unui mesaj) care au un înțeles specific.

1.2. Structura unui sistem de monitorizare

În figura 1 este prezentată schema bloc a unui sistem de monitorizare.

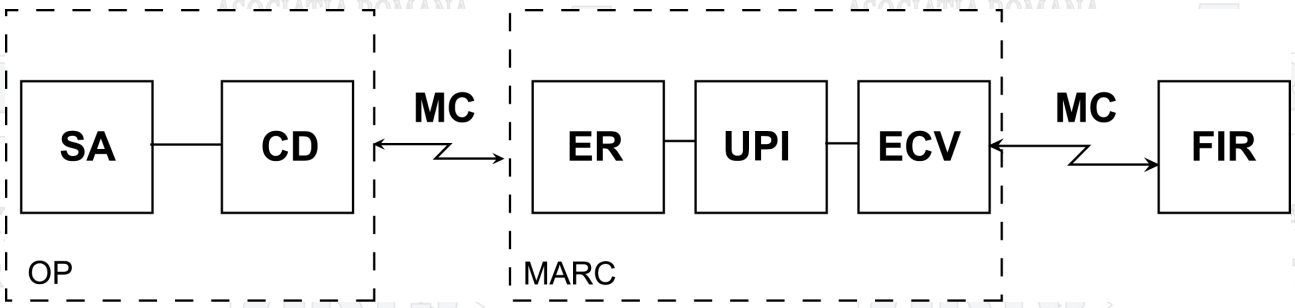


Fig.1 Schema bloc sistem monitorizare

Unde:
OP – obiectiv protejat
SA – sistem de alarma instalat la obiectivul protejat
CD – comunicator digital, care poate fii interior sau exterior sistemului de alarmă
MC – mediu de comunicare
MARC – Centrul de monitorizare şi recepție a alarmelor (CMRA)
ER – echipament de recepție
UPI – unitate de procesare a informației
ECV – echipament comunicare vocală
FIR – forță de intervenție rapidă

1.3. Timpul de răspuns al echipelor de intervenție

Eficiența unui sistem de monitorizare a unui sistem de securitate depinde de modul cum este conceput acesta și de respectarea cu strictețe a scenariului de securitate inițial. Încă din faza de proiectare a unui sistem de securitate trebuie luat în calcul dacă respectivul sistem urmează a fii monitorizat local sau la distanță, și care dintre subsistemele sistemului integrat urmează a fii monitorizate.
Din analiza de risc care se face asupra obiectivului, proiectantul poate concepe sistem integrat de securitate astfel încât el să poată fii monitorizat. Analiza de risc poate să evidențieze situații în care nu este nevoie de o monitorizare ulterioară a sistemului, în acest caz proiectantul concepând structura sistemului astfel încât acesta să ofere nivelul de securitate cerut și să asigure informații despre sistem și o alarmare locală.
Dacă în schimb analiza de risc impune pentru asigurarea unui nivel de securitate ridicat, monitorizare sistemelor de securitate, atunci proiectantul trebuie să gândească sistemele de așa manieră încât pe de o parte acestea să ofere posibilitatea tehnică a monitorizării, iar pe de altă parte să ofere CMRA informații utile și rapide despre evenimentele petrecute la obiectivul protejat.
Dacă într-un sistem de securitate nu este prevăzută și o forță sau o acțiune de răspuns, de intervenție în cazul declanșării unei alarme reale, pentru a opri sau limita efectele cauzei care a provocat-o înainte ca aceasta să-și atingă țelul propus, acel sistem se poate considera incomplet, oprindu-se în funcționalitatea lui numai la nivelul semnalizării.
Pentru ca acțiunea forței de intervenție rapidă să fie eficientă este foarte important ca timpul scurs de la declanșarea unei alarme reale până la momentul intervenției trebuie să fie cât mai mic
Pentru a exemplifica considerăm un obiectiv protejat cu sistem de alarmare și detecție a efracției, care este supus unei efracții.
Cu cât este mai scurt timpul scurs de la declanșarea alarmei până la sosirea echipei de intervenție la locul producerii acesteia sau la locul indicat de operator în baza urmăririi răufăcătorului cu mijloacele tehnice din cadrul sistemului de securitate, cu atât crește probabilitatea ca acțiunea echipei să fie încununată de succes.
Diagrama de timp cuprinzând corelația dintre timpul necesar infractorului pentru a-și atinge ținta și timpul de acțiune al sistemului de securitate este prezentată în Fig. 2

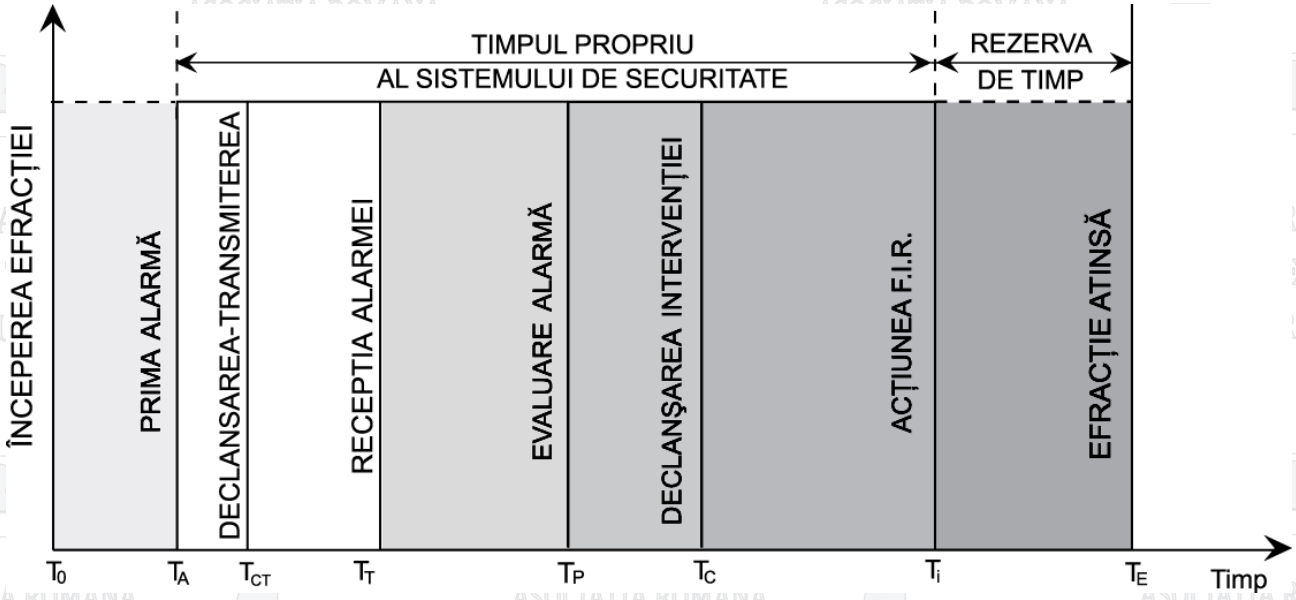


Fig. 2 Timpii desfășurării acțiunilor și contracțiunilor unei efracții

$\mathbf{T_0}$ – timpul la care infractorul își începe acțiunea efracția
$\mathbf{T_A}$ – timpul primei alarme. Acest interval de timp ($T_0 - T_A$) este unul dependent de tehnologia aparaturii folosite pentru detecția tentativei de efracție, dar și de structura sistemului de securitate implementat.

$\mathbf{T_{CT}}$ – timpul de comandă transmitere a alarmei. Acest interval de timp ($T_A – T_{CT}$) este unul dependent de algoritmii folosiți în programarea sistemului de alarma pentru discriminarea alarmelor false

$\mathbf{T_T}$ – timpul de transmisie a alarmei. Este durata de transmisie a mesajului de alarmă, din momentul în care alarma a fost semnalizată de către echipamentul de emisie al centralei de alarmă către echipamentul de recepție central.

$\mathbf{T_P}$ – timpul de procesare a alarmei. Este timpul necesar procesării informației recepționate de echipamentul de emisie recepție a dispeceratului şi luarea deciziei de către dispecer de declanşare a F.I.R.

$\mathbf{T_C}$ – timpul de comunicare. Este timpul necesar transmisiei informațiilor despre alarma către echipajul de intervenție

$\mathbf{T_I}$ – timpul de intervenție este timpul de acțiune al echipei de intervenție pentru oprirea acțiunii şi anihilarea răufăcătorului.

$\mathbf{T_E}$ – timpul de efracție este timpul necesar infractorului pentru a duce la sfârşit acțiunea sa

Calculul acestor timpi trebuie efectuat încă din faza de proiectare a sistemului de securitate şi reluat, eventual corectat, în fazele de simulare şi evaluare a eficienței acestuia.

Astfel timpul de efracție $\mathbf{T_E}$ trebuie mărit din faza proiectării construcției prin utilizarea unor materiale de construcție rezistente la şocuri mecanice, pentru uşi şi ferestre trebuie luate în calcul măsuri de securizare adecvate, de asemenea în scenariul de securitate se pot prevedea diferite bariere de natură a întârzia producerea efracției.

Aceeaşi diagramă este aplicabilă şi în cazul unui incendiu, cu singura deosebire că rezultatul acțiunii distructive asupra obiectivului protejat este focul, iar forța de intervenție rapidă este reprezentată de acțiunea trupelor de pompieri.

1.4. Optimizare sistemului de securitate monitorizat în faza de proiectare

După cum arătam, analiza de risc făcută asupra unui obiectiv poate recomanda monitorizarea sistemului de securitate pentru reducerea riscurilor producerii unui eveniment nedorit şi asigurarea unui nivel de protecție ridicat.

Prin proiectul de arhitectură, dacă se ține cont de analiza de risc, se pot alege soluții constructive şi materiale adecvate care să diminueze riscurile producerii unei efracții sau a unui incendiu. Proiectul de arhitectură poate reduce timpul de efracție - $\mathbf{T_E}$ sau timpul de foc - $\mathbf{T_F}$ în cazul unui incendiu, dar în nici un caz nu poate reduce major riscul producerii unui eveniment nedorit, acest lucru se realizează în primul rând prin implementarea unui sistem de securitate adecvat importanței destinației obiectivului şi riscurilor la care acesta este supus.

Prin proiectarea corectă a sistemului de securitate Timpul propriu al sistemului de securitate - TPS se poate reduce semnificativ, făcând posibilă mărirea rezervei de timp între acțiunea FIR producerea efracției sau consumarea incendiului.

În cele ce urmează voi încerca să arăt cum poate fi optimizat un sistem de securitate monitorizat astfel încât să ducă la reducerea TPS.

Pentru exemplificare vom folosi planul obiectivului din Fig. 3, considerând necesitatea implementării unui sistem de alarmă antiefracție şi a unui sistem de detecție şi avertizare în caz de incendiu.

Cel mai important obiectiv al unui sistem de securitate este acela de a face posibil ca intervalul ($T_0 – T_A$) să tindă spre zero. În cazul sistemelor de alarmă contra efracției acest lucru este posibil dacă tentativa de efracție este detectată la momentul producerii ei, la nivelul perimetrului obiectivului. Folosirea detectoarelor de spargere de geam, a detectoarelor de vibrații şi/sau şoc, a barierelor infraroşii instalate la nivelul ferestrelor şi uşilor etc., duc la detecția infractorului în afara spațiului protejat. În cazul sistemelor de detecție şi avertizare la incendiu acest lucru se poate realiza în principal prin alegerea corectă a tipului de detector folosit în concordanță cu modul de exprimare a materialelor combustibile din suprafețele de acțiune, şi de asemenea utilizarea unor detectoare cu timp mic de răspuns duc la reducerea timpului primei alarme - T_A

O altă cerință a unui sistemului de securitate monitorizat este aceea de a avea toate spațiile și încăperile supravegheate. Neîndeplinirea acestei cerințe neglijate de mulți proiectanți, pentru reducerea costurilor de implementare, duce la diminuarea pe de o parte a eficienței sistemului de alarmă propriu zis, dar în principal duce la creşterea timpului de procesare - $\mathbf{T_p}$

Foarte important în eficiența unui sistem de securitate monitorizat este reducerea timpului de transmisie - $\mathbf{T_T}$. Acest lucru se realizează în principal prin utilizarea unei comunicator digital care să suporte formate de comunicare rapide și utilizarea unui mediu de comunicare performant. De asemenea și echipamentul de recepție montat la MARC, capacitatea și performanțele lui, pot influența direct acest timp.

Cel mai greu de optimizat este timpul de intervenție – $\mathbf{T_I}$ - în primul rând datorită condițiilor de trafic și al restricțiilor urbane. Totuși și acest timp poate fii redus în baza unor simulări adecvate și prin costuri materiale ridicate.

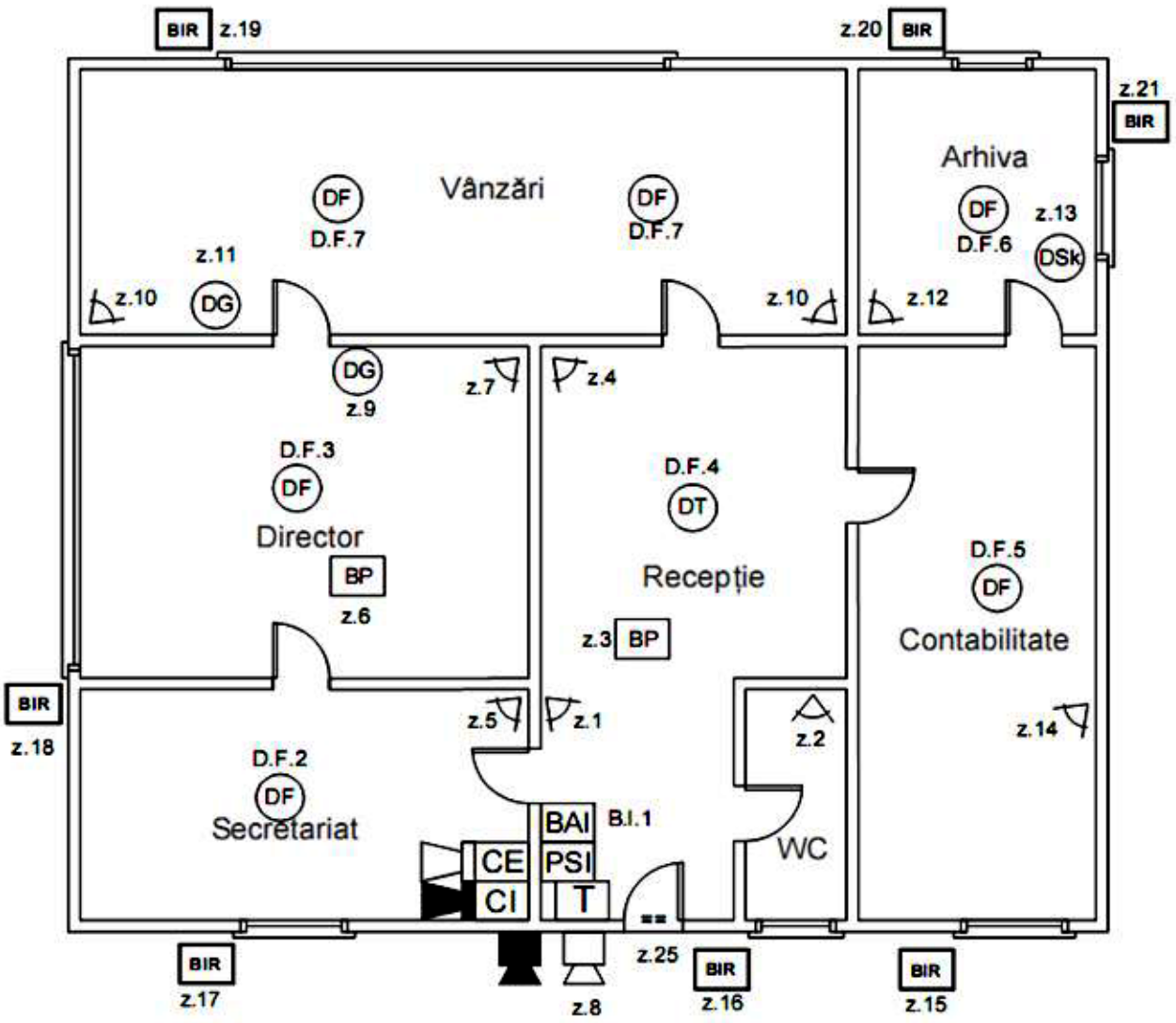


Fig. 3 Studiu de caz

Legenda:

Cap. 2 Semnale procesate şi transmise la CMRA de către sistemele de alarmă

Scopul unei alarme este întotdeauna acela de a iniția o reacție, pe plan local sau de la distanță. Modul de funcționare a alarmei are, în unele cazuri, un rol dublu: să prevină ceva ce ar putea să apară, de exemplu, intrarea prin efracție, şi să reacționeze în cazul în care ceva se întâmplă. În majoritatea cazurilor, sistemele de alarmă cuprind echipamentul de detecție al evenimentelor posibile, echipamentul de transmisie a alarmei, un centru de monitorizare şi forțele de reacție: poliție, jandarmi, pompieri, asistență medicală etc.

Caracteristicile pentru fiecare dintre aceste componente din întregul sistem de prevenire şi răspuns trebuie să corespundă tipului de amenințare împotriva căreia asigură protecția:

Pentru sisteme antiefracție, protecție în caz de sabotaj sau transport, caracteristicile importante sunt: nivelul gradului de risc, şi cel mai important, disponibilitatea sistemului.

Pentru un sisteme de alarmă la incendiu cele mai importante caracteristici pot fi timpul de transmisie şi disponibilitatea, desigur raportate la gradul de risc.

Pentru o intervenție corespunzătoare, trebuie oferite suficiente informații prin sistemul de transmisie a alarmei. Semnale transmise de centralele de alarmă sunt:

- Semnalizări de stare
- Alarme la efracție şi hold-up
- Alarme la incendiu
- Alarme sociale
- Alarme medicale
- Alarme de control al accesului
- Semnalizări tehnice
- Semnalizări auxiliare

2.1. Semnalizări de stare

Aceste tipuri de mesaje aduc operatorului CMRA informații despre starea principalelor funcții ale sistemului de alarmă:

- starea armată sau dezarmată a sistemului
- alimentare AC
- alimentare CC
- ceasul intern al sistemului
- baypas-are zone
- memorie de evenimente
- partiții

2.2. Alarme la efracție şi hold-up

În această categorie de mesaje sunt incluse mesajele de panică şi efracție:

- alarmă zonă efracție
- restaurare zonă efracție
- panică
- restaurare panică
- alarmă sabotaj
- restaurare sabotaj
- constrângere
- restaurare constrângere

2.3. Alarme la incendiu

În această categorie de mesaje sunt incluse mesajele alarmă la incendiu

- alarmă fum
- restaurare fum
- alarmă termică
- restaurare termică
- alarmă inundație
- restaurare inundație
- alarmă manuală incendiu
- restaurare manuală incendiu
- alarmă flacără
- restaurare flacără
- alarmă gaz
- restaurare gaz

2.4. Alarme de control al accesului

În această categorie de mesaje sunt incluse mesajele alarmă pentru acces

- armare/ dezarmare utilizator
- autoarmare sistem
- armare rapidă
- acces validat
- acces refuzat
- armare cu baypas-are
- armare/dezarmare devreme
- armare/dezarmare târzie
- armare/dezarmare parțială

2.5. Semnalizări tehnice

În această categorie de mesaje sunt incluse mesajele referitoare la starea tehnică a sistemului:

- lipsă/restaurare AC
- lipsă/restaurare CC
- defect/restaurare zonă
- test periodic
- defect/restaurare periferice
- sabotaj cod utilizator
- lipsă ceas intern

- programare locală
- eroare comunicare
- lipsă/restaurare comunicație
- pierdere date

Cap. 3 Sisteme şi echipamente de transmisie şi recepție a mesajelor la CMRA

3.1. Cerințe ale sistemelor şi echipamentelor de transmisie şi recepție

Una dintre componentele sistemului de securitate având o importanță foarte mare în eficiența unui sistem monitorizat este comunicatorul digital – CD, vezi fig. 1.Caracteristica acestei componente determină pe de o parte valoarea timpului de transmisie - $\mathbf{T_t}$, dar foarte important poate asigura un nivel de securitate ridicat sistemului, prin posibilitatea sau imposibilitatea violării comunicării între sistemul de securitate şi echipamentul de recepție instalat la CMRA. Colecția de standarde EN 50136 reglementează tocmai cerințele tehnice care trebuie respectate de echipamentele de emisie – recepție a mesajelor, dar şi a mediului de comunicație pe care se face comunicarea.

Până în momentul de față sunt adoptate următoarele standarde:

EN 50136 -1 Cerințe generale pentru sistemele de transmitere ale alarmei
EN 50136 - 2 Cerințe generale pentru echipamentul de transmitere al alarmei
EN 50136 - 3 Protocoalele de transmitere a alarmei (în pregătire)
EN 50136 - 4 Echipamentul de anunțare
EN 50136 - 5 Liber
EN 50136 - 6 Liber
EN 50136 - 7 Ghidul de aplicație

Aceste standarde specifică cerințele generale pentru performanța, încrederea şi caracteristicile de securitate ale sistemelor de transmitere ale alarmei, acoperă cerințele generale pentru conexiunile între un sistem de alarmă şi un centru de recepționare al alarmei. EN 50136 ar trebui să aplice pentru transmiterea tuturor tipurilor de alarme: incendiu, efracție, control acces.. În aplicarea acestui standard pentru comunicații făcute prin rețele publice de comunicații, se va ține cont şi de standardele de comunicare relevante pentru acestea.

Depinzând de nivelul de siguranță şi caracteristicile operaționale ale echipamentelor de recepție disponibile la CMRA, configurația sistemelor de transmisie ce vor fi folosite va varia, incluzând şi folosirea a mai mult de o căi de transmitere a mesajelor între un sistem de alarmă şi unul sau mai multe CMRA

Pentru asigurarea nivelului de siguranță impus sistemul de transmisie trebuie să fie reduntant, de exemplu o cale de transmisie să fie rețeaua de telefonie publică, iar reduntanță să fie asigurată de o cale de transmisie dedicată.

Pentru a îndeplini cerințele EN 50136, un sistem de comunicare trebuie să asigure că transmiterea stării sistemului de alarmă va fi:

- continuă,sau
- periodică şi/sau
- atunci când starea sistemului de alarmă se schimbă.

Dacă transmisia nu este continuă, aceasta trebuie controlată de către

- de sistemul de alarmă, şi/sau
- CMRA şi/sau
- sistemul transmisie de alarmă

Performanțele unui sistem de transmisie a alarmei sunt evaluate după criterii cum ar fi timpul de transmisie al mesajelor de alarmă, timpul de raportare a defectelor, semnalizarea securității şi disponibilității, inclusiv a rețelei de transmisie.

Rețeaua de transmisie trebuie aleasă în conformitate cu performanțele cerute. Deoarece performanțele rețelei de transmisie nu pot fi influențate, înainte de alegerea performanțelor sistemului de transmisie a alarmei, este necesară analizarea performanțelor rețelei de transmisie împreună cu operatorul de rețea.

Pentru anumite caracteristici specifice este introdus un sistem de clasificare sau măsurare. Fiind aplicabil la un număr al unei aplicații foarte diferite precum efracția, focul şi controlul accesului, cerințele pentru fiecare aplicație vor trebui specificate şi vor include clase pentru:

- timpul de transmitere (tabelul 1)
- timpul maxim (tabelul 2)
- perioada de raportare (tabelul 3)
- disponibilitatea (tabelul 4)

Timpul de transmisie (tabelul1) este durata de transmisie a mesajului de alarmă, din momentul în care alarma a fost semnalizată de către echipamentul de emisie al spațiului supravegheat către echipamentul de recepție central. Întrucât timpul de transmisie poate varia de la o transmisie la alta, datorită rețelei de transmisie (disponibilitatea liniilor, tipul şi numărul de comutări,..), valoarea acestuia este statistică. Din acest motiv, se specifică media aritmetică şi limita superioară de 95% a acestei valori.

Atunci când se proiectează un sistem pentru un caz concret este important să se verifice performanța intrinsecă a rețelei, prezentată pe clase în tabelul 1 Adițional, cea mai nefavorabilă valoare a timpului de transmisie trebuie luată în calcul în raport cu valoarea limită a aplicației. Clasele superioare cu timp de transmisie scurt sunt mult mai relevante dacă timpul de răspuns este imediat sau scurt.

Timpul maxim (tabelul 2) este specificat separat. De fiecare dată când timpul maxim este depăşit trebuie să fie considerat eroare pe timpul verificărilor de performanță. Fiecare eroare afectează criteriul de disponibilitate al sistemului de transmisie a alarmei

	Transmiterea timpului (sec)				
Clasa	D0	D1	D2	D3	D4
Medial aritmetică a tuturor transmisiilor	-	120	60	20	10
95% din toate transmisiile	240	240	80	30	15

Tabelul 1 Clasificarea timpilor de transmisie

	Timp maxim (sec)				
Clasa	MO	M1	M2	M3	M4
Timpul de transmisie maxim acceptabil	-	480	120	60	20

Tabelul 2 Timpul de transmisie, valori maxime

Timpul de raportare (tabelul 3) este perioada de timp din momentul apariției erorii în sistemul de transmisie a alarmei până la raportarea centrului de recepție a mesajului de eroare. Este folosit pentru a dovedi că sistemul de transmisie alarme este operațional, rezultând disponibilitatea practică a sistemului de transmitere a alarmelor. Timpul de raportare a erorii este legat de necesitățile de timp ale transmisiei, disponibilitate şi de protecția la manipulare.

Există mai multe moduri de a evalua timpul de raportare pentru a putea stabili o clasificare. Metodele selectate trebuie cuprinse într-o procedură scrisă clară. Câteva de exemple de evaluare:

- măsurarea timpului de la ultimul mesaj receptat cu succes de către centrul de recepție a alarmei(de către centrul de emisie – recepție sau de la echipamentul de avertizare)

- monitorizarea continuă folosind mesaje de test.

	Timpul raportat					
Clasa	T1	T2	T3	T4	T5	T6
Perioada maximă	32 Zile	24h	300 min	180 s	90 s	20 s

Tabelul 3, Clasificarea timpului de raportare

Disponibilitatea sistemului de transmisie alarme reprezintă perioada de timp, măsurată anual sau lunar, în care sistemul de transmisie este capabil de a transmite informații; această evaluare include probabilitatea apariției unor erori şi a timpului necesar pentru repunerea în funcțiune. Clasificarea adecvată, rezultată din metoda de calcul este de exemplu exprimată în procente. Evaluarea disponibilității depinde de echipamentul sistemului de transmisie a alarmei şi de rețelele de transmisie care vor fi selectate. Metoda de evaluare trebuie de exemplificată clar printr-o procedură scrisă. Suplimentar, aceste rețele trebuie alese în mod adecvat, luând în considerație următoarele:

- în cazul în care se utilizează o rețea de cablu trebuie acordată o atenție deosebită calității şi vulnerabilității legăturilor locale;
- trebuie acordată atenție solidității rețelei de transmisie cu clasificarea disponibilității cerută de compania de securitate (de exemplu: rețea de telefonie, rețea de transmisii de date, linii închiriate,...).

Disponibilitatea poate fi mărită prin folosirea căilor secundare sau a echipamentelor redundante. Acesta poate fi un alt sistem de transmisie a alarmei sau alt sistem sau linie de același tip. O combinație specială care îmbunătățește substanțial disponibilitatea poate fi introducerea complementară pe lângă telefonia fixă a unui sistem de telefonie mobilă,radio, IP.

Aceasta va duce la creşterea disponibilității totale a sistemului combinat de transmisie a alarmei. Trebuie identificate părțile comune ale sistemelor de transmisie a alarmei deoarece acestea pot reduce disponibilitatea în ansamblu.

	Disponibilitate				
Clasa	A0	A1	A2	A3	A4
Disponibilitatea tuturor sistemelor în orice perioadă din cele 12 luni	Nici o cerință	97%	99,3%	99,5%	99,8%
Disponibilitate lunară	Nici o cerință	75%	91%	95%	98,5%

Tabelul 4 Disponibilitatea sistemului

O altă caracteristică foarte importantă a unui sistem de transmisie este **semnalizarea securității transmisiei.** Sistemul de transmitere al alarmei va asigura măsurile de prevenire sau detectare ale atacurilor deliberate care interferează cu transmisia unui mesaj de alarmă sau o altă informație transmisă între un sistem de alarmă şi centrul receptor asociat prin blocarea sau substituirea în unul din următoarele feluri:

- SO – nici o măsură
- S1 – Măsuri de detectare a substituției ale anexelor transmițătorului prin adăugarea unei identități sau adrese în toate mesajele transmise la calea de transmitere a alarmei.
- S2 – măsuri de detectare a substituției ale anexelor supravegheate prin:
  - criptarea identității sau adresei în toate mesajele transmise la calea transmițătorului de alarmă

- autentificarea anexelor supravegheate prin adăugarea unui cod diferit şi nespus pentru fiecare transmițător conectat sau,
- o altă măsură precum este specificat de către furnizor

Autentificarea cere întotdeauna un număr de chei suficient pentru a asigura fiecare transmițătorul conectat la un cod unic. Marja de identitate în S2 nu trebuie să fie mai mică de 250 adrese unice.
Protecția informației transmisă de către CMRA va fi asigurată într-una din următoarele feluri:

- I0 – fără măsuri
- I1 – măsuri de prevenire a citirii neautorizate a informației transmise, acest lucru poate fi realizat prin criptare
- I2 – măsuri de prevenire modificări neautorizate a informației transmise, acest lucru poate fi realizat prin criptarea sau criptografierea metodei de autentificare
- I3 – măsuri de prevenire a citirii neautorizate şi a modificării neautorizate a informației transmise.

O altă caracteristică importantă a unui sistem de transmisie este **lățimea de bandă** sau puterea de trecere.
Comunicarea între un sistem de alarmă şi un echipament de recepție va continua să întâmpine cerințele unei transmisii adecvate de timp din tabelul 1 şi clasa de timp a unei transmisii maxime din tabelul 2 când alarma sau mesajele greşite sunt generate:

- la o rată echivalentă unui asemenea mesaj pe minut de la fiecare număr al anexelor supravegheate reprezentând până la 0,1% din capacitatea sistemului şi
- la o rată de cel puțin 2 mesaje de alarmă pe minut la interfața centrului receptor către echipamentul de anunțare.

Evaluarea va fi făcută atunci când sistemul de transmisie al alarmei este într-o condiție stabilă cu rata stipulată de mesaje. Când se stabileşte lățimea de bandă pentru un sistem de transmisie a alarmei trebuie luată în considerare şi o posibilă creştere a numărului de mesaje de alarmă ce pot apărea pe o perioadă scurtă de timp.
Performanța sistemului de transmisie poate fi afectată de transmisia simultană a mesajelor de eroare a centralelor în cazul unei căderi de tensiune într-o arie largă (de exemplu: oraş). În acest caz, o metodă de păstrare a ratei de transmisie este atribuirea unui centru de transmisie fiecărui tip de alarmă (de exemplu: incendiu, efracție) sau creşterea numărului de canale.
Un alt mod de a preîntâmpina încărcări mari pe liniile de transmisie este de exemplu echiparea dispozitivelor de transmisie cu baterii de rezervă şi întârzierea pentru un timp a alarmei datorate căderii de tensiune pentru a reduce numărul alarmelor simultane.

3.2. Clasificarea sistemelor şi echipamentelor de transmisie

Cu condiția respectării cerințelor impuse sistemelor de transmisie prin standardul EN 50136, echipamentele de transmisie pot fi clasificate în funcție de modul cum se face transmisia spre echipamentele de recepție instalate la MARC, în:

- comunicatoare vocale
- comunicatoare de date.

Datorită limitărilor tehnice pentru respectarea cerințelor standardului, comunicatoarele vocale mai sunt astăzi întrebuințate doar pentru alarmele sociale sau ptr. avertizări secundare. Pentru aplicațiile de securitate antiefracție şi incendiu sunt utilizate cu preponderență comunicatoarele digitale.
În funcție de modul de preluare a informației de la sistemul de securitate ele se clasifică în:

- comunicatoare analogice
- comunicatoare digitale.

Comunicatoarele analogice preiau de la sistemul de alarmă semnale analogice în principiu: nivele de tensiune sau stări ale unor contacte, pe care le convertesc în semnale digitale şi le transmit spre echipamentul de recepție. Dezavantajul acestui tip de comunicatoare este numărul limitat de semnale preluate din sistem (4 – 16), şi implicit un nivel scăzut de informații puse la dispoziția unității de

procesare a informației – UPI. Avantajul acestor tipuri de comunicatoare este că pot fii interfațate la orice sistem de alarmă, ele fiind în general un echipament exterior centralelor de alarmă.

Comunicatoarele digitale, care în momentul de față sunt cele mai utilizate, în general preiau informația de la centralele de alarmă prin interfețe RS 232 sau 485, având astfel posibilitatea să transmită toate schimbările de stare ale sistemului de alarmă.

O altă posibilitate de clasificare a comunicatoarelor poate fii făcută după calea de transmisie.:

- comunicatoare telefonice – PST
- GSM
- SMS
- comunicatoare radio
- comunicatoare IP – pe rețele internet
- GPRS

Comunicatoarele telefonice pe rețele publice PSTN sunt cele mai răspândite, majoritatea centralelor având integrate acest tip de comunicator.

Comunicatoarele GSM şi cele SMS sunt în principiu echipamente externe centralelor de alarmă, preluând informația de la acestea fie prin interfețe 485 fie de la comunicatorul telefonic, transmițând – o prin intermediul rețelelor de telefonie mobilă, pe purtătoarea de voce. Comunicatoarele GSM sunt utilizate cu precădere ca sistem de transmisie redundant pentru rețeaua de transmisie pe telefonia PSTN, sau în cazul în care nu există posibilitatea de conectare la o astfel de rețea.

Comunicatoarele SMS au deoarece nu pot îndeplinii întru – totul cerințele standardului sunt utilizate în mod special pentru semnalizări auxiliare.

Comunicatoarele radio datorită costurilor ridicate a rețelei de radio – transmisie sunt tot mai puțin utilizate.

Viitorul comunicațiilor constă în momentul în comunicatoarele IP. Comunicatoarele GPRS utilizează canalele de date ale rețelelor de telefonie mobilă, asigurând în momentul de față costuri de comunicație foarte reduse. Comunicatoarele IP pe rețele internet pot utiliza rețele deschise de internet sau rețele închise tip VPN.

3.3. Clasificarea sistemelor şi echipamentelor de recepție

Având în vedere diversitatea sistemelor de transmitere precum şi a comunicatoarelor digitale, producătorii au dezvoltat o gamă variată de echipamente de recepție a mesajelor de la sistemelor de securitate. Este greu de făcut o clasificare a acestora, totuşi pentru clarificare o să facem o clasificare a lor.

După mediul de transmisie al mesajelor de la comunicatorul digital putem face clasificarea următoare:

- Echipamente de recepție telefonic
- Echipamente de recepție GSM
- Echipamente de recepție radio
- Echipamente de recepție IP
- Echipamente de recepție combinate

Echipamentul de recepție poate să îndeplinească doar rolul de recepție a mesajelor, să decodifice formatul de comunicare, iar informația să o transmită unei unități de procesare a informației care poate fii un calculator dotat cu un soft adecvat. Constructiv aceste tipuri de echipamente sunt fie de tip PC Base, fie sub forma unor echipamente externe calculatorului. Avantajul acestor tipuri de echipamente constă în prețul redus de cost. Marele dezavantaj constă în faptul că oferă o autonomie redusă în cazul căderii alimentării AC, precum ridică probleme în ceea ce privește redundanța.

Corespunzând într-u totul standardului EN 50136 sunt echipamentele de recepție care includ partea de unitate de procesare a informației, acestea asigurând un nivel de securitate ridicat, şi o autonomie de funcționare în regim de avarie foarte mare.

Acest curs nu dorește să prezinte echipamente de recepție, deoarece varietatea conceptelor pe care producătorii de astfel de produse face dificilă alegerea unor echipamente. Este util însă a informa cursantul despre anumite caracteristici pe care aceste echipamente trebuie să le îndeplinească, pentru a putea concepe un sistem de monitorizare performant.
Acceptând că echipamentul selectat corespunde prevederilor standardelor, când alegem tipul de echipament de recepție este bine să ținem cont de următoarele recomandări:

- Echipamentul de recepție trebuie să poată asigura funcționarea în regim de avarie, asigurând pe lângă recepționarea mesajelor de la sistemelor de alarmă și posibilitatea punerii la dispoziția operatorului dispecer un minim de informații utile necesare luării deciziei și coordonării FIR
- Echipamentul de recepție trebuie să aibă în cazul utilizării liniilor telefonice publice sau a rețelelor de telefonie mobilă a mai multor canale de intrare.
- Echipamentul de recepție trebuie să aibă posibilitatea ca fiecare canal de intrare să aibă posibilitatea să recepționeze mai multe formate de comunicare
- Echipamentul de recepție trebuie să aibă posibilitate să lucreze cu echipamente redundante fără a fii necesară intervenția umană
- Echipamentul de recepție trebuie să aibă dacă e posibil să poată recepționa, utilizând aceeași unitate de procesare a informației, de la mai multe tipuri de comunicatoare digitale

Cap. 4 Formate de comunicare la CMRA

În configurarea unui sistem de securitate monitorizat, proiectantul trebuie să ia în calcul reducerea cât mai mult posibilă a timpului din momentul producerii efracției până la momentul acțiunii FIR. Reducerea timpului de transmisie - $\mathbf{T}_{T,}$ arătam că poate fi realizată prin alegerea unui sistem de comunicare adecvat, care să elimine pe cât posibil erori în transmiterea mesajelor, și să asigure o disponibilitate mare.
In cazul comunicatoarelor digitale foarte important pentru reducerea timpului de transmisie - $\mathbf{T}_{T}$ este alegerea formatului de comunicare ales pentru transmiterea informației. În funcție de tipul de format ales timpul din momentul când centrala de alarmă dă comanda trimiterii mesajului până în momentul când primește confirmarea de la echipamentul de recepție al MARC poate să varieze între câteva zeci de milisecunde până la câteva minute. Performanțele formatului depind de algoritmii de criptare utilizați, dar și de adaptibilitatea formatului la diferite medii de comunicare.
Fiecare producător de sisteme de securitate la început a dezvoltat propriul format de comunicare, încercând securizarea cât mai bună a semnalului transmis, dar și adaptarea formatului la diferite tipuri de medii de comunicare: radio, rețele de telefonie publice, rețele de telefonie private.
Diversitatea de formate de comunicare a creat probleme pe piața serviciilor de securitate prin incompatibilitatea între centralele de alarmă și echipamentele de recepție, impunând o standardizare a acestora. Primul standard a fost adoptat de către organismele de standardizare din SUA – UL și Canada – ULC. În lipsa unui standard european, și producătorii europeni de echipamente utilizează practic aceleași formatele de comunicare.
Cele mai răspândite formate de comunicare, la majoritatea producătorilor, sunt prezentate în tabelul 5, cu principalele caracteristici.

	Nume	Handshake	Data	Rata transm.	Format	Kiss off
1	Ademco Slow	1400 Hz	1900 Hz	10 BPS	3-1,3-2,4-1,4-2,4-2+	1400 Hz
2	S.K Fast	1400 Hz	1900 Hz	14 BPS	3-1,3-2,4-1,4-2,4-2+	1400 Hz
3	Franklin	2300 Hz	1800 Hz	20 BPS	3-1,3-2,4-1,4-2,4-2+	2300 Hz
4	Radionics	2300 Hz	1800 Hz	40 BPS	3-1,4-2, 4-2+	2300 Hz
5	Sur-Gard	2300 Hz	DTMF	DTMF	4-1, 4-2, 4-3	2300 Hz
6	Sur-Gard	Dual Tone/1400 Hz	DTMF	DTMF	4-1, 4-2, 4-3	1400 Hz
7	Acron	1400 Hz	DTMF	DTMF	3-8, 4-8	1400 Hz
8	DTMF Express	Dual Tone	DTMF	DTMF	4-1,4-2	1400 Hz
9	S.F.DTMF	Dual Tone	DTMF	DTMF	4 – 8 - 1	1400 Hz
10	Scantronics	Dual Tone	DTMF	DTMF	4-8-1,4-16-1,6-16-1	1400 Hz
11	FBI Super Fast	2300 Hz	DTMF	DTMF	4 – 3 - 1	2300 Hz
12	Contact ID	Dual Tone/1400 Hz	DTMF	DTMF	4-2-1-3-2-3	1400 Hz
13	SIA	FSK MARK	FSK MARK	110/300 BPS		Data ACK

Tabelul 5 Caracteristici formate de comunicare

Formatele de la 1 la 8 sunt formate de comunicare mai lente, foarte stabile şi adaptabile oricărui mediu de comunicare, dar datorită algoritmilor de criptare utilizați si ai ratei mici de transmisie, necesită un timp mare de transmisie.
Formatele de la 9 la 13 sunt formate de comunicare rapide realizând transmiterea mesajelor într-un timp extrem de scurt.
Cele mai utilizate formate de comunicare în momentul de față de majoritatea producătorilor de sisteme de securitate sunt Contact ID şi SIA.

4.1 Formatul Contact ID

Protocolul de comunicare Contact ID este următorul:

18 AAAA Q XYZ GG CCC

Unde:

18 – Identificator de protocol pentru dispecerat
AAAA – Codul de abonat
Q – Identificator de eveniment: E = 1 Eveniment nou
R = 3 Restabilire eveniment
P = 6 Eveniment anterior
XYZ – Codul evenimentului (3 cifre in format Hexazecimal)
GG – Identificator de grup (de regula 2 cifre in format Hexazecimal)
CCC – Identificator de zonă, număr de senzor, identificator de utilizator (3 cifre în format Hexazecimal)

Clasificarea Codurilor de raportare a evenimentelor in formatul Contact ID

Alarma Medicala – 100
101 Transmitator de tip "Pedala"
102 Lipsa raportare

Alarma Medicala - 100
101 Transmitator de tip "Pedala"
102 Lipsa raportare

Alarma Medicala - 100
101 Transmitator de tip "Pedala"
102 Lipsa raportare

Alarma de foc - 110
111 Fum
112 Combustie
113 Scurgere de apa
114 Caldura
115 Buton de incendiu
116 Galerie (cu referire la galeriile de aerisire sau ventilare)
117 Flacara
118 Alarma locala

Alarma de panica - 120
121 Constrangere
122 Silentios
123 Audibil

Alarma efractie - 130
131 Perimetral
132 Interior
133 24 ore
134 de tip Intrare/Iesire
135 de tip Zi/Noapte
136 De exterior
137 Sabotaj

Defectiuni de sistem – 300 si 310
301 Pierdere AC
302 Acumulator descarcat
303 Semnal control RAM incorect
304 Semnal control ROM incorect
305 Reset de sistem
306 Modificare Parametrii de programare
307 Imposibilitate efecture Auto-Test
308 Oprire sistem
309 Imposibilitate efecture test acumulator
310 Defect de impamantare

Defecte de sirena/relee - 320
321 Sirena 1 (defect iesirea de comanda sirena)
322 Sirena 2
323 Releu de alarma
324 Defect Releu de alarma
325 Inversare

Defecte periferice de sistem - 30/340
331 Bucla deschisa
332 Scurtcircuit bucla
333 Pierderea comunicatiei cu modulele
334 Defectiune repetor
335 Lipsa hartie imprimanta
336 Defectiune imprimanta

Defect de comunicatie - 350 / 360
351 Defectiune linie telefonica 1
352 Defectiune linie telefonica 2
353 Sistem de transmisie

Operatii de la distanta - 410
411 Cere de apelare executata
412 Acces autorizat pentru descarcare
413 Acces neautorizat
414 Inchidere sistem
415 Inchidere apelator

Control Acces - 420
421 Acces refuzat
422 Acces raportat de catre utilizator
441 Armare cu ramanere
451 Deschider/Inchidere devreme
452 Deschider/Inchidere tirzie
453 Intarziere la deschidere (dezarmare)
454 Intarziere la inchidere (armare)
455 Autoarmare nerealizata
459 Inchidere recenta (alarma a avut loc in mai putin de 2 minute de la armare)
470 Inchidere partiala (una sau mai multe zone au fost ocolite)

Operatii de dezactivare sirene/relee- 520
521 Sirena 1 dezactivata
522 Sirena 2 dezactivata
523 Releu de alarma dezactivat
524 Dezacticare raportare defect releu de alarma
525 Dezactivare raportare revers releu de alarma
Operatii de dezactivare module periferice - 530 /540

Deactivare comunicatie- 550 / 560
551 Apelator dezactivat

Alarme generale - 140
141 Bucla deschisa
142 Bucla in scurt
143 Defect Modul de Extesie
144 Sabotaj Senzor

Evenimente Non-Efractie de tip 24H 150 and 160
151 Detectie Gaz
152 Refrigerare
153 Pierdere de caldura
154 Scurgeri de lichid
155 Spargere fina/ușoară
156 Problema zilnica
157 Nivel scazut de Gaz in recipient
158 Temperatura mare
159 Temperatura scazuta
161 Diminuare debit de aer

Supervizare la foc – 200 si 210
201 Presiunea apei scazuta
202 Nivel scazut CO2
203 Senzor valva
204 Nivel scazut apa
205 Activare Pompa
206 Defectiune Pompa

Radio(VHF-UHF)
354 Defect de comunicare
355 Pierdere supervizare modul Radio
356 Pierdere supervizare de la dispecerat

Defecte de zona - 370
372 Defect de zona
373 Defect la zona de foc

Defecte senzori - 380
381 Pierdere semnal de supervizare RF
383 Sabotaj Senzor
384 Baterie descarcata dispozitiv radio (sensor radio)

Inchideri/deschideri - 400
401 Inchidere/Deschidere de catre Utilizator
402 Inchidere/Deschidere de Grup
403 Inchidere/Deschidere Automata
404 Intarziere la armare/ dezarmare
405 Anulare autoarmare
406 Dezarmare cu alarma in memoria de evenimente
407 Armare/dezarmare de la distanta
408 Armare rapida
409 Inchidere/deschidere cu cheie (functia “keyswitch arm”)

552 Transmitator radio dezactivat

Operatii de ocolire – 570 (bypass)
570 Ocolire zone
571 Ocolire zona de foc
572 Ocolire zona 24h
573 Ocolire zone antiefractie
574 Ocolire de grup

Test - 600
601 Test sistem (test declansat manual)
602 Test periodic de sistem
603 Test periodic al transmitatorului RF
604 Test incendiu
605 Urmarire raport de stare
606 Urmarire ascultare
607 Activarea modului de testare local
621 Reset memoria de evenimente
622 Memoria de evenimente la 50%
623 Memoria de evenimente la 90%
624 Depasire capacitate de memorare
625 Resetare ora/data
626 Ora/Data inexacte
627 Intrare in modul de programare
628 Iesire din modul de programare
631 Exceptare modificare orar

4.2 Formatul SIA

COD	Denumirea codului	Descrirea	Campul de adresă
AR	Restabilire AC	Tensiunea de alimentare a fost restabilita	nefolosi
AT	Lipsa AC	Nu exista alimentare cu energie electrica	nefolosit
BA	Zona in alarma	Zone in alarma	zona
BB	Ocolire zona	Una din zone a fost ocolita	zona
BC	Anulare alarma	Alarma a fost anumata de catre utilizator	utilizator
BH	Restabilire zona	Restabilirea zonei in alarma	zona

BJ	Restabilire defect de zona	Eliminarea cauzei de defect	zona
BR	Restabilire generala zone	Cauzele care au declansat alarma au fost eliminate	zona
BS	Supervizare alarma efractie	Conditie sistem: Detecție patrundere efracție	zona
BT	Defect zona	Zona testata raporteaza un defect	zona
BU	Dezactivare Ocolire zona	Ocolirea zonei/zonelor dezactivata	zona
BV	Confirmare Efractie	Mail mult de 3 zone au fost declansate	zona
BX	Test zona efractie	Testare zona efractie	zona
CA	Inchidere automata	Sistemul a fost armat in mod automat	partitia
CE	Armare extinsa	Timpul automat de armare a fost extins	utilizator
CF	Armare fortata	Sistemul a fost armat, unele zone sunt deschise	utilizator
CG	Armare partitie	O partitie a fost armata	utilizator
CI	Armare nereusita	O paritie nu a putut fi armata la expirarea timpului	utilizator
CJ	Intarzierea la armare	O partitie a foast armata dupa timpul alocat	utilizator
CK	Armare grabita	Armare normala	utilizator
CL	Armare	O partitie a fost armata ianintea timpului alocat	utilizator
CP	Armare automata	Sistemul a fost armat in mod automat	utilizator
CR	Armare recenta	Sistemul a dat alarma intr-un interval de 5min de la armare	utilizator
CS	Armare prin keyswitch	Sistemul a fost armat printr-o zona de keyswitch	zona de keyswitch
CT	Intarziere la deschidere	Sistemul nu a fost dezarmat la timp	partitia
CW	A fost armat fortat	Inceputul se sesiunii de armare fortata	partitia
CZ	Armarea unei zone	O zona (nu o partitie) a fost armata	Zona
DC	Acces restrictionat	Accesul restrictionat tuturor utilizatorilor	usa
DD	Acces nepermis	Acces nepermis, cod incorect	Usa
DF	Usa fortata	Usa a fost deschisa fara o cerere de acces autorizat	usa
DG	Acces permis	Accesul a fost autorizat	usa
DK	Acces blocat	Accesul a fost blocat, codul este valid	usa
DO	Acces deschis	Accesul a fost alocat pentru utilizatorii autorizati	usa
DR	Restabilire usa	Alarmele/ defectele au fost eliminate	usa
DS	Post Uşa	Identifica usa corespunzatoare raportului urmator	usa
DT	Defect Acces	Defectiune la sistemul de control acces	nefolosit
DU	ID apelator	Descrierea zonei ce oferă ID apelator	ID apelator
EA	Alarma de iesire	O zona de iesire a fost deschisa peste timpul alocat	zona

ER	Reset modul extensie	Defectul de pe modulul de extensie a fost eliminat	numarul modulului
ET	Defectiune modul extensie	Unul din modulele de extensie are un defect	numarul modulului
FA	Alarma de incendiu	Afost detectata o conditie de alarma incendiu	zona
FB	Ocolire zona incendiu	O zona de incendiu a fost ocolita	zona
FH	Restabilire zona incendiu	Conditia de alarma a fost eliminata	zona
FI	Declansare Test incediu	Declansarea testului de incendiu	partitie
FJ	Restabilire defect zona	Defetul de zona a fost eliminat	zona
FK	Incheiere Test incendiu	Incheierea testului de incendiu	partitie
FR	Restabilire zona incendiu	Alarma/defectul a fost eliminat	zona
FS	Supervizare la incendiu	A fost detectata o posibila conditie de alarma	zona
FT	Defect zona incendiu	Zona a fost dezactivata din cauza unui defect	zona
FU	Ocolire zona foc dezactivata	Ocolirea zonei de foc a fost dezactivata	zona
FX	Test zona foc	Zona de foc a fost activate in timpul testului	zona
FY	Detector lipsa	Lipsa detector de pe bucla	zona
GA	Alarma de gaz	O zona de gaz a fost declansata	zona
GB	Ocolire zona de gaz	Zona a fost ocolita	zona
GH	Restabilire zona gaz	Zona a revenit din alarma	zona
GJ	Restabilire zona gaz dupa defect	Cauza defectului a fost eliminata	zona
GR	Restaurare zona gaz	Toate alarmele/defectele depe zona de gaz au foat eliminate	zona
GS	Supervizare la gaz	Detectia unei scurgeri de gaz	zona
GT	Defect pe zona de gaz	Zona a fost dezactivata din cauza unei defectiuni	zona
GU	Dezactivare ocolire zona gaz	Ocolirea zonei de gaz a fost dezactivata	zona
GX	Testare sensor GAZ	A fost activate o zona de gaz in timpul testului	zona
HA	Panica	Alarma silentioasa de panica, utilizator sub constrangere	zona
HB	Ocolire Panica	Zona de panica a fost dezactivata/ocolita	zona
HH	Restabilire panica	Cauza declansarii alarmei de panica a fost eliminata	zona
HJ	Restabilire zona de panica dupa defect	Cauza defectiunii a fost eliminata	zona
HR	Restabilire panica	Toate alarmele/defectle au fost eliminate	zona
HS	Supervizare panica	A fost detectata o posibila conditie de alarma	zona

HT	Defect zona de panica	Zona a fost dezactivata datorita unei cause de defect	zona
HU	Dezactivare ocolire panica	Ocolirea zonei de panica dezactivata	zona
JA	Sabotaj cod utilizator	Incercari repetate si fara success de a introduce un cod utilizator	Partitia
JD	Schimbare data	Data a fost modificata	utilizator
JH	Schimbare orar vacanta	Orarul de vacanta a foast modificat	utilizator
JL	Prag critic capacitate memorie evenimente	A fost atins un prag critic al capacitatii memoriei	neutilizat
JO	Capacitate memorie evenimente depasita	A fost depasita capacitatea de stocare a memorie	neutilizat
JR	Executare Orar	A fost executat un eveniment dupa un orar stabilit	partitia
JS	Schimbare Orar	A fost schimbat un orar	utilizator
JT	Modificare Timp	Timpul de TX/RX a fost schimbat	utilizator
JV	Modificare cod utilizator	A fost schimbat un cod de utilizator	utilizator
JX	Stergere cod utilizator	A fost schimbat un cod de utilizator	utilizator
KA	Alarma de temperatura	A fost depistata o crestere de temperature	zona
KB	Ocolire zona temperatura	Senzorul de temperature a fost ocolit	zona
KH	Restabilire alarma temperature	Conditia de alarma a fost eliminata	zona
KJ	Restabilire defect temperatura	Restabilirea sensorului de temperature dupa defect	zona
KR	Restabilire temperatura	Toate conditiile de alarma/defect au fost eliminate	zona
KS	Supervizare termică	Condiție system: detectare termică	zona
KT	Defeciune sensor temperatura	Zona a fost desactivata din cauza unei defectiuni	zona
KU	Ocolire sensor temperature dezactivat	A fost dezactivata ocolirea zonei	zona
LB	Intrare programare locala	Intrarea in meniul instalator pentru programare	nefolosit
LD	Intrare programare locala nepermisa	Accesul in meniul de programare nepermisa	nefolosit
LE	Sfarsit sesiune Listen-In		nefolosit
LF	Inceput sesiune Listen-In		nefolosit
LR	Restabilire linie telefonica	Linia telefonica a fost reconectata	linia
LS	Programare locala	Programarea locala realizata cu succes	nefolosit
LT	Defectiune linie telefonica	Linia telefonica a fost deconectata sau intrerupta	linia
LU	Programare locala nerealizata	Nu sa putut realize programarea	nefolosit

LX	Sfasit sesiune programare locala	S-a incheiat sesiunea de programare	nefolosit
MA	Panica medicala	Cerere asistenta medicala de urgenta	zona
MB	Ocolire panica medicala	Zona de panica medicala a fost ocolita	zona
MH	Restabilire panica medica	Conditia de panica medicala a fost anulata	zona
MJ	Restabilire defect panica medicala	Conditia de defect a fost inlaturata	zona
MR	Restabilire generala panica medicala	Toate alarmele/defectele medicale anulate	zona
MS	Supervizare medicala	Existenta condiție sistem	zona
MT	Defectiune panica medicala	Defectiune la zona de panica medicala	zona
MU	Ocolire zona medicala dezactivata	Ocolirea zonei de panica medicala dezactivata	zona
NA	Fara activitate	Nu a existat nici un eveniment in intervalul de timp programat	nefolosit
NF	Perimetru cu armare fortata	Armarea partitiei/perimetrului cu zone neinchise	partitia
NL	Perimetru armat	O partitie a fost armata in mod stay/ perimetral	partitia
OA	Deschidere automata	Sistemul s-a dezarmat automat	partitia
OC	Anulare raport	Anulare zona nedefinita	utilizator
OG	Partitie dezarmata	Sistemul a fost partial dezarmat	Partiti
OI	Deschidere nerealizata	O partitie nu a fost dezarmata la expirarea timpului alocat	partitie
OJ	Intarziere la deschidere	O partitie nu a fost dezarmata la timp	utilizator
OK	Deschidere radida	Partitia a fost dezarmata mai repede de timpul alocat	utiliztor
OP	Deschidere	Dezarmarea sistemului	utilizator
OR	Dezarmare dupa alarma	Sistemul a fost dezarmat in timpul unei alarme	zona
OS	Dezarmare keyswitch	Ssitemul a fost dezarmat printr-o zona de keyswitch	utilizator
OT	Intarziere la inchidere	Sistemul nu a fost armat la timp	zona
OZ	Deschidere partiala	A fost dezarmata o zona (nu o intreaga partitie	zona
PA	Panica	Alarma de panica, activate manual	zona
PB	Ocolire declansare panica	Zona de panica a fost ocolita	zona
PH	Restabilire panica	Alarma de panica a fost eliminata	zona
PJ	Restabilire defect panica	Defcetul de pe zona de panica a fost eliminate	zona
PR	Restabilire generala panica	Toate alarmele/defectele au fost eliminate	zona
PS	Supervizare panica	Existenta conditie sistem	zona

PT	Defect zona panica	Zona de panica este defecta	zona
PU	Ocolirea zonei de panica dezactivata	Ocolirea zonei de panica dezactivata	zona
QA	Urgenta	Cerere de asistenta de urgrnta	zona
QB	Ocolire urgenta	Ocolire zona de urgenta	zona
QH	Restabilire urgenta	Alarma de urgenta a fost eliminate	zona
QJ	Restabilire defectiune urgenta	Defectul de urgenta a fost eliminat	zona
QR	Restabilire generala urgenta	Toate alarmele/defectele de urgenta au fost eliminate	zona
QS	Supervizare urgenta	Existenta conditie sistem	zona
QT	Defectiune zona urgenta	Defectiune la zona de urgenta	zona
QU	Ocolirea zonei de urgenta dezactivata	Ocolirea zonei de urgenta dezactivata	zona
RA	Comunicare nerealizata	Comunicare nerealizata cu calculatorul de programare	nefolosi
RB	Inceput sesiune download cu calculatorul	Inceput sesiune download cu calculatorul	nefolosi
RC	Releu activat	Releul cu numarul din adresa s-a activate	adresa releu
RD	Comunicare remote nepermisa	Parola incorecta	nefolosit
RN	Reset de la distanta	Sistemul a fost resetat de la distanta	nefolosit
RO	Releu dezactivat	Releul cu numarul din adresa s-a dezactivat	adresa releu
RP	Test Automat	Test comunicatie generat autonat	nefolosit
RR	Punere in functiue	Sistemul a fost realimentat	nefolosit
RS	Programare de la distanta reusita	Programarea de la distanta s-a incheiat cu succes	nefolosit
RT	Pierdere date	Pierdere mesaje, probleme la comunicator	linia
RU	Programare de la distanta nerealizata	Programare de la distanta nerealizata	nefolosit
RX	Test manual	Test de comunicatie declansat manual	utilizator
SA	Declansare sprinkler	Exista o conditie de declanzare a sprinklerelor	zona
SB	Ocolire declansare sprinkler	Ocolire declansare sprinkler	zona
SH	Restabilire sprinkler	Conditia de declansare sprinklere eliminata	zona
SJ	Restabilire defect sprinkler	Eliminarea conditiei de defectiune la sprinklere	zona
SR	Restabilire generala sprinklere	Toate conditiile de alarna/defect sprinklere eliminate	zona
SS	Supervizare sprinklere	conditie system: sprinkler neasigurat	zona
ST	Defectiune sprinkler	Defectiune la zona de sprinklere	zona

SU	Dezactivare ocolire sprinkler	Dezactivare ocolire sprinkler	zona
TA	Alarma de sabotaj	Sabotaj la carcasa echipamentului	zona
TB	Ocolire zona sabotaj	Dezactivare zona de sabotaj	zona
TE	Sfarsit de test	Comunicatia a fost restabilita, test ok	nefolosit
TR	Restabilire sabotaj	Zona de tamper a fost restabilita (inchisa)	zona
TS	Inceput de test	Inceput de test	nefolosit
TU	Dezactivare ocolire sabotaj	Comunicatia a fost orpita	zona
TX	Raportare de test	Declansarea unui test de comunicatie manual/automatic	zona
UA	Alarma zona nespecificata	conditie de alarma nespecificata de la o zona nedefinita	zona
UB	Ocolire zona nespecificata	Ocolire zona nespecificata	zona
UH	Restabilire zona nespecificata	Conditia de alarma a foast eliminata	zona
UJ	Restabilire defect azona nespecificata	Conditia de defect a foast eliminata	zona
UR	Restabilire generala zona nespecificata	Toate conditiile de alarma/defect au fost eliminate	zona
US	Supervizare zona nedefinita	Conditie de la tip zona necunoscuta	zona
UT	Defectiune zona nespecificata	Defectiune la zona nedefinita	zona
UU	Desactivare ocolire zona nespecificata	Desactivare ocolire zona nespecificata	zona
UX	Nespecificat	O conditie de alarma a fost declansata (nespecificat)	nefolosit
UY	Lipsa zona nespecificata	O zona/punct care nu a fost armata lipseste fizic	zona
UZ	Alarma la lipsa zona nespecificata	Alarma la lipsa zona nespecificata	Nefolosit
VI	Incarcare hartie imprimanta	Incarcare hartie imprimanta	Printer
VO	Lipsa hartie imprimanta	Lipsa hartie imprimanta	Printer
VR	Restabilire imprimanta	Restabilire imprimanta	Printer
VT	Defect imprimanta	Defect imprimanta	Printer
VX	Test imprimanta	Test imprimanta	Printer
VY	Imprimanta conectata	Imprimanta receptorului este on-line	Printer
VZ	Imprimanta deconectata	Imprimanta receptorului este off-line	Printer
WA	Alarma de inundatie	Detectare infiltrare/scurgere de apa	zona
WB	Ocolire zona inundatie	Zona de inundatie a fost dezactivata/ocolita	zona
WH	Restabilire zona inundatie	Conditia de declansare alarma inundatie a fost elimincata	zona
WJ	Restabilire defectiune zona inundatie	Defectul a fost eliminat	zona

WR	Restabilire generala zona inundatie	Tote alarmele/defectele au fost eliminate	zona
WS	Supervizare umiditate	conditie system: detectie umuditate	zona
WT	Defectiune zona inundatie	Dezactivare datorata defectiunii	zona
WU	Dezactivare ocolire zona inundatie	Dezactivare ocolire zona inundatie	zona
XE	Punct exterior	Centrala sesizeaza un punct exterior	nedefinit
XF	Punct exterior RF	Centrala sesizeaza un punct RF	nedefinit
XI	Reset senzor	Un utilizator a resetat o zona	zona
XR	Restabilire baterie telecomanda	Bateria din telecomanda a fost inlocuita	zona
XT	Baterie telecomanda descarcata	Baterie telecomanda descarcata	zona
XW	Punct fortat	Punct fortat in afara sistemului pe perioada armata	zona
YB	Secunde ocupate	Procentaj de timp in care cardul de line este on-line	card
YC	Lipsa comunicatie	Lipsa comunicatie	nefolosit
YD	Defectiune cartela de linie receptor	Defectiune cartela de linie receptor	linie
YE	Restabilire cartela de linie receptor	Restabilire cartela de linie receptor	linie
YF	Camp de control necorespunzator	Camp de control necorespunzator	nefolosit
YG	Schimbare parametrii	Schimbare parametrii	nefolosit
YK	Restabilire comunicatie	Sistemul a reluat comunicarea cu receptorul	nefolosit
YM	Lipsa acumulator	Lipsa acumulatorul sistemului/receptorului	nefolosit
YN	Raport Invalid	Sistemul a trimis un mesaj invalid	nefolosit
YO	Mesaj necunoscut	A fost receptionat un mesaj necunoscut	nefolosit
YP	Defectiune sursa alimentare	Defectiune sursa alimentare	nefolosit
YQ	Restabilire sursa alimentare	Restabilire sursa alimentare	nefolosit
YR	Restabilire lipsa acumulator	Restabilire lipsa acumulator	nefolosit
YS	Defect de comunicatie	Defect de comunicatie	nefolosit
YT	Defectiune acumulator	Defectiune acumulator	nefolosit
YW	Reset watchdog	Sistemul s-a resetat intern	nefolosit
YX	Necesar interventie service	Sistemul necesita verificare	nefolosit
YY	Raport de stare	Inceput de transmisie	nefolosit
YZ	Service efectuat	Service efectuat	nefolosit
ZA	Alarma de inghet	A fost detectata o conditie de inghet	zona
ZB	Ocolire zona inghet	Ocolire zona inghet	zona
ZH	Restabilire zona inghet	Conditia de alarma a fost inlaturata	zona

ZJ	Restabilire defect zona inghet	Conditia de defect a fost inlaturata	zona
ZR	Restabilire generala zona inghet	Toate conditiile de alarma/defectiune au fost eliminate	zona
ZS	Supervizare inghetare	Conditie sistem:inghetare nesigura	zona
ZT	Defectiune zona inghet	Defectiune zona inghet	zona
ZU	Dezactivare ocolire zona inghet	Dezactivare ocolire zona inghet	zona

Cap. 5 Centrul de Recepționare şi Monitorizare a Alarmelor

5.1. Cerințe ale organizării şi funcționării CMRA

Pe lângă condițiile tehnice prevăzute în EN 50136, necesare a fii îndeplinite de sistemele de transmisie a sistemelor de securitate şi de către echipamentele de recepție, colecția de standarde EN 50518 reglementează aspecte organizatorice şi funcționale ale CMRA, plecând de la măsurile de protecție ale obiectivului unde este amplasat, trecând la măsurile de electro – alimentare până la procedurile de funcționare şi conducere.
Până în momentul de față sunt în curs de adoptare următoarele standarde:
EN 50518 -1 Cerințele pentru locația şi construcția
EN 50136 - 2 Cerințe pentru facilitățile tehnice
EN 50136 - 3 Procedurile şi condițiile de operare

5.2. Cerințe constructive ale CMRA

CMRA trebuie situat pe un amplasament care oferă riscuri scăzute de incendiu, explozie, inundații, vandalism şi expunere la pericole de la alte obiective. Acolo unde CMRA nu ocupă toată clădirea în care se află, ar trebui sa fie separat de restul clădirii printr-o limitare fizică.
Accesul în clădire sau într-o parte a clădirii ar trebui să fie utilizat exclusiv de către compania care operează CMRA. Constructiv CMRA trebuie să dispună minim de următoarele încăperi: camera operațiuni,vestibul, grup sanitar, loc de luat masa. In fig. 4 este prezentată un model de organizare a unui CMRA.

Suprafața clădirii ocupată de compania unde operează centrul de monitorizare trebuie sa fie protejat printr-un sistem de alarma contra efracției, sistem de detecție şi avertizare în caz de incendiu, sistem de supraveghere video, sistem de control al accesului. De asemenea clădirea trebuie prevăzută cu mijloace manuale de stingere a incendiului.
Siguranța şi securitatea personalului CMRA trebuie să fie monitorizate în mod automat, la intervale de maxim 60 minute. In cazul lipsei răspunsului la controlul de securitate al personalului în termenul stabilit, trebuie alarmat un alt CRMA.

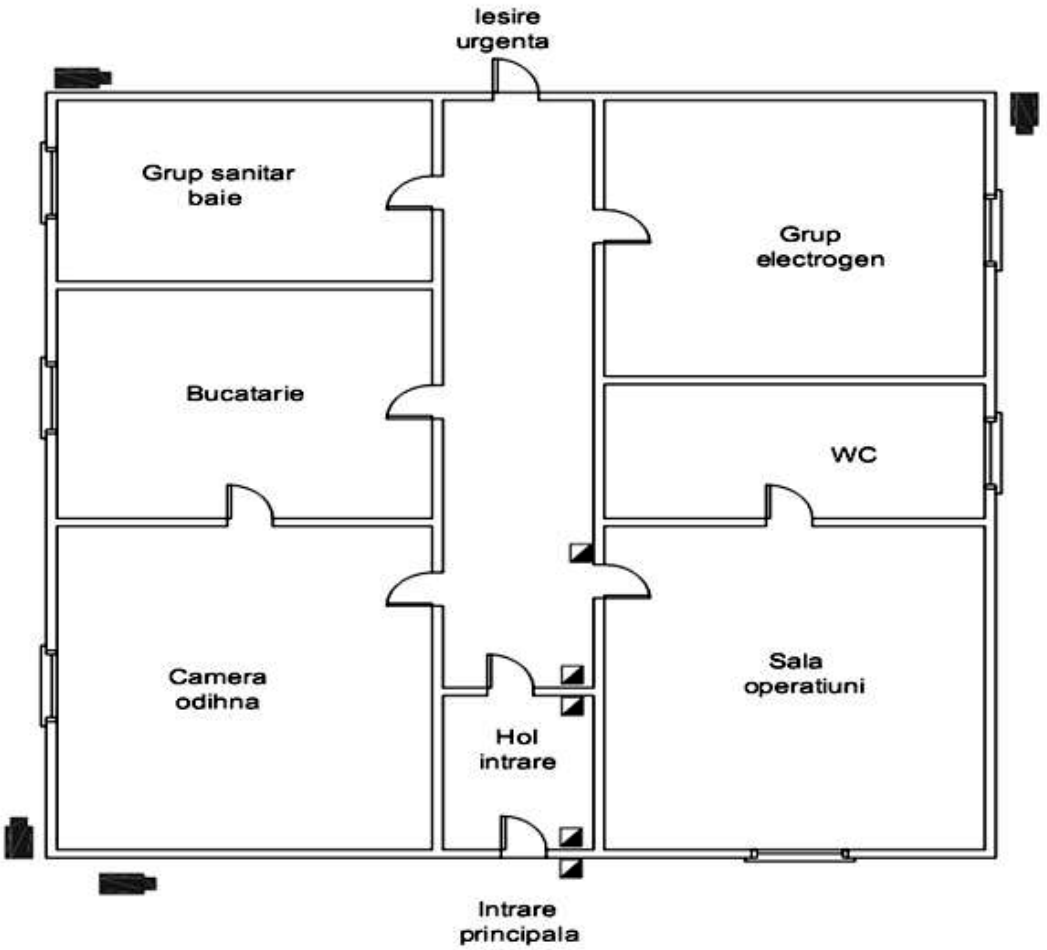


Fig. 4 Model CMRA

5.3 Alimentarea CMRA

Rețeaua publică de alimentare va fi folosită ca sursă principală de alimentare pentru centrul de monitorizare. Distribuția consumatorilor interni se va face pentru următoarele circuite:

- pentru echipamentul de recepționare semnale de alarmă,
- pentru echipamentul de securitate
- pentru iluminat şi consumatori electrocasnici

Tabloul de distribuție se amplasează obligatoriu în interiorul MARC.

În cazul unei întreruperi a rețelei publice de alimentare, un generator al sursei stand-by se va conecta automat. Sursa Stand-by va conține o baterie reîncărcabilă, localizată în interiorul centrului de monitorizare, de o capacitate suficientă de susținere a funcționări echipamentului de recepție şi a sistemelor proprii de securitate, pentru o perioadă nu mai mica de 24 ore, sau nu mai puțin de 4 ore în cazul unui singur generator Stand-by instalat sau 30 minute unde există un generator secundar. Pentru calculatorul centrelor de monitorizare, bateria reîncărcabilă va opera prin intermediul unui sistem UPS.

Capacitatea amperoră sursei stand-by va fi calculată in baza mediei curentului de descărcare din ora în ora înmulțit cu 1.5. Orice facilitate de încărcare va fi suficientă pentru a produce maximum de încărcare cerută şi simultan să reîncarce bateria din faza de complet descărcată la 80% din capacitatea ceruta în mai puțin de 24 ore.

Unde este instalat un generator stand-by, nu neapărat în suprafața protejată, acesta va produce capacitatea de alimentare stand-by mai mult decât este necesar. Se va pregăti o cantitate suficienta de combustibil adecvat pentru ca acesta să funcționeze cel puțin 24 ore. Un asemenea generator va porni automat.

5.4 Recepționarea semnalelor

Natura şi locația fiecărui semnal recepționat va fi separate identificat la centrul de monitorizare şi toate
semnalele vor fi automat înregistrate, oferind cel puțin următoarele informații:

- Identificarea clientului/utilizatorului.
- Natura semnalului
- Data şi ora recepționării semnalului.

Adițional, unde acțiunea operatorului rezultă din recepționarea unui semnal, detaliile acțiunilor luate vor fi înregistrate, inclusiv data şi timpul completări şi identitatea persoanei/persoanelor care a/au luat măsurile.
Mesajele pe bandă magnetică sau mesajele vocale generate electronic nu vor fi folosite pentru a transmite semnale centrului de monitorizare de la sistemele de alarma contra efracției care apelează automat.
O altă cerință impusă CMRA, în ceea ce priveşte recepționarea semnalelor, este aceea referitoare la monitorizarea conexiunilor liniilor de comunicare.
În cadrul unui sistem de comunicare digital calea de transmisie a alarmei este stabilită doar temporar pentru transmisia unui eveniment. De aceea monitorizarea continuă de la un capăt la celălalt al căi de transmisie, nu este posibilă.
Una dintre cele mai folosite metode de monitorizare poate fi atinsă prin inițierea transmisiilor test la intervale regulate.
O altă soluție de monitorizare este cea de supervizare a liniilor de comunicare de către operatorul care asigură mediul de comunicare, şi notificarea CMRA pentru aplicarea procedurilor în astfel de situații.

5.5. Procedurile de funcționare şi operare

Centrul de monitorizare va fi în permanență întreținut de minim doi operatori. Daca un CMRA operează împreună cu un al doilea CMRA în acelaşi timp si metodele operaționale asigură că efectul este acelaşi cu cel în care exista minim doi operatori, această cerință este nulă
Întreg personalul CMRA trebuie să dețină competențele profesionale şi experiență în activitatea pe care o desfăşoară. Înaintea intrării în serviciul operativ trebuie să existe o perioadă minimă de instruire pentru a asigura competența necesară îndeplinirii obligațiilor de serviciu.
Pentru asigurarea disponibilității CMRA, se recomandă asigurarea redundanței cu un alt centru CMRA. De asemenea este recomandat ca fiecare CMRA să fie monitorizat de un alt CMRA, în următoarele circumstanțe:

- deschiderea simultana a ambelor uşi de la intrarea in centru
- atac personal
- activarea alarmelor de efracție şi/sau incendiu

Informații despre fiecare sistem conectat la CMRA sunt disponibile dispecerilor. Informațiile pot fi scrise sau stocate în memoria unui calculator dar în ambele cazuri listarea trebuie să fie disponibilă.
Informațiile trebuie să include:

- numele, adresa şi numărul de telefon de contact al clientului
- numărul de referință al localului şi orice aranjament special
- numele, adresa si numerele de telefon ale utilizatorilor
- acțiunile care trebuie executate în cazul unei alarme
- înțelegerile existente şi resetarea timpilor acolo unde e necesar

Toate comunicările către CMRA trebuie înregistrate şi informația trebuie arhivată pentru o perioadă de minim:

- 3 luni – toate comunicările telefonice către si din spre CMRA împreună cu data şi ora
- 12 luni - toate informațiile comunicate către şi de la CMRA cu privire la evenimentele monitorizate împreună cu data şi ora.

- 12 luni - Perioada de arhivare a comunicărilor sau informaţilor telefonice cu privire la incidente supuse cerinţelor autorităţilor.

5.6. Procedurile de urgență

Procedurile de urgență trebuie sa țină cont de posibilele pericole care pot apare. Unele ar putea fi următoarele:

- Incapacitatea totală de procesare a CMRA
- Distrugerea sau avarierea utilităților
- Foc, sau expunerea la foc de la locațiile învecinate
- Inundație, sau avariile țevilor de apă.
- Eşecul comunicărilor de infrastructură
- Accidente rutiere, inclusiv feroviare şi aviatice
- deteriorare intenționată a CMRA
- Atac criminal, amenințare cu bombă sau situații de constrângere
- activități anormale sau deficit de personal

In cazul în care un CMRA este scos din funcție procedurile de urgenta trebuie aplicate pentru a face față situației date. Procedurile de urgență trebuie să facă față oricărei apariții anormale la CMRA Aici se include orice problema la CMRA, care degradează serviciului. Procedura de urgenta trebuie să acopere o situație tehnică sau orice situație. Planul de urgență trebuie sa conțină:

- modalitatea de informare a serviciilor de urgență
- modalitatea de conducere spre CMRA secundar şi/sau redirecționarea semnalelor.
- modalitatea de informare a utilizatorilor de sistem afectat
- modalitatea de informare a clienților/utilizatorilor

Cap. 6 Mentenanța sistemelor de securitate monitorizate

Pentru păstrarea în parametrii inițiali ai sistemului de securitate monitoritzat este obligatoriu asigurarea mentenanței periodice atât la echipamentele aparținând CMRA, cât mai ales asupra sistemelor de securitate instalate la obiectivele monitorizate.

6.1. Mentenanța CMRA

Următoarele echipamente ale centrului de monitorizare vor fi verificate pentru a funcționa normal, şi rezultatele vor fi înregistrate:

- La intervale de maxim 24 ore:
  - Ora(orele) interne ale echipamentului de recepționare a semnalului de alarmă, împreună cu orice alt echipament implicat în asigurarea întregi activități, inclusiv acțiunile operatorului, sunt exact datate.
  - Comunicările externe.
- La intervale nu mai mari de 7 zile**:**
  - Sursele de alimentare principala si stand-by, transformatorul, iluminatul de urgenta si sistemul de alarma al MARC.
  - Toate liniile care recepționează semnalele de alarmă împreună cu cele ce furnizează comunicarea vocala cu centrul de monitorizare.

6.2. Mentenanța sistemelor de securitate monitorizate

Verificările periodice ce trebuie operate asupra echipamentelor şi sistemelor de securitate, sunt de regulă prevăzute de producătorii echipamentelor, dar şi prin norme tehnice ale autorităților de reglementare. Aceste verificări cad atât în sarcina utilizatorului – verificări zilnice, săptămânale, cât şi în sarcina personalului firmelor de specialitate care asigură mentenanța – verificări lunare, trimestriale, anuale. Când sistemul de securitate este monitorizat este foarte important pe lângă aceste verificări, firma care asigură monitorizarea să asigure verificări asupra sistemelor de transmisie a mesajelor.
Verificarea funcționalității a unui sistem transmițător de alarmă trebuie să cuprindă un număr de aspecte precum cele enumerate mai jos:

- Verificare comunicării corecte la MARC a alarmei date pe fiecare dispozitiv de detecție sau alarmare manuală;
- Verificare comunicării corecte la MARC a sabotajului pentru fiecare dispozitiv, circuite electrice, şi/sau elemente constructive ale sistemului
- Verificare comunicării corecte la MARC a mesajelor de defect
- Verificarea autonomiei sistemelor pe sursa stand - by
- Verificarea faptului că mesajele de alarmă sunt trimise printr-un sistem la destinația intenționată şi testată de sistemul de monitorizare.
- verificarea timpului de transmitere al alarmei
- o verificare vizuală a sistemului de securitate şi identificarea modificărilor operate asupra acestuia de natură a diminua nivelul de securitate inițial

NOȚIUNI DE MANAGEMENTUL CALITĂȚII – PROCEDURI ŞI INSTRUCȚIUNI

Întocmit:
Ing.Adrian Mihai VASU

CUPRINS

CAPITOLUL 1 – INTRODUCERE ÎN MANAGEMENTUL CALITĂȚII

1.1 DEFINIREA CALITATII

Pentru a putea intelege sistemele de management al calitatii este important sa definim in primul rand calitatea.
Sa incepem cu un exemplu concret.
Cred ca suntem cu totii de acord ca un Mercedes S600 nou (cu motor de 517 CP la 5000rpm), care are un pret de lista (fara optionale) de 129.500 Euro, este un autoturism de calitate.
De ce ?Din cauza pretului ? Din cauza designului ? Din cauza ca proprietarul lui este bogat si poate renumit ?
Sa-l comparam cu Daewoo Cielo, al vecinului meu de bloc (dl. Nelu).
Acesta e vechi cam de opt ani, a costat cel mult 2000 Euro si trebuie reparat destul de des.
Daca punem problema astfel, cu siguranta ca automobilul d-lui Nelu nu poate fi descris ca un produs de calitate.
Dar ce este mai potrivit pentru necesitatile vecinului meu ?
Utilizarea potrivita este unul dintre factori.
Cielo il duce pe vecinul meu la serviciu la timp.
Are un consum de benzina rezonabil.
Reparatiile nu costa mult.
Masina este suficient de incapatoare pentru nevoile lui de transport.
Alt factor ar fi valoarea oferita pentru banii cheltuiti.
Daca e cat de cat intretinut Cielo mai rezista cativa ani.
Pentru a-si merita pretul, Mercedesul ar trebui sa-l duca pe vecinul meu la serviciu mai mult de 100 de ani.
Astfel Cielo va oferi o valoare superioara pentru banii cheltuiti de dl. Nelu.
Ce ne spun toate acestea despre calitatea masinii domnului Nelu ?
Se potriveste scopului sau, ofera valoare pentru banii cheltuiti si satisface exact necesitatile proprietarului – ceea ce il face un autoturism de calitate.
In schimb Cielo nu ar satisface necesitatile unui proprietar de firma cu cifra de afaceri anuala de 50 de milioane de Euro care trebuie sa-si impresioneze potentialii clienti cu confortul si luxul unui Mercedes S600.
Calitatea ceruta de scopurile nostre este deci strans legata de necesitati.
Cel mai bun nivel al calitatii este acela care satisface exact necesitatile noastre si care ofera cea mai buna valoare pentru banii cheltuiti.
Cand furnizam produse catre clientii nostrii, chiar daca preturile sunt scazute, daca produsele sau serviciile noastre nu le vor satisface asteptarile, ei vor cauta produse de o calitate mai buna in alta parte.
Esential este ca in calitate de furnizori sau prestatori de servicii sa determinam necesitatile clientilor nostrii si sa le satisfacem la pretul pe care ei vor sa-l plateasca; numai atunci putem spune ca oferim cea mai buna calitate.

Acum putem defini CALITATEA - este *aptitudinea de utilizare potrivita* si *valoarea oferita pentru banii cheltuiti*, si mai mult decat atat, *satisfacerea necesitatilor clientilor.*

1.1 NECESITATEA IMPLEMENTARII UNUI SISTEM DE MANAGEMENT AL CALITATII

Toate firmele preocupate de calitate trebuie in primul rand sa stie exact care sunt clientii lor.
Numai dupa aceea putem raspunde la cerintele specifice ale acestora si astfel sa reusim sa livram produse si servicii de calitate.

Departamentul de marketing al firmei identifica clientii, nevoile lor si gradul in care ei sunt pregatiti sa cheltuiasca pentru a-si satisface aceste nevoi.
Tot ce avem de facut in acest stadiu este sa obtinem acele produse si servicii care vor permite ca firma noastra sa prospere.

Dar cum ne vom asigura ca:

- proiectam produsele si serviciile noastre in concordanta cu cerintele clientilor ?
- furnizam servicii pe linia acestor cerinte ?
- folosim in produsele noastre numai materiale si servicii care ne fac capabili sa indeplinim aceste cerinte ?
- managementul firmei si angajatii cunosc toate cerintele si sunt instruiti in mod adecvat ?
- procesele noastre de prestare a serviciilor sunt capabile sa indeplineasca toate cerintele ?
- controlul calitatii va fi corespunzator mentinerii nivelului standardizat ?
- daca exista diferite probleme, ele pot fi identificate si corectate ?
- invatam din greselile noastre si ne dezvoltam intr-un mediu de perfectionare continua ?

Raspunsul la toate aceste intrebari este:

prin implementarea unui sistem eficient de management al calitatii.

1.3 Familia de standarde ISO 9000

ISO semnifică "International Organization for Standardization" (Organizatia Internațională de Standardizare), care este o federație mondială ai cărei membrii sunt reprezentanți aleşi din aproape 100 de organizații nationale de standardizare.Fiecare organism membru al ISO reprezintă organizația de standardizare din țara de origine. Din fiecare țară este acceptat ca membru un singur organism.
ISO este compus din 182 comitete tehnice şi 633 subcomitete, fiecare comitet având competența şi responsabilitatea unui proiect de standardizare. Secretariatul central al ISO cu sediul în Genf- Elveția, coordonează activitatea comitetelor.
ISO are ca obiectiv dezvoltarea standardizării şi facilitarea schimbului internațional de mărfuri şi servicii. Rezultatele activității ISO sunt publicate sub forma standardelor internaționale, ghidurilor sau altor documente similare.
Familia de standarde ISO 9000 este rezultatul unui îndelungat proces de evoluție care îşi are începutul în anii '50 în S.U.A..Creşterea cerințelor de calitate în domeniul militar a condus la primele reglementări de asigurare a calității. Acestea conțineau condiții referitoare la implementarea şi controlul măsurilor de asigurare a calității, structurate şi formulate după principiul aplicabilității practice. Scopul acestor reglementări a fost îmbunătățirea performanțelor calitative ale întreprinderilor.

În anul 1958, au apărut primele standarde de asigurarea calității în industria militară.
- MIL – Q – 9858 – Specificații ale sistemului calității
- MIL – L – 45208 –Cerințe ale sistemului de inspecție

Aceste standarde se utilizează şi astăzi în S.U.A. în contractele cu furnizorii de armament.

Ele au fost preluate prin filiera NATO în toate țările participante sub forma unor reglementări militare seria AQAP 1,4 şi 9 referitoare de asemenea la sistemele calității
(AQAP) şi de inspecție (AQAP 4 – Fabricație, inspecție şi încercări; AQAP 9 – Inspecții finale).
În anul 1979, Marea Britanie le-a adaptat prin intermediul BSI, pentru a fi aplicabile în întreaga economie britanică sub forma seriei de standarde voluntare BS 5750 părțile 1,2,3
(prezentarea cerințelor) şi BS 5750 părțile 4,5,6 (interpretări ale acestora).

În anul 1987, ISO le-a preluat într-o măsură aproape integrală sub forma ISO 9000, prima ediție.
În anul 1994, ISO 9001,2,3 au fost modificate şi revizuite aducându-se îmbunătățiri considerabile structurii inițiale.
În anul 2000, s-a modificat modalitatea de abordare, standardele având acum la bază modelul procesului.
Standardele 9001,9002 si 9003 au fost combinate si a rezultat un singur standard ISO 9001.
Editia din 2000 a standardului ISO 9001 a reprezentat o modificare radicala a abordarii sistemelor calitatii, trecandu-se de la asigurarea calitatii la managementul calitatii.
In 2008, ISO 9001 a fost modificat pentru a clarifica unele puncte si pentru a imbunatati compatibilitatea cu ISO 14001 standardul de referinta pentru cerintele de mediu. Nu au aparut cerinte noi.

În România, seria ISO 9000 a fost preluată şi adaptată limbii române prin intermediul CT 56 al IRS (acum ASRO) înființat în 1990.
Cele mai cunoscute standarde din seria 9000 sunt urmatoarele:

SR EN ISO 9000: 2006	Sisteme de management al calității – Principii fundamentale şi vocabular
SR EN ISO 9001: 2008	Sisteme de management al calității – Cerințe
SR EN ISO 9004: 2001	Sisteme de management al calității – Linii directoare pentru îmbunătățirea performantelor
SR EN ISO 19011: 2003	Ghid pentru auditarea sistemelor de management al calitatii si/sau de mediu

Putem afirma că seria de standarde ISO 9000 este cel mai răspândit model de conducere a unei organizații. Acceptarea universală de care se bucură standardul se datorează şi faptului că formulează numai cerințele pe care trebuie să le îndeplinească un sistem de management al calității. Modul de transpunere în practică este lăsat la latitudinea companiilor. Prin aceasta, reglementările pot fi utile oricărei organizații, indiferent de mărimea ei sau de domeniul în care activează.

CAPITOLUL 2 – TERMINOLOGIE ŞI MODELE APLICATIVE ALE CALITĂȚII

CALITATE
Măsura în care un ansamblu de caracteristici intrinseci îndeplineste cerințele.

ASIGURAREA CALITĂȚII
Parte a managementului calității concentrată pe furnizarea încrederii că cerințele referitoare la calitate vor fi îndeplinite.

CONTROLUL CALITĂȚII
Parte a managementului calității concentrată pe îndeplinirea cerințelor referitoare la calitate.

MANAGEMENTUL CALITĂȚII
Activități coordonate pentru a orienta şi controla organizația în ceea ce priveşte calitatea.

SISTEMUL DE MANAGEMENT AL CALITĂȚII
Sistem de management prin care se orientează şi se controlează o organizație în ceea ce priveşte calitatea.

POLITICA REFERITOARE LA CALITATE
Intenții şi orientări generale ale unei organizații referitoare la calitate aşa cum sunt exprimate oficial de managementul de la cel mai înalt nivel.

AUDIT
Proces sistematic, independent si documentat in scopul obtinerii de dovezi de audit si evaluarea lor cu obiectivitate pentru a determina masura in care sunt indeplinite criteriile de audit.

INSPECȚIE
Evaluare a conformității prin observare şi judecare însoțite după caz, de măsurare, încercare sau comparare cu un calibru.

PLANUL CALITĂȚII
Document care specifică ce proceduri şi resurse asociate trebuie aplicate, de cine şi când pentru un anumit proiect, produs, proces sau contract.

SPECIFICAȚIE
Document care stabileşte cerințe.

DOVADA OBIECTIVĂ
Date care susțin că ceva există sau este adevărat.

NECONFORMITATE
Neîndeplinirea unei cerințe.

AUDITOR
Persoană care are aptitudini demonstrate si competenta demonstrata de a efectuaun audit.

CLIENT
Organizație sau persoană care primeşte un produs.

FURNIZOR
Organizație sau persoană care furnizează un produs.

PROCES
Ansamblu de activități corelate sau în interacțiune care transformă elemente de intrare în elemente de ieşire.

- ***PRESCURTĂRI***
  SMQ – Sistemul de Management al Calității

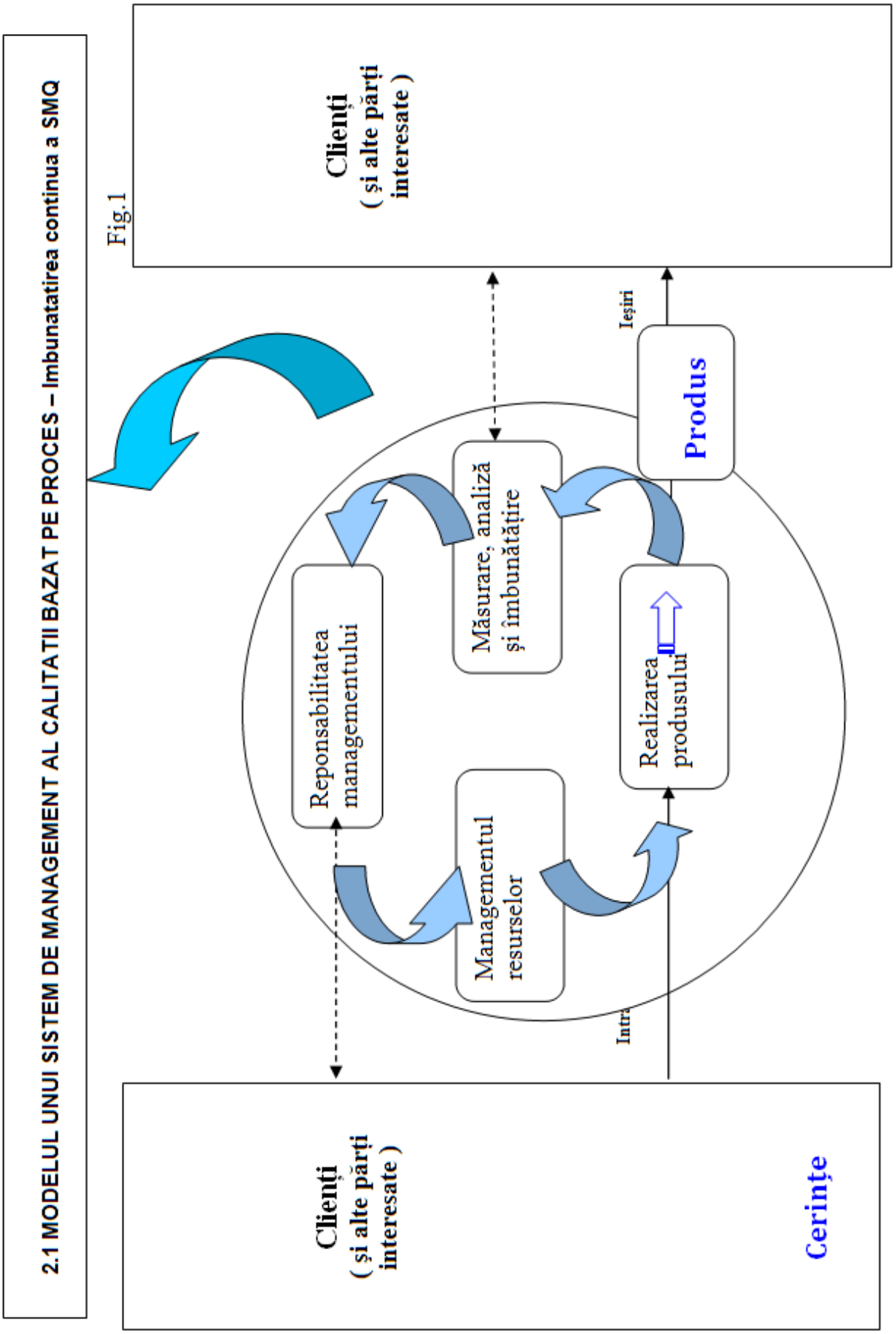
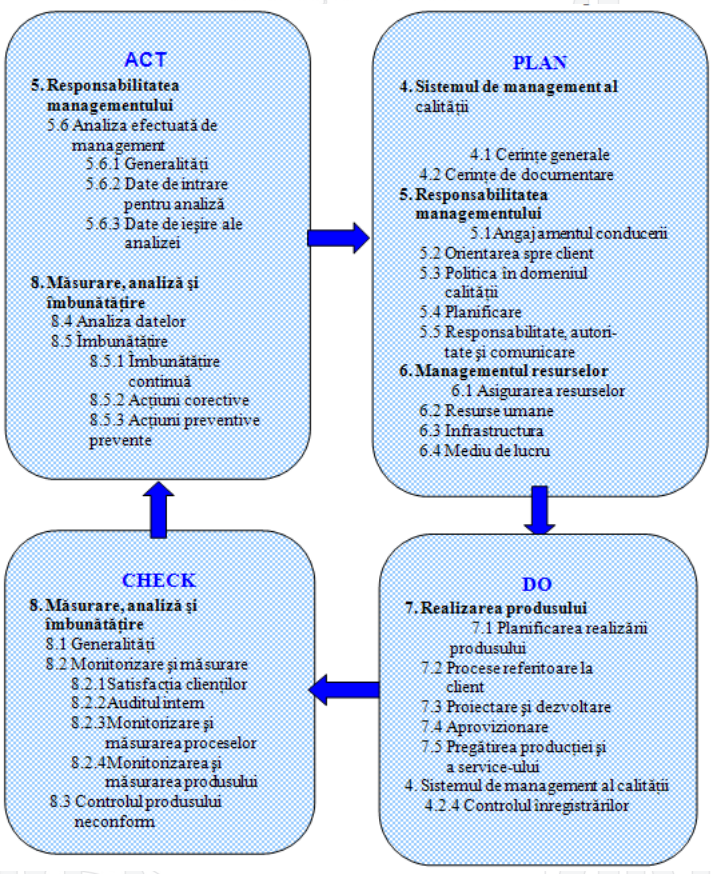

2.1 MODELUL UNUI SISTEM DE MANAGEMENT AL CALITATII BAZAT PE PROCES – Imbunatatirea continua a SMQ
Clienți
(și alte părți interesate)
Ieșiri
Produs
Măsurare, analiză și îmbunătățire
Reponsabilitatea managementului
Realizarea produsului
Managementul resurselor
Intrări
Clienți
(și alte părți interesate)
Cerințe

Fig.1

Fig.1

2.2 Imbunatatirea continua a unui proces (ROATA LUI DEMING)

Fig.2



P - Plan (planifica) – stabileste obiectivele si procesele necesare obtinerii rezultatelor in concordanta cu cerintele clientului si cu politicile organizatiei

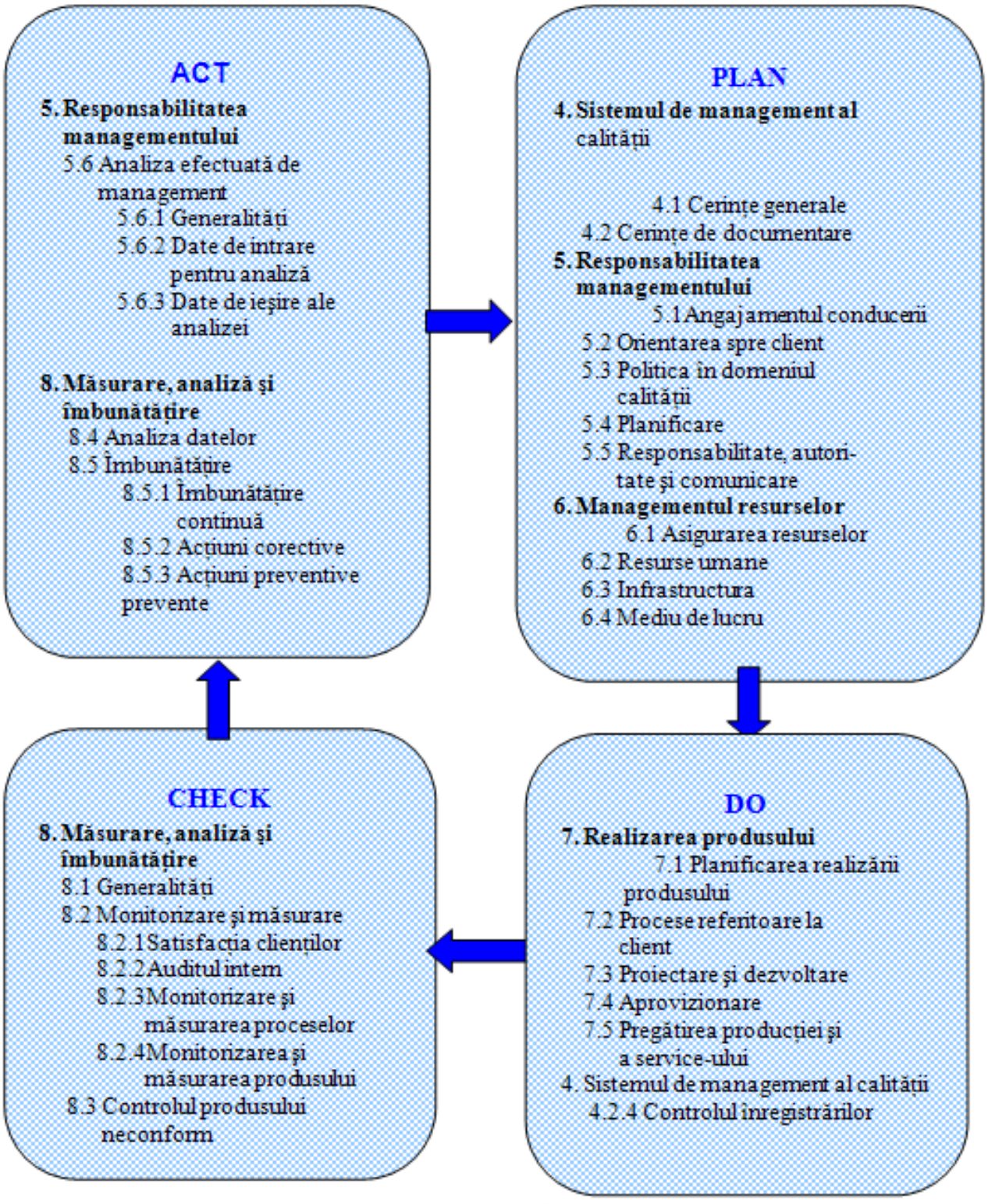
D - Do (efectueaza) – implementeaza procesele

C - Check (verifica) – monitorizeaza si masoara procesele si produsul fata de politicile, obiectivele si cerintele pentru produs si raporteaza rezultatele

A - Act (actioneaza) – intreprinde actiuni pentru imbunatatirea continua a performantelor proceselor

Adoptarea unui SMQ ar trebui sa fie o decizie strategica a unei organizatii. Pentru ca o organizatie sa fie eficienta trebuie sa identifice si sa conduca numeroase activitati corelate.
Aplicarea unui sistem de procese in cadrul unei firme, impreuna cu identificarea si interactiunile acestor procese, precum si conducerea lor poate fi considerata „abordare bazata pe proces”
Modelul unui SMQ bazat pe proces prezentat in fig.1 ilustreaza legaturile intre procesele la care se refera cerintele din capitolele 4 pana la 8 ale standardul ISO 9001:2008 (vezi fig. 3)
Fig. 1 arata rolul semnificativ pe care clientii il joaca in definirea cerintelor ca elemente de intrare. Monitorizarea satisfactiei clientului necesita evaluarea informatiilor referitoare la perceptia clientului asupra faptului ca organizatia a satisfacut cerintele sale.

PDCA ISO 9001- 2008 CERINTE Fig. 3



NOTĂ: Numerotarea corespunde capitolelor standardului ISO 9001-2008

CAPITOLUL 3 – PRINCIPII ALE MANAGEMENTULUI CALITATII

- **Orientarea către client**
- **Leadership**
- **Implicarea personalului**
- **Abordarea bazată pe proces**
- **Abordarea managementului ca sistem**
- **Îmbunătățirea continuă**
- **Abordarea bazată pe fapte pentru luarea deciziilor**
- **Relații reciproc avantajoase cu furnizorii**

- ***Orientarea către client***

Organizațiile depind de clienții lor şi de aceea trebuie să înțeleagă nevoile curente şi viitoare ale clienților, să îndeplinească cerințele acestora şi să le depăşească aşteptările.

Clienții ştiu să aprecieze managementul calității după cum:
- Primesc la timp produsele/serviciile;
- Produsele/serviciile răspund cerințelor lor explicite şi implicite;
- Recurg la reclamații mult mai rar.

- ***Leadership***

Conducătorii stabilesc sensul, direcția şi mediul intern al unei organizații. Ei crează mediul adecvat în care oamenii pot deveni pe deplin implicați în atingerea obiectivelor organizației.

Managementul calității este o problemă colectivă dar conducerea organizației este responsabilă pentru crearea premiselor procesului de îmbunătățire a calității; ea însăşi trebuie să participe activ în acest proces şi să stimuleze totodată implicarea tuturor angajaților.

- ***Implicarea personalului***

Oamenii de la toate nivelurile sunt esența unei organizații şi implicarea lor totală face posibilă utilizarea abilităților lor pentru beneficiul maxim al organizației.

Nu numai clienții vor profita de sistematizarea proceselor din interiorul organizației şi de creşterea eficienței generată de aceasta. În egală măsură, managementul calității aduce schimbări în bine şi pentru angajați. În acest sens, creşterea nivelului profitului aduce, pe lângă posibilitatea creşterii nivelului veniturilor salariale şi creşterea implicării organizației din punct de vedere social. (contracte de muncă speciale, grădinițe pentru copiii salariaților, sponsorizări pentru continuarea studiilor etc). Principial, fiecare angajat este integrat în acest sistem. Un sistem de management al calității asigură transparența firmei. Procesele şi responsabilitățile sunt clar definite. Fiecare angajat îşi cunoaşte locul pe care îl ocupă în cadrul acestor procese. El devine conştient de importanța sa ca parte componentă a întregului sistem şi de răspunderea pe care o poartă pentru calitatea produselor şi serviciilor, pentru succesul firmei.

Fiecare angajat care cunoaşte sensul muncii sale şi se poate identifica cu aceasta, îşi va îndeplini bine obligațiile. Cine constată că inițiativele şi propunerile sale de eficientizare sunt luate în serios, va participa activ la procesul de ameliorare a calității.

Managementul calității trebuie să asigure transpunerea în practică de către angajați a obiectivelor firmei şi ale calității. Aceasta garantează bunul mers al afacerii – dar nu ”într-un fel sau altul”, ci conform planificării “conştiente “.

- ***Abordarea bazată pe proces***

Rezultatul dorit este atins mai eficient atunci când resursele şi activitățile care au legătură între ele sunt administrate ca fiind un proces.

Funcționarea eficace a unei organizații este determinată de identificarea şi conducerea a numeroase activități corelate. O activitate care este condusă astfel încât să permită transformarea elementelor de intrare în elemente de ieşire este considerată *un proces.*

- ***Abordarea managementului ca sistem***

Identificarea, înțelegerea şi administrarea unui sistem de procese interdependente pentru atingerea unui obiectiv dat, contribuie la eficacitatea şi eficiența unei organizații.

Sistemul se defineşte ca fiind un ansamblu de elemente aflate în corelație sau interacțiune, în cazul de față un ansamblu integrat, format din unul sau mai multe procese, hardware, software, infrastructură şi oameni, care furnizează o capabilitate de a satisface o necesitate sau un obiectiv specificat.

- ***Îmbunătățirea continuă***

Obiectivul permanent al organizației este îmbunătățirea continuă.

Îmbunătățirea continuă se referă la acțiuni întreprinse pentru sporirea trăsăturilor şi caracteristicilor produselor / serviciilor şi / sau creşterea eficacității şi eficienței proceselor utilizate pentru producerea şi livrarea lor.

Astfel de acțiuni includ următoarele:

- definirea, măsurarea şi analizarea situației existente;
- stabilirea obiectivelor pentru îmbunătățire;
- căutarea soluțiilor posibile;
- implementarea soluțiilor selectate;
- măsurarea, verificarea şi analizarea rezultatelor implementării;
- oficializarea schimbărilor.

- **Abordarea bazată pe fapte pentru luarea deciziilor**

Deciziile eficace se bazează pe analiza logică şi anticipativă a datelor şi informațiilor.

Analiza logică şi anticipativă trebuie întreprinsă în mod sistematic şi documentat pentru a se asigura că subiectul în discuție este potrivit, adecvat, eficace şi eficient pentru îndeplinirea obiectivelor stabilite.

- **Relații reciproc avantajoase cu furnizorii**

Capacitatea organizației de a crea valoare este mărită de existența unor relații reciproc benefice cu furnizorii.

Furnizorul este definit ca partea care este responsabilă pentru un produs, proces sau serviciu. Definiția poate fi aplicată fabricanților, distribuitorilor, importatorilor, montatorilor, furnizorilor de servicii, interni sau externi organizației.

CAPITOLUL 4 – ISO 9001- 2008 PREZENTAREA CERINȚELOR

ISO 9001 specifica cerinte pentru un SMQ atunci cand o organizatie are nevoie sa-si demonstreze abilitatea de a furniza produse care indeplinesc cerintele clientului si ale reglementarilor aplicabile si urmareste sa creasca satisfactia clientului.

Sistemele de management al calitatii pot ajuta organizatiile la cresterea satisfactiei clientului.

Clientii solicita produse cu caracteristici care sa le satisfaca necesitatile si asteptarile.
Aceste necesitati si asteptari sunt exprimate in specificatiile produsului si sunt mentionate prin termenul generic de cerinte ale clientului.
Cerintele clientului pot fi specificate contractual de catre client sau pot fi determinate de organizatia insasi. In oricare din cazuri, clientul decide in ultima instanta acceptarea produsului.
Deoarece necesitatile si asteptarile clientului se schimba si datorita presiunilor competitiei si progresului tehnic, organizatiile sunt determinate sa-si imbunatateasca continuu produsele si procesele.

Abordarea SMQ incurajeaza organizatiile:

- sa analizeze cerintele clientului
- sa defineasca procesele care contribuie la realizarea unui produs acceptabil pentru client
- sa tina procesele definite sub control

Un SMQ poate:

- ✓ furniza cadrul pentru imbunatatirea continua pentru a mari probabilitatea de crestere a satisfactiei clientului
- ✓ furniza incredere organizatiei si clientilor sai ca este capabila sa ofere produse care indeplinesc in mod consecvent cerintele

Standardele din familia ISO 9000 fac distinctie foarte clara intre cerintele pentru SMQ si cerintele pentru produse.

Cerintele pentru sistemele de management al calitatii sunt specificate in ISO 9001.
Aceste cerinte sunt generice si aplicabile organizatiilor din orice sector industrial sau economic indiferent de categoria de produse oferite.

ISO 9001 nu stabileste cerinte pentru produse

CAPITOLUL 5 – ETAPE PENTRU DEZVOLTAREA SI IMPLEMENTAREA SMQ

O abordare a dezvoltarii si implementarii unui SMQ consta din mai multe etape care include urmatoarele:

a) determinarea necesitatilor si asteptarilor clientilor si ale altor parti interesate
b) stabilirea politicii si obiectivelor organizatiei referitoare la calitate
c) determinarea proceselor si responsabilitatilor necesare pentru a atinge obiectivele calitatii
d) determinarea si asigurarea resurselor necesare in scopul realizarii obiectivelor calitatii
e) stabilirea metodelor de masurare a eficacitatii si eficientei fiecarui proces
f) aplicarea acestor masurari pentru a determina eficacitatea si eficienta fiecarui proces
g) determinarea mijloacelor de prevenire a neconformitatilor si de eliminare a cauzelor acestora
h) stabilirea si aplicarea unui proces pentru imbunatatirea continua a SMQ

O organizatie care adopta modul de abordare de mai sus genereaza incredere in capabilitatea proceselor sale si in calitatea produselor sale si asigura o baza pentru imbunatatirea continua. Aceasta poate sa conduca la cresterea satisfactiei clientilor si a altor parti interesate si la succesul organizatiei.

CAPITOLUL 6 – DOCUMENTELE SISTEMULUI DE MANAGEMENT AL CALITĂȚII

6.1 GENERALITĂȚI

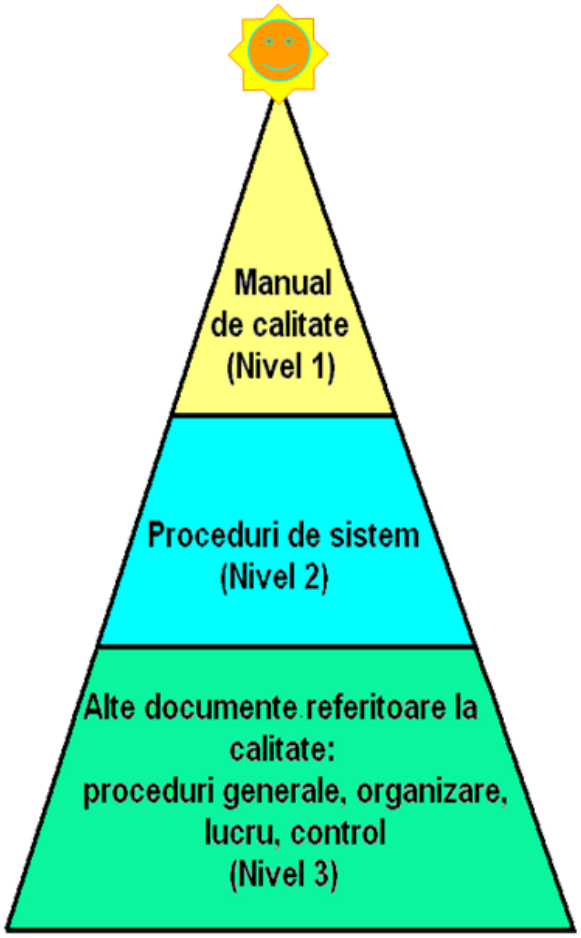
Documentele unui sistem de management al calității descriu structura organizației şi modul de funcționare.

Un sistem de management al calității este unic pentru fiecare organizație. Din această cauză, standardele internaționale nu intenționează să definească o structură, o formă, un conținut sau o metodă de prezentare unice pentru descrierea elementelor sistemului calității care pot fi aplicate tuturor produselor / serviciilor. Gradul de detaliere, responsabilitățile, autoritățile, precum şi ierarhizarea acestor documente sunt determinate de situația concretă a fiecărei organizații. Ierarhia tipică a documentelor sistemului calității este prezentată la pagina următoare.

Este obligatoriu ca fiecare document al SMQ să fie aprobat de persoanele cu responsabilități pe nivelul respectiv, cu scopul de a se asigura claritatea, exactitatea, adecvarea şi structura corespunzătoare. De regulă, cu cât nivelul documentației este mai ridicat, cu atât autoritatea care aprobă trebuie să fie mai înaltă.

De-a lungul duratei de viață a unui document vor apărea necesități de schimbare a conținutului. Documentele depăşite sau care nu mai sunt necesare trebuie eliminate din sistemul de documente pentru a preveni folosirea lor inadecvată. Controlul emiterii şi al modificării documentelor este esențial pentru a se asigura că este autorizat în mod adecvat conținutul documentului. Schimbările trebuie controlate de persoanele care au creat originalul sau de personal autorizat care are acces la informații adecvate pe baza cărora s-a creat originalul.

6.2 IERARHIA TIPICĂ A DOCUMENTELOR SISTEMULUI DE MANAGEMENT AL CALITĂȚII



Politica referitoare la calitate

Conținutul documentelor

Descrie sistemul calității în conformitate cu politica managementului în domeniul calității şi cu obiectivele stabilite, precum şi cu standardul aplicat.

Descriu activitățile unităților funcționale individual necesare pentru implementarea elementelor sistemului calității.

Constau din elemente de lucru detaliate.

- **Politica referitoare la calitate**

Acest document este o declarație a managementului de la cel mai înalt nivel, în general semnată de directorul general. Poate conține de la 2-3 propoziții la 2-3 pagini, în toate cazurile ea reprezentând dovada angajării conducerii pe drumul calității.

- **Manualul calității**

Scopul manualului este de a informa personalul despre politica managementului şi despre obiectivele calității. În plus el poate informa clienții sau potențialii clienți despre modul în care este asigurată calitatea în cadrul organizației.

Manualul conține ca cerințe minimale ale ISO: domeniul de aplicare al sistemului de management al calității, inclusiv detalii şi justificări ale oricăror excluderi, procedurile de sistem ale sistemului de management al calității sau o referire la acestea şi o descriere a interacțiunii dintre procesele sistemului de management al calității.

Manualul face de asemenea legături între politica şi obiectivele organizației şi cerințele standardului precum şi cine este responsabil pentru atingerea acestor obiective.

Deoarece manualul este deseori folosit ca un ajutor în promovarea imaginii organizației, el conține informații de prezentare a acesteia, despre produsele şi serviciile oferite.

- **Manualul de proceduri**

Scopul procedurilor este de a instrui angajații asupra modului în care politica conducerii, aşa cum este descrisă în manualul calității, va fi pusă în aplicare.
Manualul de proceduri va fi format din una sau mai multe proceduri legate direct de fiecare afirmație făcută în manualul calității. Ele vor defini modul în care grupuri de angajați din acelaşi departament sau din departamente diferite vor colabora pentru a îndeplini obiectivele de calitate stabilite de management.

Procedurile trebuie să atingă fiecare cerință a clauzelor relevante din cadrul standardelor. Puse la un loc, procedurile vor arăta cum acționează o organizație pentru a transforma cererea inițială în produs finit sau serviciu.

- **Instrucțiuni de lucru**

Scopul instrucțiunilor de lucru este de a furniza o descriere detaliată a operațiilor sau a activităților specifice pentru un produs sau serviciu.
Aceste documente pot fi: modele, metode de lucru şi verificare cu aparate, desene, imagini, fluxuri de inspecție etc. Esențial de subliniat este faptul că aceste documente nu provin absolut necesar din interiorul organizației, ele pot fi furnizate de către client.

- **Înregistrări şi formulare**

Scopul înregistrărilor şi formularelor este de a putea demonstra că un produs / serviciu a fost realizat în conformitate cu cerințele specificate şi deci dovedesc operaționalitatea sistemului calității.
Documentele de la acest nivel se constituie ca probe pentru activitățile ce au fost executate la alte nivele. În general, pentru un auditor ele furnizează dovezile necesare că organizația îşi atinge obiectivele declarate.

Aceste documente pot fi variate, dar cele mai comune sunt:

1 Rapoarte de audit, contracte, NIR-uri, fişe de verificare, rapoarte de încercări etc.
2 Înregistrări ale cerințelor ISO 9001 (Procese verbale ale analizelor managementului, liste ale furnizorilor acceptați, înregistrări ale cursurilor de instruire etc.).

- **Planul calității**

" Un document care stabileşte practicile specifice referitoare la calitate, resursele şi activitățile legate de un proiect, produs, contract sau obiectiv "

Planul calității face de obicei referire la procedurile existente dar necesită documente suplimentare, rapoarte de inspecție şi autorizații ale personalului.

6.3 PROCEDURI SI INSTRUCTIUNI

6.3.1 Definitia procedurii si tipuri de proceduri

O procedura (conform ISO9000/2005) este **"un mod specificat de desfasurare a unei activitati sau a unui proces"**
Fiecare organizatie isi proiecteaza propriul model de proceduri. O procedura este particularizata prin format, structura si continut.
Formatul nu este impus de nici o reglementare scrisa sau nescrisa. Experienta a demonstrat ca nu forma asigura eficacitatea unei proceduri, ci continutul acesteia.
Continutul unei proceduri are doar constrangeri dictate de eficienta utilizarii ei: trebuie sa fie clar, usor de inteles si de pus in practica, sa prezinte actiunile in ordinea lor fireasca, suficient de detaliat pentru

a putea fi aplicate fara retinere, cu responsabilitatile bine definite, cu descrierea exacta a metodelor de lucru si de control, sa stabileasca modul de prezentare sau confirmare a rezultatelor, sa prezinte inregistrarile aplicabile.

Trebuie reamintit ca standardul ISO 9001/2008 impune fara echivoc procedurarea urmatoarelor sase procese:

- Controlul documentelor (4.2.3)
- Controlul înregistrărilor (4.2.4)
- Auditul intern (8.2.2)
- Controlul produsului neconform (8.3)
- Acțiune corectiva (8.5.2)
- Acțiune preventiva (8.5.3)

Procedurile pot fi cu caracter general, precum cele de mai sus, aplicabile intregului SMQ (proceduri generale sau de sistem), pot fi aplicabile anumitor "zone" ale sistemului (proceduri operationale) sau unui singur process simplu (proceduri de lucru).

6.3.2 Structura unei proceduri

O procedura trebuie sa aiba o structura care sa descrie cat mai clar si complet activitatea sau procesul vizat.

Trebuie retinut ca procedura, pentru a fi eficace trebuie sa raspunda la intrebarile clasice:

- **Ce ?** - Ce trebuie facut ?
- **Unde ?** - Unde trebuie facut ?
- **Cine ?** - Cine trebuie sa faca ?
- **Cum ?** - Cum trebuie sa faca ?
- **Cand ?** - Cand trebuie sa faca ?
- **De ce ?** - De ce trebuie sa faca ?

In general practica a demonstrat ca o procedura trebuie sa contina capitolele:

- **Scopul procedurii** – Se precizeaza scopul activitatii/procesului care se procedureaza
- **Domeniul de aplicare** – Se precizeaza limitele de aplicativitate ale procedurii
- **Documente de referinta si conexe**: Se enumera toate documentele pe baza carora s-a elaborat procedura, precum si elementele de legislatie, specificatii si coduri aplicabile. Pentru procedurile de lucru trebuie amintit si manualul calitatii dar si procedurile SMQ care apeleaza activitatea procedurata. Se enumera procedurile conexe cu procedura descrisa, in cazul in care acestea exista.
- **Definitii si prescurtari aplicabile** – Se precizeaza termenii si abrevierile apelate in procedura
- **Responsabilitati** – Se precizeaza cine si pentru ce este responsabil, adica atributiile personalului, sectiilor, compartimentelor, referitoare la activitatea procedurata.
- **Procedura propriu-zisa**: Se precizeaza cum, cand, unde si de ce se executa activitatea sau operatia procedurata, modul in care este condusa, monitorizata si masurata. Se enumera, in ordine logica, ceea ce este necesar sa fie efectuat pentru a atinge scopul procedurii. Se pot face trimiteri la alte proceduri care preiau detalii din activitatea sau operatia procedurata.

Este indicat sa se introduca paragrafe care sa descrie problemele de protectie a mediului, de sanatate si securitate a muncii specifice activitatii/procesului procedurat, pentru a veni in intampinarea viitoarelor abordari ale managementului organizatiei.

- **Inregistrari** - Se enumera formularele apelate prin procedura, specificand codul formularului, denumirea inregistrarii, alte caracteristici definitorii (emitent, perioada de pastrare etc.)
- **Anexe -** Cuprinde formulare anexe, organigrame, scheme logice, schite etc. precum si amprentele stampilelor si etichetele utilizate.

6.3.3 Instructiuni tehnologice de lucru

Acestea sunt proceduri al caror scop este descrierea in detaliu a modului de desfasurare a unei activitati sau proces de productie.
Ele trebuie sa fie redactate clar, coerent si sa cuprinda toate informatiile necesare pentru desfasurarea in bune conditii a activitatii respective.
Instructiunea va respectat firesc structura unei proceduri.
O instructiune trebuie scrisa in asa fel incat orice persoana calificata corespunzator sa poata executa operatia descrisa fara probleme urmarind instructiunea respectiva.

O instructiune este eficienta daca aplicarea ei este usoara si nu genereaza intrebari sau, si mai rau, incurcaturi.

Dupa elaborare si aprobare este indicat ca instructiunea sa fie implementata imediat, pentru o scurta perioada de proba. Astfel se pot corecta eventualele deficiente cu sprijinul direct al utilizatorilor.

BIBLIOGRAFIE

SR EN ISO 9000: 2006	*Sisteme de management al calității – Principii fundamentale şi vocabular*
SR EN ISO 9001:2008	*Sisteme de management al calității – Cerințe*
Niculae Hertog	*Procedura completa de implementare ISO9001- acum simpla si rapida*
Mike Mirams si Paul McElheron	*Certificarea ISO 9000*

COMUNICAREA INTERPERSONALA
COMUNICAREA EFICIENTA IN CADRUL UNEI ECHIPE

Întocmit: Ing.Adrian Mihai VASU

Desi comunicarea este o caracteristica fundamentala e existentei, oamenii nu se preocupa de modul in care comunica – fie ca sunt prea ocupati, fie ca nu au timp pentru lucruri atat de "neimportante".

Statisticile spun ca:

- peste 65 % din fiecare zi de munca se petrece discutand si ascultand;
- peste 70% din ceea ce auzim auzim inexact;
- peste 75% din ceea ce auzim cu precizie uitam in 3 saptamani.

COMUNICAREA – este transmiterea unui mesaj de la un emitator la un receptor.
MESAJ – ideea , informatia care trebuie transmisa receptorului
EMITATOR – RECEPTOR: comunicarea implica prezenta a cel putin doua persoane, fara de care nu are sens.

Comunicarea umana "fata in fata" are 3 componente distincte:

- ✓ continut sau cuvinte exprimate;
- ✓ tonul vocii;
- ✓ limbajul trupului (gesturi, contact vizual, pozitia corpului etc).

Exista diferite pareri asupra procentelor in care cele trei componente influenteaza receptarea mesajului. Ce este important de retinut: un procent extrem de mare din semnificatia mesajului receptionat, dupa unii specialisti chiar de 50-55%, este data de limbajul trupului (in cazul transmiterii de sentimente sau atitudini).
De aceea voi enumera cateva reguli pentru utilizarea comunicarii non-verbale (limbajul trupului):

- adaptarea posturii (pozitia corpului) la aceea a interlocutorului;
- orientarea corpului spre interlocutor (vis-à-vis);
- contactul vizual (nu lasati capul in piept si nici nu va uitati in alta parte);
- evitarea incrucisarii mainilor si a picioarelor;
- atingerea cotului, strangerea mainii sau o usoara bataie pe spate indica intentii de apropiere, cooperare.

Comunicarea poate fi:

- ✓ **scrisa**
- ✓ **verbala**
- ✓ **non-verbala**.

Pasii procesului de comunicare:

1. Expeditorul (emitatorul) **codifica** mesajul – decide exact ce vrea sa comunice si alege cu grija limbajul potrivit;
2. Expeditorul **trimite** mesajul in cea mai adecvata forma: scrisa, verbala, non-verbala;
3. Destinatarul (receptorul) **primeste** mesajul – el filtreaza comunicarea pentru a inlatura elementele perturbatoare (denaturarile);
4. Destinatarul **decodifica** mesajul pe baza experientei anterioare, a unor puncte de vedere personale, cunostinte, stari emotionale, preferinte.

Scopul fiecarui proces de comunicare este de a ajunge la o intelegere reciproca cu ascultatorul.

Desi teoretic suna foarte frumos ce am scris mai sus referitor la pasii procesului de comunicare, exista cateva adevaruri fundamentale aplicabile in procesul de comunicare de care este foarte important sa tinem cont:

- Mesajele transmise nu sunt intotdeauna si primite;
- Doua persoane nu interpreteaza acelasi mesaj in acelasi fel (sau acelasi mesaj nu are aceeasi semnificatie pentru doua persoane);
- Sensul unui mesaj este in intelect (in minte), nu in cuvintele sau simbolurile utilizate;
- Simbolurile alese pentru a comunica nu sunt perfecte; cuvintele pot avea intelesuri diferite.

Transmiterea mesajului

Pentru a transmite cat mai bine un mesaj este necesar sa stabiliti:

- CE doriti sa spuneti – trebuie sa stabiliti obiectivele comunicarii;
- CUI doriti sa spuneti – e bine sa abordati persoana cea mai potrivita, de care depinde sau care poate sa va ajute in rezolvarea unei probleme;
- CAND veti transmite mesajul – alegeti momentul cel mai bun pentru a aborda subiectul;
- UNDE veti transmite mesajul – alegeti locul potrivit, astfel incat mesajul sa fie receptat pe cat posibil fara perturbari;
- CUM veti transmite mesajul – alegeti cuvintele potrivite si forma cea mai potrivita.

Receptarea mesajului

O greseala extrem de des intalnita in comunicare:
Expeditorul trimite mesaje si presupune ca ascultatorul sau cititorul intelege semnificatia a ceea ce s-a incercat sa se comunice. Cei mai multi expeditori (emitatori) nu verifica daca mesajul a fost bine primit. Daca punem intrebari sau permitem comentarii si sugestii, inseamna ca reusim sa verificam si sa echilibram procesul comunicarii.

In realitate lucrurile stau cam asa:

100%---------- →10%
EMITATOR RECEPTOR
100% Ce vrea sa comunice
90% Ce se gandeste sa spuna
80% Ce stie sa spuna
70% Ce spune efectiv
Ce asteapta 60%
Ce asculta 50%
Ce intelege efectiv 40%
Ce admite 30%
Ce retine 20%
Ce va spune 10%

Am realizat mai sus o reprezentare sugestiva a factorilor care pot afecta eficienta comunicarii, constituind BARIERE IN COMUNICARE.

Pentru a imbunatati receptia unui mesaj putem folosi ASCULTAREA ACTIVA.
Se stie ca oamenii asculta de 4 ori mai rapid decat vorbesc. Pentru a deveni un bun ascultator, trebuie sa invatam sa ne folosim viteza de ascultare cat mai eficient. Exista cateva reguli simple ale tehnicii de ascultare activa:

- Incurajati interlocutorii sa vorbeasca aratandu-le interes, zambind si dand semne aprobative;

- Evitati distragerile din afara;
- Opriti-va din ceea ce faceti si acordati vorbitorului intreaga atentie (puneti-va mobilul deoparte pe SILENT);
- Permiteti celor cu care vorbiti sa termine ideea inceputa. Nu ii intrerupeti, nu anticipati ceea ce vi se va spune, nu trageti concluzii;
- Fiti atenti la comunicarea nonverbala ca sa intelelgeti mai bine mesajul real;
- Cereti explicatii daca o informatie lipseste sau nu este suficient de clara;
- Incercati sa va puneti in locul vorbitorului ca sa percepeti problema din perspectiva lui;
- Repetati ce s-a spus cu cuvintele dvs. (parafrazati), ca sa fiti siguri ca ati inteles corect ceea ce s-a spus.

Reactia de FEED–BACK

In procesul comunicarii indivizii primesc o multitudine de informatii dintre care unele sunt reactii legate de propriul comportament. Fenomenul de feed-back poate oferi fiecaruia o sansa de a invata sa foloseasca reactiile celorlalt ca pe o oglinda in care se reflecta rezultatele propriului comportament.

Feed-back-ul este o modalitate prin care fiecare poate deveni mai constient de ceea ce face , cum face; astfel putem deveni mai eficienti in relatia cu ceilalti. Este important sa oferim feed-back (raspuns / reactie) la cele ascultate.
Exista o serie de factori prin care putem imbunatati rezultatele FEED-BACK-ului atat la emitator, cat si la receptor. Astfel reactia de feed-back trebuie:

- Sa se refere in primul rand la comportament si nu la persoana;
- Sa se bazeze pe observatii directe si nu pe supozitii;
- Sa se concentreze pe descriere si nu pe judecati;
- Sa se refere la o situatie concreta (AICI si ACUM) si nu teoretic la comportamentul in general (ACOLO si ATUNCI);
- Sa caute alternative mai curand decat sa reprezinte solutii sau decizii;
- Sa se concentreze pe valoarea pe care o poate avea pentru cel care o primeste si nu pe importanta mentionata de cel care o ofera;
- Sa cuprinda cantitatea de informatii pe mcare receptorul este in stare sa o primeasca si nu tot ceea ce poate fi oferit;
- Sa fie oferita la momentul si locul potrivit;
- Sa se refere la ceea ce s-a spus si nu la motivul pentru care s-a spus.

O forma importanta de comunicare este COMUNICAREA PRIN TELEFON.

Telefonul este un mijloc de comunicare folosit foarte frecvent.
Folosirea eficienta a telefonului are în vedere:

- Pregatirea mesajului: înseamna sa realizam o detasare de la problemele care ne preocupau pana în acel moment si definirea prealabila a subiectului convorbirii, obiectivul conversatiei. Într-o conversatie telefonica se includ numai 2-3 idei principale;
- Pregatirea pentru apelul telefonic: sa ne gandim la tonul si atitudinea pe care vom adopta, sa avem o pozitie comoda. Vom vorbi mai rar decat in mod obisnuit, dar nu trebuie sa vorbim tare, ci direct în telefon;
- Prezentarea corecta a mesajului: trebuie sa evitam cuvintele si formularile negative si sa prezentam clar si la obiect mesajul;
- Ascultarea interlocutorului: se asculta cu mare atentie ce ni se spune, iar daca acesta se opreste un timp, nu trebuie întrerupt, se va lasa timp de gandire;
- Concluzia convorbirii: la sfarsitul convorbirii se reformuleaza concluzia la care s-a ajuns. Convorbirea trebuie încheiata întotdeauna într-un climat amical, indiferent de rezultatul ei.

Forme de COMUNICARE SCRISA

Comunicarea scrisa, alaturi de cea verbala, reprezinta o componenta a comunicarii umane. Caracteristicile mesajului scris sunt urmatoarele:

- anumite restrictii de utilizare;
- sa fie conceput explicit;
- implica un control exigent privind informatiile, faptele si argumentele folosite;
- poate fi exprimat sub diferite forme;
- este judecat dupa fondul si forma textului.

Un indicator care caracterizeaza comunicarea scrisa este lizibilitatea (lizibil = a putea fi citit cu usurinta). Pentru acest aspect se recomanda metoda FLESCH, care consta în calculul lungimii medii a propozitiei si al numarului mediu de silabe pentru fiecare 100 de cuvinte. Pentru textele normale care trebuie citite si întelese de 83% dintre oameni, media lungimii propozitiei trebuie sa fie de 15-17 cuvinte, cu 147 silabe la 100 de cuvinte.

Am enumerat mai jos cateva forme de comunicare scrisa, mai des folosite in firme:

- Procesul verbal – reprezinta un document oficial în care se înregistreaza o anumita constatare sau se consemneaza pe scurt discutiile si hotararile unei anumite adunari.
- Minuta – este un document care consemneaza anumite lucruri, asemanandu-se cu procesul verbal de constatare. Se deosebeste de acesta prin faptul ca aceasta din urma înregistreaza si propuneri sau actiuni întreprinse la un moment dat care urmeaza a fi completate ulterior.
- Referatul – este documentul scris în care sunt prezentate aspecte concrete, date si aprecieri în legatura cu o anumita problema, precum si propuneri de modificare a situatiei existente. Structura sa este compusa din: prezentarea succinta a problemei abordate; concluzii si propuneri; semnatura.
- Raportul – cuprinde o relatare a unei activitati (personale sau de grup). Se face din oficiu sau la cererea unui organ ierarhic. Se bazeaza pe cercetari amanuntite, schimburi de experienta, diverse documentari.

Tehnicianul de securitate este de multe ori sef de echipa sau sef de lucrare sau chiar sef de departament intr-o firma de instalare de sisteme de securitate. In acest sens, pentru a realiza un proces de comunicare eficient, trebuie sa asigure:

- o comunicare reala cu subordonatii sai (membrii echipei);
- o ascultare activa a membrilor echipei;
- o informare corecta a membrilor echipei care presupune transparenta si utilizarea numai a informatiilor corecte cat si o circulatie rapida a informatiei.

Seful de echipa trebuie:

- sa asigure un climat de comunicare adecvat;
- sa fie obiectiv;
- sa evite contrazicerile directe si cearta;
- sa dea raspunsuri clare si la obiect pentru a evita neîntelegerile;
- sa comunice membrilor echipei schimbarile care se fac si sa tina cont si de parerile acestora;
- sa evite monopolizarea discutiei;
- sa protejeze membrii echipei de zvonuri si barfe;
- sa ofere argumente rationale in procesul de comunicare.

Un sef de echipa competent si corect stie sa comunice cu fiecare membru al echipei, individual, si stie totodata sa-si tina promisiunile facute.

ASPECTE LEGISLATIVE PRIVIND APĂRAREA ÎMPOTRIVA INCENDIILOR.

SISTEME DE SECURITATE LA INCENDIU.

SUPRAVEGHEREA PIEȚEI

1. Aspecte legislative privind apărarea împotriva incendiilor

Apărarea împotriva incendiilor reprezintă ansamblul integrat de activităţi specifice, măsuri şi sarcini organizatorice, tehnice, operative, cu caracter umanitar şi de informare publică, planificate, organizate şi realizate potrivit prezentei Legii nr. 307/2006, în scopul prevenirii şi reducerii riscurilor şi asigurării intervenţiei operative pentru limitarea şi stingerea incendiilor în vederea evacuării, salvării şi protecţiei persoanelor periclitate, protejării bunurilor şi mediului împotriva efectelor situaţiilor de urgenţă determinate de incendii.

Activitatea de apărare împotriva incendiilor constituie o activitate de interes public, naţional, cu caracter permanent, la care sunt obligate să participe, autorităţile administraţiei publice centrale şi locale, precum şi toate persoanele fizice şi juridice aflate pe teritoriul României.

Coordonare, controlul şi acordarea asistenţei tehnice de specialitate în domeniul apărării împotriva incendiilor se asigură de Ministerul Internelor şi Reformei Administrative, la nivel central prin Inspectoratul General pentru Situaţii de Urgenţă, iar la nivel local prin inspectoratele judeţene pentru situaţii de urgenţă şi al Municipiului Bucureşti.

Aşa cum am precizat anterior actul normativ care reglementează la nivelul ţării noastre apărarea împotriva incendiilor este Legea nr. 307/2006 privind *apărarea împotriva incendiilor.*

Actele normative, de interes, subsecvente acestei legi sunt:

- HGR nr. 1.739/2006 pentru aprobarea categoriilor de construcţii şi amenajări care se supun avizării şi/sau autorizării privind securitatea la incendiu.
- HGR nr. 537/2007 privind sancţionarea contravenţională în domeniul apărării împotriva incendiilor.
- OMAI nr. 712/2005 pentru aprobarea Dispoziţiilor generale privind instruirea salariaţilor în domeniul situaţiilor de urgenţă modificat şi completat cu OMAI 786/2005.
- OMAI nr. 130/2007 pentru aprobarea Metodologiei de elaborare a scenariilor de securitate la incendiu.
- OMAI nr. 163/2007 pentru aprobarea normelor generale de apărare împotriva incendiilor.
- OMIRA nr. 252/2007 pentru aprobarea Metodologiei de atestare a persoanelor care proiectează, execută, verifică, întreţin şi/sau repară sisteme şi instalaţii de apărare împotriva incendiilor, efectuează lucrări de termoprotecţie şi ignifugare, de verificare, întreţinere şi reparare a autospecialelor şi/sau a altor mijloace tehnice destinate apărării împotriva incendiilor;
- OMAI nr. 132/2007 pentru aprobarea Metodologiei de elaborare a Planului de analiză şi acoperirea riscurilor şi a Structurii-cadru a Planului de analiză şi acoperire a riscurilor.
- OMAI nr. 210/2007 pentru aprobarea Metodologiei privind identificarea, evaluarea şi controlul riscurilor de incendiu.
- OMAI nr. 105/2007 pentru modificarea OMAI 585/2005 pentru aprobarea unor măsuri privind funcţionarea Comisiei de recunoaştere a organismelor pentru atestarea conformităţii produselor pentru construcţii cu rol în satisfacerea cerinţei securitate la incendiu.
- OMAI nr. 106/2007 pentru aprobarea Criteriilor privind stabilirea consiliilor locale şi operatorilor economici care au obligaţia de a angaja cel puţin un cadru tehnic sau personal de specialitate cu atribuţii în domeniul apărării împotriva incendiilor.
- OMAI nr. 1.474/2006 pentru aprobarea Regulamentului de planificare, organizare, pregătire şi desfăşurare a activităţii de prevenire a situaţiilor de urgenţă.

Exercitarea autorității de stat în domeniul apărării împotriva incendiilor se realizează prin activități de reglementare, avizare, autorizare, atestare, recunoaştere, desemnare, informare preventivă, control şi asistență tehnică de specialitate, coordonarea organizării şi a pregătirii serviciilor voluntare şi a populației, asigurarea intervențiilor în situații de urgență a serviciilor profesioniste, coordonarea intervențiilor la nivel național, control şi sancționarea încălcării prevederilor legale.

Controlul de stat, în domeniul apărării împotriva incendiilor, la nivel central, se exercită prin inspecția de prevenire şi alte compartimente şi unități din subordinea IGSU, respectiv, la nivel local, prin inspecțiile de prevenire din cadrul inspectoratelor.

În toate fazele de cercetare, proiectare, execuție şi pe întreaga lor durată de existență, construcțiile şi amenajările de orice tip, echipamentele, utilajele şi instalațiile tehnologice se supun unei analizări sistematice şi calificate pentru evaluarea şi controlul riscurilor de incendiu.

Una din formele cele mai importante ale activității de apărare împotriva incendiilor este prevenirea.

Principalele forme ale activității de prevenire sunt: reglementarea, avizarea, autorizarea, acordul, atestarea, recunoaşterea, desemnarea, supravegherea pieței, controlul, asistența tehnică de specialitate, informarea preventivă a autorităților, organismelor, factorilor implicați şi a populației, precum şi pregătirea acestora pentru situații de urgență, coordonarea serviciilor voluntare, publice şi private, pentru situații de urgență, auditul de supraveghere a persoanelor fizice şi juridice atestate, constatarea şi sancționarea încălcărilor prevederilor legale.

2. Sisteme de securitate la incendiu

Având în vedere noul statut al României de stat membru al UE, cu obligația de a respecta riguros reglementările europene, dar şi progresul tehnic remarcabil din ultimii ani, care a dus la o varietate tot mai mare de produse şi instalații de stingere a incendiilor, inclusiv de agenți de stingere se impune analiza diferențelor dintre normele de proiectare din țara noastră şi standardele europene din domeniu.

Noua concepție europeană privind securitatea la incendiu, cuprinsă în documentul interpretativ nr. 2, se referă şi la diferitele tipuri de instalații, atât la cele utilitare, cât şi la cele de stingere a incendiului. Documentul prezintă o nouă abordare a evaluării instalațiilor într-o construcție analizând atât rolul lor în funcționarea clădirii, respectiv în protecția împotriva incendiului, cât şi rezistența lor la foc, deci atât ca perioadă de timp în care pot să asigure funcția pentru care au fost proiectate şi executate, cât şi din punct de vedere al contribuției lor la propagarea incendiului.

Documentul interpretativ nr. 2 prezintă pe scurt principalele tipuri de instalații şi componente pentru instalații de detectare şi alarmare la incendiu, controlul fumului, instalații de stingere a incendiilor, instalații pentru căile de evacuare şi pentru securitatea echipelor de salvare.

Au fost elaborate familii de standarde pentru familii de instalații/componente ale instalațiilor. Aceste standarde oferă prezumția de conformitate, adică permit aplicarea marcajului CE pe produsul care îndeplineşte toate cerințele standardului, aplicând schema de atestare a conformității. Ca urmare **vor putea fi proiectate, comercializate sau utilizate numai acele instalații sau componente de instalații care sunt conforme cu standardele europene armonizate**.

Principala reglementare națională în vigoare referitoare la instalațiile de stingere a incendiilor este Normativul pentru proiectarea, executarea şi exploatarea instalațiilor de stingere a incendiilor, indicativ NP 086-05.

Mijloacele tehnice de apărare împotriva incendiilor reprezintă sistemele, instalațiile, echipamentele, utilajele, aparatele, dispozitivele, accesoriile, materialele, produsele, substanțele şi autospecialele destinate prevenirii, limitării şi stingerii incendiilor.

Armonizarea legislației este un proces continuu care evoluează în contextul integrării europene propriu-zise.

Problema armonizării implică perfecționarea actualelor reglementări, a structurării acestora în raport de exigențele comunitare.

Lista produselor pentru construcţii cu rol în satisfacerea cerinţei de securitate la incendiu, dintre acestea făcând parte şi sistemele de securitate este cuprinsă în anexa nr. 1 din OMAI nr. 607/2005.

1. Seturi pentru instalare:
Detectarea incendiului/alarme de incendiu:
- seturi de sisteme combinate de detectare a incendiului şi alarmare a incendiului;
- seturi de sisteme de detectare a incendiului;
- seturi de sisteme de alarmare la incendiu;
- seturi de sisteme de comunicaţii de alertare în caz de incendiu;

Prevenirea şi stingerea incendiilor:
- seturi de sisteme de hidranţi interiori;
- seturi de sisteme de hidranţi exteriori cu coloană uscată şi umedă;
- seturi de sisteme cu sprinklere şi apă pulverizată;
- seturi de sisteme de stingere cu pulbere uscată;
- seturi de sisteme de stingere cu gaz (inclusiv CO2);

Instalaţii pentru controlul focului:
- seturi de sisteme de evacuare a fumului şi gazelor fierbinţi (desfumare);
- seturi de sisteme cu presiune diferenţială;
- autodetectoare/semnalizatoare de fum.

2. Componente:
Detectarea incendiului/alarme de incendiu:
- detectoare de fum, de căldură şi de flacără;
- dispozitive de control şi indicatoare;
- dispozitive de transmitere alarme la distanţă;
- izolatori pentru scurtcircuit;
- dispozitive de alarmă;
- surse de energie;
- dispozitive de pornire/oprire;
- butoane manuale de semnalizare;

Prevenirea şi stingerea incendiilor:
- hidranţii de incendiu;
- indicatoare/comutatoare pentru debitul de apă;
- indicatoare/comutatoare pentru presiune;
- tubulatură de admisie;
- pompe şi seturi de pompare pentru combaterea focului;
- ştuţuri/sprinklere/drencere;
- seturi de supape de alarmă în circuit umed;
- seturi de supape de alarme uscate;
- seturi de supape de alarme inundate;
- dispozitive de control multiple;
- seturi de supape pentru containere sub presiune ridicate şi dispozitivele lor de acţionare;
- supape de distribuţie şi dispozitivele lor de acţionare;
- dispozitive neelectrice de dezactivare;
- racorduri flexibile;
- manometre şi presostate;
- dispozitive mecanice de măsurare;
- supape de închidere şi supape de control.

Controlul focului:
- perdele de fum;
- umidificatori;

- canale;
- ventilatoare electrice;
- ventilatoare naturale;
- panouri de control;
- panouri de control pentru urgențe;
- surse de energie.

3. Supravegherea pieței

Actele normative care reglementează această activitate sunt:

- Legea nr. 608/2001 *** republicată, privind evaluarea conformității produselor;
- HGR nr. 622/2004 *** republicată, privind stabilirea condițiilor de introducere pe piață a produselor pentru construcții;
- HGR nr. 891/2004 *** republicată, privind stabilirea unor măsuri de supraveghere a pieței produselor din domeniile reglementate, prevăzute în Legea nr. 608/2001 privind evaluarea conformității produselor, republicată;
- OMAI nr. 607/2005 pentru aprobarea Metodologiei de control privind supravegherea pieței produselor pentru construcții cu rol în satisfacerea cerinței de securitate la incendiu;
- OMTCT nr. 1558/2004 pentru aprobarea Regulamentului privind atestarea conformității produselor pentru construcții, cu modificările şi completările ulterioare;
- OMAI nr. 770/2005 pentru aprobarea Regulamentului de autorizare a laboratoarelor şi poligoanelor de încercări la foc şi a celor de distrugere a muniției neexplodate modificat şi completat de Ordinul ministrului internelor si reformei administrative nr. 311/2007.

Supravegherea pieței, precum şi recunoaşterea şi desemnarea organismelor pentru atestarea conformității produselor cu rol în satisfacerea cerinței de securitate la incendiu sunt forme ale activității de prevenire care se execută prin structuri specializate, la nivel național, de către Inspecția de Prevenire.

Statele Membre ale Uniunii Europene au considerat că le revine sarcina de a se asigura că, pe teritoriile lor, clădirile şi lucrările de inginerie civilă sunt şi trebuie să fie proiectate şi executate astfel încât să nu pună în pericol siguranța persoanelor, a animalelor domestice şi a proprietății, cu respectarea totodată şi a altor cerințe esențiale în interesul bunăstării generale.

În acest sens la nivelul Uniunii Europene a fost adoptată Directiva referitoare la produsele pentru construcții nr. 89/106/CEE.

Direcțiile principale urmărite prin adoptarea şi aplicarea directivei mai sus amintite sunt:

- elaborarea şi aplicarea de dispoziții referitoare la siguranța clădirilor, sănătate, durabilitate, economia de energie, protecția mediului, aspecte economice şi alte aspecte importante din punct de vedere al interesului public unitar la nivelul Uniunii Europene. S-a luat în considerare faptul că aceste reglementări, pot avea o influență directă asupra naturii produselor pentru construcții folosite şi care ar putea fi reflectate în standarde de produs, agremente tehnice şi alte specificații şi dispoziții tehnice naționale, care prin diversitatea lor, pot împiedica schimburile comerciale în cadrul Comunității.
- constituirea unor cerințe esențiale drept criterii, atât de ordin general cât şi specifice, pe care construcțiile trebuie să le satisfacă;
- constituirea unei baze de referință pentru standardele armonizate sau alte specificații tehnice elaborate la nivel European;
- stabilirea documentelor interpretative pentru întocmirea sau acordarea unui agrement tehnic European, având ca scop transpunerea cerințelor esențiale într-o formă concretă la nivel tehnic;
- formularea precisă a acestor standarde armonizate având în vedere natura specială a produselor pentru construcții;

- includerea, în cadrul standardelor armonizate, a unor clasificări care să permită plasarea pe piață a produselor pentru construcții care satisfac cerințele esențiale şi care sunt fabricate şi utilizate conform legii în concordanță cu tradițiile tehnice justificate de condițiile locale de climă sau de altă factură;
- aplicarea marcajului CE pentru produsele adecvate pentru utilizare, în scopul recunoaşterii cu uşurință, permițând totodată libera circulație şi utilizarea fără restricții în scopurile prevăzute.

În cazul produselor pentru care standardele Europene nu pot fi întocmite sau prevăzute într-un interval rezonabil de timp sau al produselor care se abat substanțial de la standard, adecvarea pentru utilizare a unor asemenea produse poate fi dovedită prin intermediul agrementelor tehnice Europene pe baza unor ghiduri comune.

În absența standardelor armonizate şi a agrementelor tehnice Europene, specificațiile tehnice naționale nearmonizate pot fi recunoscute doar dacă asigură o bază corespunzătoare pentru presupunerea că sunt satisfăcute cerințele esențiale.

S-a considerat că este necesar să se asigure conformitatea produselor cu standarde armonizate şi cu specificații tehnice nearmonizate recunoscute la nivel european prin intermediul unor proceduri privind controlul producției de către producători şi privind supravegherea, evaluarea prin încercări şi certificarea de către terțe părți independente şi certificate de către producătorul însuşi.

Ca o concluzie s-a considerat că este utilă constituirea unui Comitet Permanent pentru Construcții, compus din experți desemnați de Statele Membre, care să asiste Comisia în problemele ce decurg din implementarea şi aplicarea Directivei 89/106/CEE.

La nivel național directiva produselor pentru construcții a fost transpusă prin HGR nr. 622/2004 privitoare la stabilirea condițiilor de introducerea pe piață a produselor pentru construcții.

Totodată HGR nr. 891/2004 republicată, privind *stabilirea unor măsuri de supraveghere a pieței produselor din domeniile reglementate, prevăzute în Legea nr. 608/2001 privind evaluarea conformității produselor, republicată*, stabileşte că supravegherea pieței este activitatea prin care autoritățile competente asigură că sunt respectate prevederile reglementărilor tehnice prevăzute în Legea nr. 608/2001, republicată. Activitățile de supraveghere se realizează de către structuri nominalizate, cu respectarea prevederilor art. 26-28 din Legea mai sus menționată.

Urmare a HGR nr. 622/2004 a fost emis OMAI nr. 607 din 19.04.2005 pentru aprobarea metodologiei de control privind supravegherea pieței produselor pentru construcții cu rol în satisfacerea cerinței securitate la incendiu. Ordinul precizează că Inspectoratul General pentru Situații de Urgență îşi exercită atribuțiile de organ de control, stabilite prin Hotărârea Guvernului nr. 891/2004 privind stabilirea unor măsuri de supraveghere a pieței produselor din domeniile reglementate, prevăzute în Legea nr. 608/2001 privind evaluarea conformității produselor, cu modificările şi completările ulterioare, modificată prin Hotărârea Guvernului nr. 140/2005, prin Serviciul pentru supravegherea pieței din cadrul Inspecției de prevenire - Direcția pompieri.

Prin activitatea de supraveghere a pieței se controlează dacă:
- produsele enumerate în anexa nr. 1 îndeplinesc cerințele Hotărârii Guvernului nr. 622/2004 privind stabilirea condițiilor de introducere pe piață a produselor pentru construcții, cu modificările şi completările ulterioare, denumită în continuare reglementare;
- cei responsabili de introducerea pe piață a produselor acționează pentru ca produsele neconforme să fie aduse în conformitate cu cerințele reglementării şi pun în aplicare măsurile dispuse.

Termenii utilizați în cuprinsul acestor acte normative sunt următorii cu precizarea că nu au fost menționați în totalitatea acestora:

a) agrement tehnic european - specificație tehnică ce exprimă o evaluare tehnică favorabilă a adecvării unui produs la o utilizare preconizată, bazată pe satisfacerea cerințelor esențiale aplicabile construcției în care produsul urmează a fi utilizat;

b) atestarea conformității produselor pentru construcții - sistem procedural prin care este evaluată şi stabilită conformitatea produselor pentru construcții cu specificațiile tehnice aplicabile, în vederea aplicării marcajului european de conformitate CE, denumit în continuare marcaj CE;

c) construcții - orice obiect care este construit sau rezultă din operații şi/sau lucrări de construcții şi este fixat de pământ, termenul desemnând atât clădirile, cât şi lucrările de inginerie civilă;

d) documente interpretative - documente elaborate de Comisia Europeană, prin care cerințele esențiale sunt transpuse într-o formă concretă şi care creează legăturile necesare între cerințele esențiale ale construcției şi mandatele de standardizare, mandatele pentru ghidurile pentru agremente tehnice europene sau recunoaşterea altor specificații tehnice;

e) documente tehnice directoare - ghiduri, regulamente şi proceduri elaborate în temeiul prezentei hotărâri şi în scopul aplicării acesteia;

f) familie de produse - grup de produse generice care au utilizări prevăzute similare, cum ar fi: finisaje pentru pereți interiori sau învelitori de acoperiş;

g) ghid - reglementare care cuprinde metode şi procedee detaliate de satisfacere a cerințelor aplicate;

h) organe de control - organe ale administrației publice centrale care răspund de supravegherea pieței produselor pentru construcții;

i) piața produselor pentru construcții - întreaga arie acoperită de lanțul de distribuție a produselor pentru construcții de la producător la consumatorul final, inclusiv şantierele de construcții, până la punerea în operă;

j) produs pentru construcții - orice produs realizat în scopul de a fi încorporat în mod permanent în construcții, termenul desemnând materiale, elemente şi componente individuale sau alcătuind un set, inclusiv pentru sisteme prefabricate sau instalații, plasate pe piață în forma în care urmează a fi încorporate, asamblate, aplicate sau instalate în construcții prin operații şi/sau lucrări de construcții;

k) specificație tehnică - document care stabileşte caracteristicile unui produs, cum ar fi niveluri de calitate, performanță, securitate sau dimensiuni, inclusiv cerințe care se aplică produsului cu privire la denumirea sub care acesta este comercializat, terminologie, simboluri, încercări şi metode de încercare, ambalare, marcare sau etichetare şi proceduri pentru evaluarea conformității;

l) utilizare preconizată - rol sau funcție care urmează a fi îndeplinită de produs pentru satisfacerea cerințelor esențiale ale construcției.

Verificările realizate de către Serviciul pentru supravegherea pieței sunt:

a) verificări formale - privesc prezența şi modul de aplicare a marcajului CE, declarația de conformitate dată de producător pe baza unui certificat de conformitate EC, eliberat de un organism de certificare notificat, informațiile ce însoțesc produsul şi/sau corecta alegere a procedurilor de atestare a conformității

b) verificări de fond - privesc verificarea conformității produsului cu cerințele esențiale, a conținutului declarației de conformitate date de producător pe baza unui certificat de conformitate EC, eliberat de un organism de certificare notificat, şi corecta aplicare a procedurilor de evaluare a conformității; de regulă, verificările se referă numai la aspecte privind performanțele produsului, cum sunt: caracteristici de detectare, stingere, alarmare, semnalizare.

Producătorul, reprezentantul autorizat al acestuia sau altă persoană responsabilă de introducerea pe piață ori punerea în funcțiune a produsului este obligat să pună la dispoziție Serviciului pentru supravegherea pieței declarația de conformitate, certificatul de conformitate EC şi documentația tehnică în limba română.

În conformitate cu prevederile OMIRA nr. 252/2007 pentru aprobarea *Metodologiei de atestare a persoanelor care proiectează, execută, verifică, întreține şi/sau repară sisteme şi instalații de apărare împotriva incendiilor, efectuează lucrări de termoprotecție şi ignifugare, de verificare, întreținere şi reparare a autospecialelor şi/sau a altor mijloace tehnice destinate apărării împotriva incendiilor* întregul personal care desfăşoară activitățile enumerate în titlul actului normativ trebuie să fie atestate.

Atestarea este recunoscută doar după parcurgerea unui curs de formare profesională în ocupațiile ce vizează activitățile enumerate.

După parcurgerea programului de formare atestarea în vederea practicării ocupației este realizată de către Centrul Național pentru Securitate la Incendiu și Protecție Civilă.

Întocmit

Mr. George SORESCU

MODULUL VI – Instalații/sisteme de detectare, semnalizare şi alarmare la incendiu

1.1. Instalații de protecție împotriva incendiilor/ sisteme de detectare, semnalizare şi alarmare la incendiu
Cadru legislativ național
Cadru legislativ internațional
2.3. Criterii minime de echipare a construcțiilor cu instalații/sisteme de detectare semnalizare şi alarmare la incendiu

Tema 3 – Elemente de teorie a arderii şi propagarea incendiilor
3.1. Termeni tehnici utilizați în descrierea fenomenelor de ardere
3.2. Fenomene fizice şi chimice relevante în detecția automată a incendiilor

Tema 4 – Echipamente şi dispozitive, componente ale sistemelor de detectare automată a incendiilor

Tema 5 – Arhitecturi şi topologii pentru instalațiile de protecție împotriva incendiilor/sisteme de detectare, semnalizare şi alarmare la incendiu

Tema 6 – Aspecte practice privind realizarea instalațiilor de protecție împotriva incendiilor/sisteme de detectare, semnalizare şi alarmare la incendiu
6.1. Zonarea clădirilor
6.2. Alegerea detectoarelor şi declanşatoarelor manuale
6.3. amplasarea echipamentelor de detecție şi alarmare

Tema 7 – Noțiuni generale privind instalațiile de stingere automată şi conexiunea acestora cu sistemele de detectare, semnalizare şi alarmare la incendiu

COMPETENTE NECESARE

Recunoaşterea principiilor de detecție şi tipurile de detectoare;

Recunoaşterea principiilor de funcționare ale echipamentelor de control şi semnalizare;

Recunoaşterea configurațiilor/modul de configurare a instalațiilor de protecție împotriva incendiilor/sisteme de detectare, semnalizare şi alarmare la incendiu;

Recunoaşterea surselor de alimentare cu energie electrică a instalațiilor de protecție împotriva incendiilor/sisteme de detectare, semnalizare şi alarmare la incendiu;

Recunoaşterea sistemelor de management a securității clădirii;

Recunoaşterea tipurilor de verificări şi încercări precum şi întreținerea instalațiilor de protecție împotriva incendiilor/sisteme de detectare, semnalizare şi alarmare la incendiu;

Utilizarea standardelor tehnice;

Utilizarea normativelor şi reglementările privind execuția instalațiilor de protecție împotriva incendiilor/sisteme de detectare, semnalizare şi alarmare la incendiu.

MODULUL IX – Executia si mentenanta instalatiilor /sistemelor de detectare, semnalizare si alarmare la incendiu

Tema 1- Sisteme tehnice de detectare

Tema 2 – Reglementări legale în vigoare

Tema 3 – Proceduri relevante

Tema 4 – Mentenanta sistemelor de detectare

Verificarea alimentarilor cu energie electrică

Pornirea sistemului de detectare, semnalizare si alarmare la incendiu

Efectuarea setarilor programelor de functionare a echipamentelor/ sistemelor de detectare, semnalizare si alarmare la incendiu

Verificarea stării de functionare a sistemului

Identificarea defectiunilor sistemului tehnic

Efectuarea operatiunilor de mentenantă

Focul – fenomen fizico chimic. Forme de manifestare.
Triunghiul focului si Tetraedrul focului.

Cunoscut din cele mai vechi timpuri focul a fost o unealta in dezvoltarea umanitatii insa si un permanent pericol datorita efectelor devastatoare produse la scaparea de sub control.

Cu toate ca este folosit de milenii propietatile acestuia nu sunt nici in prezent total cunoscute. Din punct de vedere chimic combustia (focul) este un **proces exoterm de oxidare** in care anumite substante reactioneaza, cu viteze de reactie diferite (de la lent la exploziv), cind se combina cu oxigenul in stare libera producind o cantitate mare de caldura si frecvent lumina (radiatii cu lungimi de unda specifice materialelor oxidate). Substantele ce reactioneaza in acest mod se numesc **combustibili** iar reactia se numeste **combustie**.

Ne vom opri in urmatoarele rinduri asupra elementelor esentiale ale unui foc:

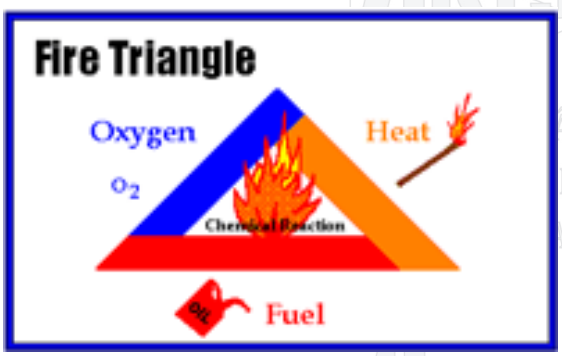


Fig. 1.0 Triunghiul Focului

Pentru a exista focul are nevoie de prezenta celor trei factori importanti: Oxigen, Material combustibil si Energie. Lipsa oricarui element impiedica producerea procesului de ardere.

Fara oxigen (prezent in orice forma) nu poate exista procesul de ardere, la fel de clar lipsa materialului combustibil in mod evident nu permite arderea. Ceva mai complicat stau lucrturile cu energia (factorul de initiere – in anumite cazuri). Astfel in anumite tipuri de incendii factorul energetic consta doar in asigurarea elementului de initiere ulterior procesul de ardere autointretinindu-se iar in alte cazuri lipsa unui aport energetic constant duce la stingerea de la sine a focului.

Anumite tipuri de incendii nu pot fi incadrate in modelul grafic prezentat (triunghiul focului) si a impus dezvoltarea unui model mai avansat denumit “Tetraedrul focului”

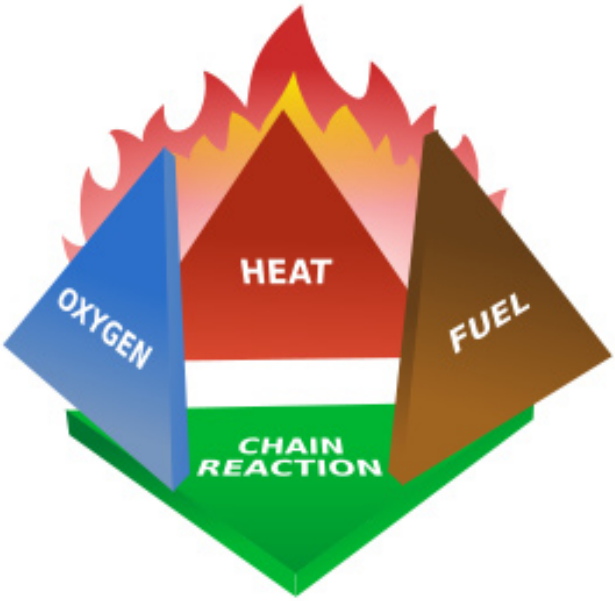


Fig. 1.1 Tetraedrul Focului

Cu usurinta observam ca elementul suplimentar este "Chain Reaction" – "Reactia in Lant". Reactia in lant este specifica incendiilor de natura chimica sau nucleara dar poate fi intilnita si in alte incendii in care combinatia materialelor combustibile genereaza prin oxidare compusi noi cu caracteristici energetice superioare ce produc prin efect cumulativ autointretinerea si cresterea incendiului. Scara de timp poate fi diferita functie de materialul combustibil ceea ce face ca unui observator perceptia rezultata sa fie de la extindere lenta la cea exploziva. Un exemplu usor de inteles este arderea amestecului motorina-nitrat de amoniu. La temperaturi ridicate rezulta o reactie in lant violenta exploziva ce degaja foarte multa energie.

Din punctul de vedere al securitatii antiincendiu suntem in special interesati de doua aspecte:

a) moduri de manifestare al unui foc

In urma procesului de oxidare (ardere) apar o intreaga pleiada de fenomene fizice chimice ce permit identificarea unui incendiu. Dintre formele de manifestare ale focului utilizate in detectia unui incendiu amintim:

- fumul ; suspensie de particule de dimensiuni diferite in aer.
- efect termic ; ca urmare a procesului de ardere se produce o degajare de temperatura semnificativa.
- efect optic ; in multe cazuri arderea este insotita de prezenta flacarilor ce genereaza radiatii in spectrul vizibil precum sii in UV/ IR (ultraviolet si infrarosu).
- aport energetic; emisia de particule cu energii inalte ca urmare a procesului de ardere poate fi pusa in evidenta cu usurinta prin efectul ionizant al acestora
- emisia unor produsi chimici tipici arderii; in cazul in care este cunoscut materialul combustibil se stiu cu precizie compusii chimici rezultati in urma arderii. Evidentierea acestora este un indiciu sigur privind existenta unui incendiu.

b) moduri de stingere

Stingerea inseamna intreruperea procesului de oxidare. Altfel spus trebuie actionat asupra unui element din triunghiul energetic al focului astfel incit arderea sa devina imposibila. Exista urmatoarele posibilitati:

i. **actionarea asupra materialului combustibil.** Este cea mai simpla metoda de stingere (se indeparteaza materialul combustibil) dar din pacate nu este practica in multe cazuri. Materialele combustibile sunt extrem de diverse si prezinta fiecare energii degajate in cazul arderii extrem de variate. Temperatura la care are loc arderea poate transforma un material greu combustibil prin descompunere intr-un compus cu valoare energetica foarte mare. Din motivele mai sus amintite singura actiune posibila asupra materialului combustibil are caracter preventiv si consta in limitarea pe cit posibil a cantitatii de material combustibil aflat intr-un anumit spatiu sau separarea materialelor combustibile functie de caracteristicile acestora.

ii. **actionarea asupra oxigenului.** Oxigenul este un gaz atmosferic prezent in compozitia aerului intr-un procent de aprox. 21%.

COMPOZITIA AERULUI ATMOSFERIC USCAT

	Masã molecularã MW	% volum (m^3 / m^3)	% masã (kg / kg)
Azot, N_2	28	78,08	75,52
Oxigen, O_2	32	20,95	23,15
Argon, A	40	0,93	1,28
Dioxid de carbon, CO_2	44	0,03	0,046
Altele		0,01	0,004

Lipsa oxigenului sau prezenta acestuia intr-un procent redus duce la intreruperea arderii. Reducerea procentului de oxigen in aer are loc de la sine la arderea intr-un spatiu inchis. Oxigenul din aer se combina, ca urmare a procesului de combustie, cu materialul combustibil pina ce aceasta reactie consuma tot oxigenul disponibil moment in care arderea inceteaza. Acest caz este rar intilnit in practica deoarece putine spatii sunt etanse si uzual etanseitatea se pierde ca urmare a celorlalte efecte ale arderii (in special datorita efectului termic). Totusi reducerea procentului de oxigen in spatiul in care are loc arderea este o metoda de stingere utilizata. Realizarea practica se face prin deversarea unor gaze sau amestecuri de gaze inerte in cantitate mare (40-100% din volumul de stins) ce vor reduce cantitatea de oxigen din spatiul respectiv stingind focul. Este evident ca aceasta metoda nu poate fi aplicata la incendiile din spatii deschise sau cu volume mari.
O alta cale este realizarea unei bariere intre oxigen si materialul combustibil. Aceasta este actiunea tipica a agentilor spumanti sau peliculari ce adera la suprafata materialului combustibil izolindu-l fata de oxigenul atmosferic.

iii. **actionarea asupra energiei.** In prezenta oxigenului si a materialelor combustibile focul nu poate apare fara un aport extern de energie sau un factor de initiere. Aportul energetic poate fi sub forme variate dar pentru o mai buna intelegere a fenomenului vom exemplifica in considerind aportul de energie ca fiind adus exclusiv sub forma energiei termice.

Pentru a declansa procesul de ardere o parte a combustibilului trebuie să aibă o temperatură mai mare decât punctul său de aprindere. Aportul termic necesar reprezinta diferenta intre temperatura initiala si temperatura punctului de aprindere specific acelui material combustibil.

Odata declansata reactia in mod punctiform energia rezultata va permite extinderea reactiei in intreaga masa* a materialului combustibil (*nota: presupunind ca materialul combustibil este un gaz sau un lichid in stare de vapori. In cazul in care materialul combustibil este un lichid sau un corp solid extinderea are loc pe intreaga suprafata expusa mediului, disponibila).
Daca aportul termic este intrerupt iar energia rezultata in reactie nu asigura depasirea temperaturii aferente punctului de aprindere specific materialului combustibil atunci procesul de ardere se intrerupe de la sine.
Concluzia este evidenta actiunea asupra energiei este eficienta in urmatoarele cazuri:

a) preventiv – cind exista conditiile aparitiei unui incendiu dar lipsa amorsei (factorului de initiere) impiedica aparitia acestuia.
b) in procesul de stingere - eliminind o cantitate de energie mai mare decit cea necesara automentinerii incendiului se produce stingerea. Uzual eliminarea energiei se face prin metode fizico-chimice cum ar fi:

- racirea spatiului de stins, uzual cu substante ce preiau energia la transformarea dintr-o faza de agregare in alta (exemplu apa lichida -> vapori) sau ca urmare a unor procese fizice (exemplu: destinderea unui gaz comprimat – proces endoterm)
- utilizarea unor substante chimice ce intervin in procesul de ardere consumind energia rezultata
- deversarea unor substante energofage la nivel molecular sau substante ce cresc in mod artifical « punctul de aprindere » al materialului combustibil

Reactii chimice

Complexitatea fenomenului de oxidare si mai ales variatiile ce pot rezulta la arderea aceluiasi material combustibil in conditii de mediu diferite fac imposibila descrierea in amanunt a reactiilor chimice specifice insa putem grupa din punct de vedere chimic in doua mari clase :

- oxidarea in mediu de oxigen pur
- oxidarea in aer

O descriere a arderii unei hidrocarburi in oxigen pur ar fi urmatoarea:

$$\text{Fuel} + \text{Oxygen} \rightarrow \text{Heat} + \text{Water} + \text{Carbon dioxide}$$

COMBUSTIBIL + Oxigen Caldura + Apa + Dioxid de carbon

In acest caz se observa ca arderea este “curata” adica avem ca produsi de ardere dioxidul de carbon si apa. Aceasta ecuatie este corecta pentru o ardere completa intr-un mediu de oxigen (practic cantitatea de oxigen este considerata nelimitata).

In realitate nu avem aceste cazuri ideale iar ecuatia trebuie sa fie scrisa astfel:

$$\text{Fuel} + \text{Air} \rightarrow \text{Heat} + \text{Water} + \text{Carbon dioxide} + \text{Nitrogen}$$

COMBUSTIBIL + AER Caldura + Apa + Dioxid de carbon + Azot

Daca tinem seama de conditii in care cantitatea de aer nu permite o ardere completa vor fi intilniti atit monoxidul de carbon cit si compusi ai azotului.

Daca la o hidrocarbura lucrurile sunt destul de complicate in cazul substantelor combustibile complexe predictia exacta a cocentratiei fiecarui componente devine aproape imposibila deoarece apar diversi compusi de ardere specifici vitezei si temperaturii de ardere.

Una din concluziile importante referitoare la procesul de ardere din punct de vedere chimic este ca fumul rezultat intr-un proces de ardere poate avea **compozitii diferite** functie de **parametri de ardere** (in mod special materialul combustibil, viteza si conditii de mediu) influentind capacitatea de detectie a unor tipuri de detectoare de fum.

DEFINITII SPECIFICE

FUMUL

Definitia simpla si totodata clasica a fumului este:

“ Suspensie de **particule solide in aer** pusa in miscare de curenti termici ascendenti”

Daca aceasta definitie succinta permite o intelegere la nivel elementar a fenomenului pentru un studiu aprofundat consideram ca o definire mult mai completa este:

“Suspensie de **particule solide si lichide mixate intr-un volum de aer si produsi de ardere gazosi** pus in miscare de curenti termali”

Partculele lichide (aerosolii) la care facem referire pot fi vapori de apa, substante volatile (uleiuri, fractiuni ale hidrocarburilor sau compusi de ardere rezultati prin descompunerea unor materiale combustibile) dar de regula in cele mai multe cazuri au proprietatile unui lichid combustibil.

Gazele din fum pot fi extrem de diferite din punct de vedere chimic functie de materialul combustibil si conditiile de ardere. Carcteristica comuna consta in gradul de inflamabilitate care ramine ridicat in cele mai multe cazuri.

Concluzia este ca fumul nu trebuie privit exclusiv ca un element pasiv ci mai degraba ca o parte componenta a unui incendiu putind transfera caldura si material combustibil intre doua zone neizolate.

TERMENI TEHNICI UTILIZATI IN DESCRIEREA FENOMENELOR DE ARDERE

Consideram utila explicarea unor termeni intilniti care pot crea confuzie in descrierea unui anumit tip de incendiu.

FLASH FIRE - Combustie cu caracter exploziv la care frontul flacarilor are o deplasare rapida. Produce unde considerabile de soc. Poate apare in conditiile in care aerul este amestecta cu combustibilul in concentratii optime. Fluxul de temperatura este de aproximativ 84 kW/mp pentru intervale de timp tipice mai mici de 3 secunde.

(Definitie provenind dinCGSB 155.20-2000 and NFPA 2113).

Observatie. In incendii de tip FLASH FIRE viteza flacarilor este subsonica iar daunele cauzate de undele de soc sunt minore. Efectul major este cauzat de fluxul termic si de aparitia incendiilor secundare

FLASHOVER – Combustie simultana (sau intr-un interval de timp redus) a tuturor materialelor dintr-un spatiu inchis. Acest fenomen apare cind majoritatea suprafetelor dintr-un spatiu inchis sunt incalzite in special prin radiatie pina la atingerea punctului de autoaprindere.

Nota – Daca fenomenul are loc in spatii deschise in conditii particulare poarta denumirea de “furtuna de foc – firestorm”. Poate apare in incendiile de padure sau ca urmare a bombardamentelor cu substante incendiare.

Poate cel mai bun exemplu este oferit de un incendiu rezidential. Astfel intr-o camera in care are loc un incendiu produsii de ardere creeaza un strat de fum supraincalzit la nivelul tavanului. Prin fenomenul de radiatie termica suprafetele materialelor combustibile din camera se incalzesc puternic eliberind gaze inflamabile (piroliza locala). Cind temperatura suprafetelor devine suficient de ridicata gazele inflamabile se aprind si intr-un interval de citeva secunde toate suprafetele din camera sunt in flacari.

Tipuri de flashover

LEAN FLASHOVER (denumit si ROLLOVER) - tipic pentru aprinderea unui strat de gaze la nivelul tavanului. Amestecul gaz aer este la limita de jos a inflamabilitatii.

Nota: Unii autori separa faza de flashover de cea de tip rollover specificind ca flashover poate precede rollover. Astfel rolover rezuminduse la efectul vizual creat de gazele pirolitice aprinse cu un efect rotational pe suprafata tavanului. Rollover astfel definit implicind aprinderea intregului volum de gazedin incapere nu a tuturor suprafetelor combustibile. Termenul sinonim fiind in acest caz FLAMEOVER distinct fata de flashover.

REACH FLASHOVER (denumit si BACKDRAFT) – amestecul exploziv este bogat (la limita de sus a inflamabilitatii – amestec suprasaturat).

DELAYED FLASHOVER (cunoscut si ca SMOKE EXPLOSION sau FIRE GAS IGNITION) – specificul acestuia consta in faptul ca aprinderea are loc in exteriorul spatiului in care a izbucnit incendiul. Functie de concentratia gazelor in mixtura combustibila arderea poate fi foarte violenta.

HOT RICH FLASHOVER - fenomen specific incendiilor violente in spatii inchise cu degajare masiva de caldura si gaze. Amestecul suprasaturat de gaze pirolitice aflat la temperaturi peste punctul de aprindere se autoaprinde la exteriorul spatiului unde a fost generat in momentul in care prin dilutie se atinge concentratia optima. Ulterior aprinderii flacarile se pot intoarce in spatiul in care a fost generat amestecul manifestindu-se asemanator unui reach flashover.

Descrierea fenomenelor observate in cazul unui incendiu real este deosebit de dificila deoarece unele fenomene sunt foarte rapide iar alte manifestari pot fi incadrate in mai multe categorii efectele vizibile fiind similare iar monitorizarea fenomenelor tranzitorii pe suprafete mari imprecisa datorita microconditiilor locale.

ECHIPAMENTE SI DISPOZITIVE COMPONENTE ALE SISTEMELOR DE

DETECTIE AUTOMATA A INCENDIILOR.

Pentru a descrie adecvat un sistem de detectie automata si partile sale componente este imperios necesar ca semnificatia termenilor folositi sa fie clara. In acest scop capitolul Definitii incearca sa expliciteze termenii tehnici uzuali. Mentionam ca definitiile sunt cele din limba romana acceptate atit de standardele romanesti SR EN 54 –xx cit si de normativele in vigoare (ex. I18/2-2002)

Definitii

Cale de transmisie – conexiune fizica externa echipamentului de control si semnalizare (centrala de semnalizare), necesara pentru transmiterea de informatii si/sau tensiuni de alimentare intre centrala de semnalizare si celelalte componente ale instalatiei de semnaliza sau intre parti ale unei centrale de semnalizare dispuse in carcase diferite.

NOTA: Calea de transmisie poate fi un cablu o fibra optica sau o conexiune pe orice frecventa a spectrului electromagnetic.

Echipament de control si semnalizare (centrala de semnalizare) - Componenta a sistemului de detectare a incendiului, echipament multifunctional care asigura receptionarea, prelucrarea, centralizarea si transmiterea semnalelor de la si catre elementele periferice interconectate in sistem.

Echipament de protectie impotriva incendiului - echipament automat de control si de interventie impotriva incendiilor (exemplu: instalatie de stingere)

Circuit de detectare – cale de transmisie care leaga punctele de detectare si/sau semnalizare la centrala de semnalizare

Detector de incendiu – Componenta a sistemului de detectare a incendiului care contine cel putin un senzor care monitorizeaza cel putin un parametru fizic si/sau chimic asociat cu incendiul si furnizeaza un semnal corespunzator la centrala de semnalizare..

Declansator manual de alarma (buton de semnalizare) – Componenta a unei instalatii de semnalizare a incendiilor care este utilizata pentru semnalizarea manuala a unui incendiu.

Dispozitiv de alarma la incendiu – componeta acustica si/sau optica a sistemului de alarma la incendiu, neinclusa in echipamentul de control si semnalizare, care este utilizata pentru avertizarea in caz de incendiu.

Dispozitiv de transmisie alarma incendiu – echipament intermediar care transmite un semnal de alarma de la o centrala de semnalizare la un dispozitiv de receptie a alarmei

Dispozitiv de transmisie semnal de defect – echipament intermediar care transmite un semnal de defect de la o centrala de semnalizare la un dispozitiv de receptie a semnalului de defect

Elemente pentru conectare – toate acele elemente care formeaza legaturile intre diferitele componente ale unui sistem de detectie si de alarma la incendiu.

Alarma - Semnal acustic si/sau optic initiat de om sau de un dispozitiv de initiere (detector sau declansator manual de alarma) prin care persoanele din incinta sunt anuntate despre existenta unui eveniment.

Alarma falsa – alarma produsa in conditii in care pericolul nu este real.

NOTA – O alarma falsa nu presupune neaparat echipament defect. Din punctul de vedere al unui detector prezenta in camera de detectie a unor particule in suspensie similare fumului constituie un motiv intemeiat de a declansa starea de alarma. Faptul ca particulele respective sunt particule de praf si nu de fum face ca alarma sa fie falsa deoarece nu a rezultat ca urmare a unui incendiu dar indicatia detectorului este corecta.

Defect de izolatie fata de pamint – conexiune accidentala intre pamint si un element oarecare al unui centrale de semnaliza a cailor de transmisie spre o centrala de semnalizare sau a cailor de transmisie dintre elementele sistemului.

NOTA- definitia se refera la cai de transmisie ce conduc curentul electric (exemplu cabluri sau alte materiale conductive). Nu poate apare la cai de transmisie nonconductive sau la cele radio.

Defect de cablu – defect al unei cai de transmisie sau al unui circuit de transmisie spre centrala de semnalizare sau intre elementele sistemului de tip scurtcircuit, intrerupere sau orice alt tip care afecteaza modul de functionare al circuitului respectiv

Nota:
Doua defecte de cablu sau de conectare pe un singur circuit nu trebuie sa impiedice protejarea unei arii desfasurate mai mari de 10000 mp.

Distanta de cautare – distanta maxima ce trebuie parcursa in cadrul unei zone pentru identificarea detectorului neadresabil care a initialt un semnal de alarma

Anulare semnalizare acustica – operatie manuala de oprire a semnalului acustic

Semnalizare – informatie furnizata de un indicator

Resetare – operatie capabila de a incheia o stare de alarma de incendiu si/sau defect

Instalatie de semnalizare a incendiului – ansamblu complex compus din declansatoare manuale si detectoare automate conectate la o centrala de semnalizare care permite monitorizarea dispozitivelor de semnalizare si care poate actiona automat instalatii de evacuare si stingere sau auxiliare.

Echipament de alimentare cu energie electrica – componenta a instalatiei de semnalizare a incendiului care asigura alimentarea cu energie electrica a echipamentului de control si semnalizare. Include sursele de alimentare principala so de rezerva.

Sursa de alimentare electrica de baza – alimentarea cu energie electrica a instalatiei de semnalizare a incendiului in conditii normale de functionare

Sursa de alimentare electrica de rezerva - alimentarea cu energie electrica a instalatiei de semnalizare a incendiului in cazul indisponibilitatii sursei de baza

Panou sinoptic (repetor) – panou pe care se totalizeaza indicatiile vizuale prin intermediul carora se poate constata rapid si in ansamblu starea unei instalatii de semnalizare a incendiului.

Zona – Subdiviziune a spatiilor protejate in care sunt instalate unul sau mai multe puncte de detectie si pentru care este furnizata o semnalizare zonala comuna.

Nota – definirea ca subdiviziune a spatiului nu trebuie considerata ca fiind neaparat separata fizic din punct de vedere al circuitelor electrice. Zona poate fi definita si prin intermediul softului daca aria pentru care se doreste semnalizarea comuna prezinta un anumit interes.

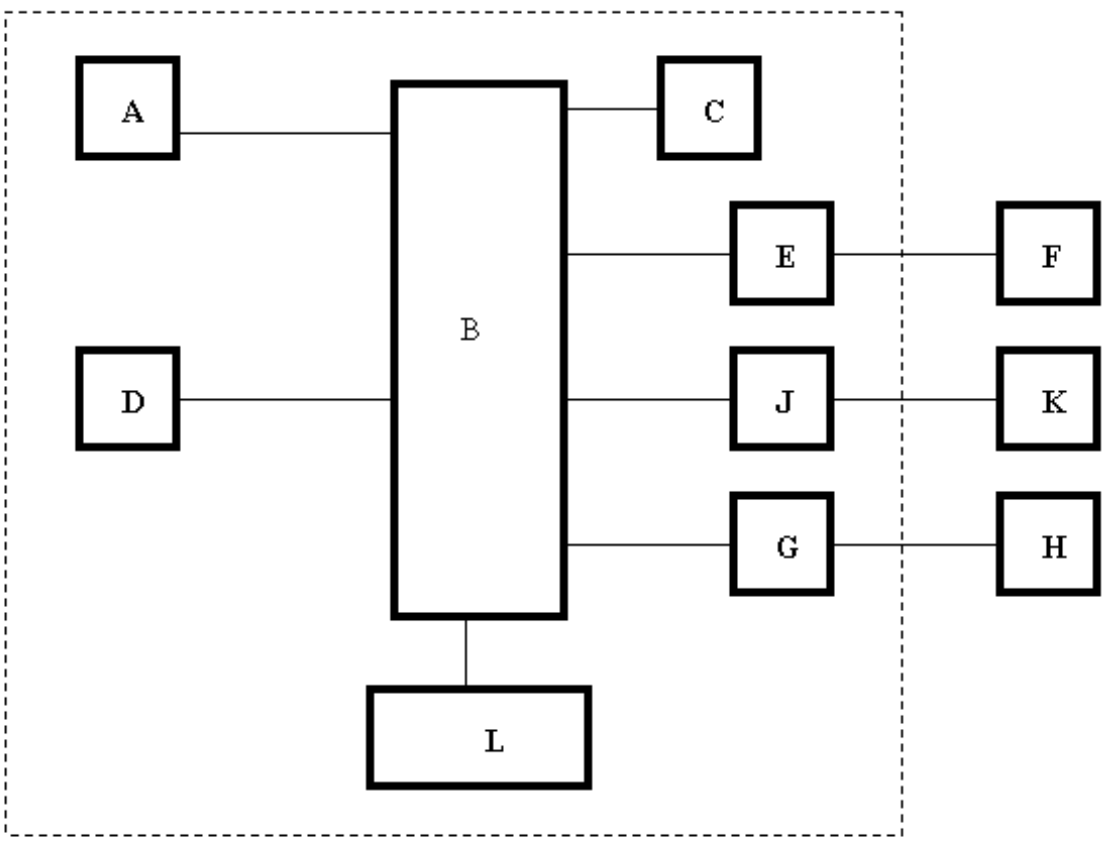
Echipamente de detectie

Pentru a detecta rapid un inceput de incendiu este necesar sa fie detectata una din formele de manifestare ale acestuia cu un grad de precizie ridicat si pe cit posibil acea forma de manifestare sa nu poata avea alta cauza. Practic acest lucru nu este posibil in acest moment fiecare tip de element de detectie avind limitarile sale. Centralele antiincendiu difera semnificativ de la un producator la altul astfel incit un mod general ne vom referi la ele numai din punct de vedere al tipului de sistem in care opereaza si anume :

Centrale conventionale – dispun de linii conventionale de detectie

Centrale conventional adresabile – dispun de linii conventionale de detectie dar cu facilitati de adresare

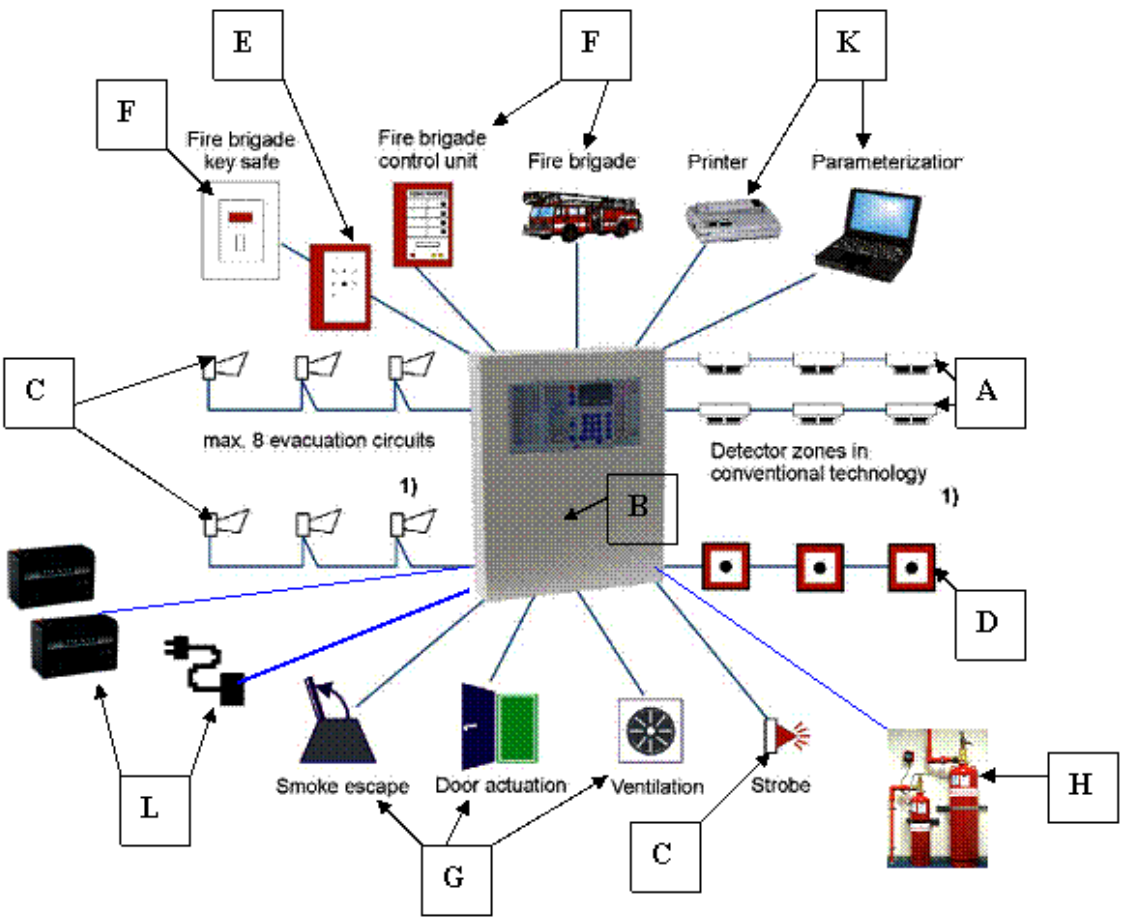
Centrale analogic adresabile – dispun de bucle analogice adresabile cu un numar de adrese si protocoale de comunicatie specifice fiecarui producator.



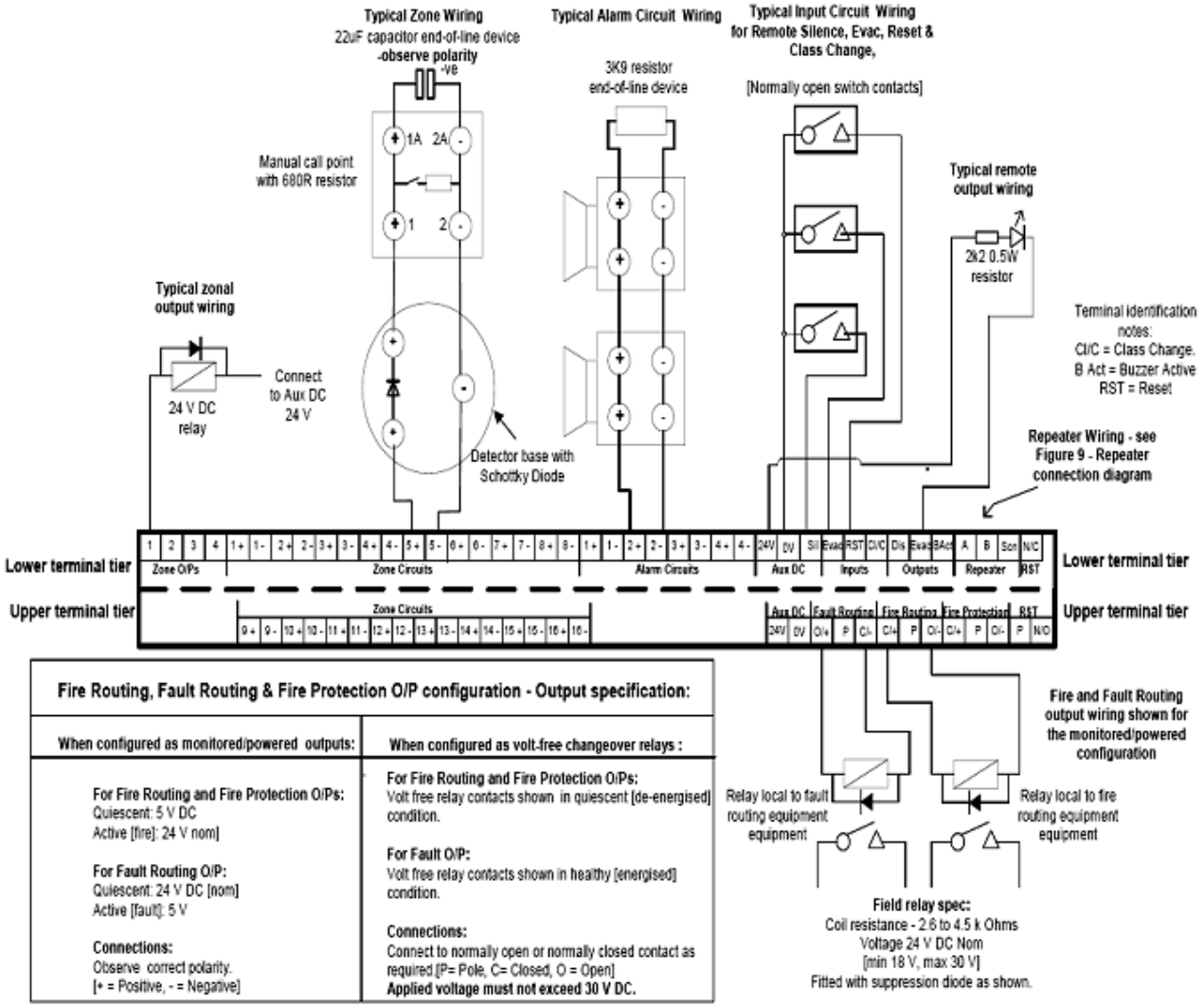
SCHEMA INSTALATIE DE SEMNALIZARE A INCENDIILOR

LEGENDA:

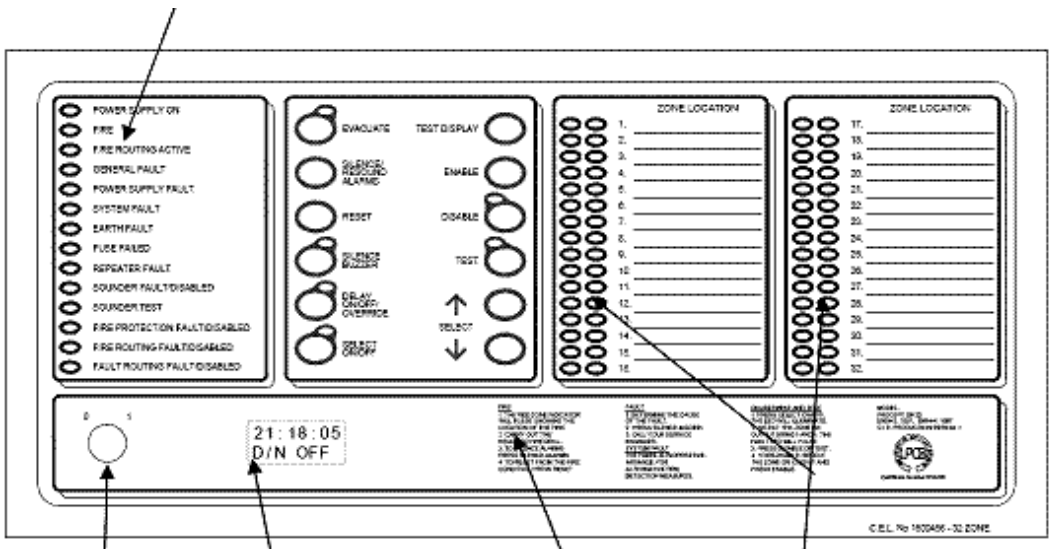
A- Detector (oare) de incendiu
B- Echipament de control si semnalizare (centrala de semnalizare)
C- Dispozitiv (e) de alarma incendiu
D- Declansator (oare) manual (e) de alarma (butoane de semnalizare)
E- Dispozitiv de transmisie alarma incendiu
F- Statie de receptie alarma incendiu
G- Comanda sistemelor automate de protectie impotriva incendiilor
H- Echipament de protectie impotriva incendiu sau instalatie de stingere
J - Dispozitiv de transmisie semnal de defect
K – Statie de receptie semnal de defect
L – Echipament de alimentare cu energie



EXEMPLU – SCHEMA DE CONECTARE CENTRALA CONVENTIONALA



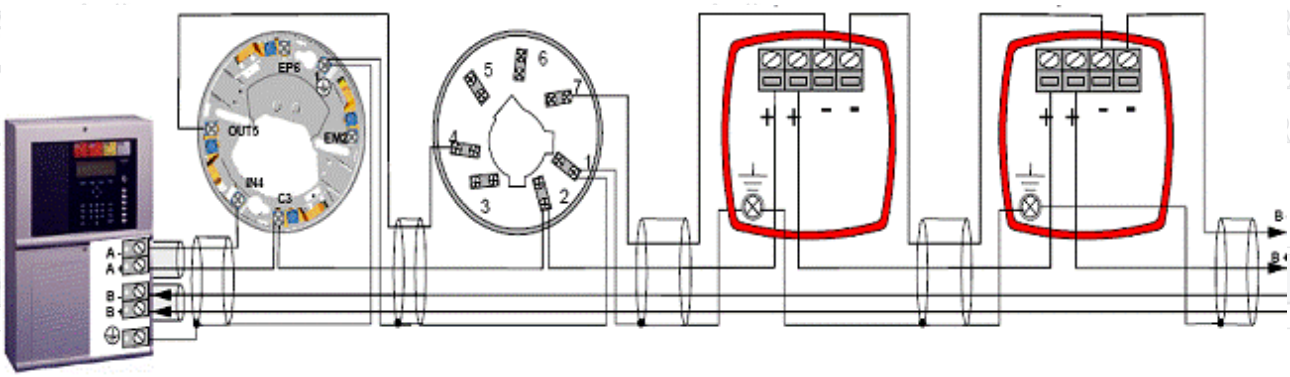
EXEMPLU – INDICATOARE SI COMENZI PE PANOUL FRONTAL AL CENTRALEI

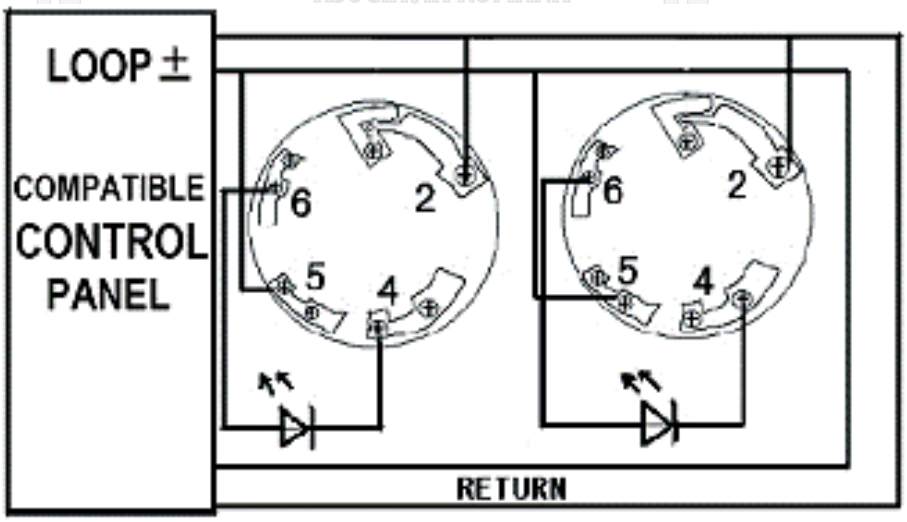


EXEMPLU Semnificatia indicatoarelor

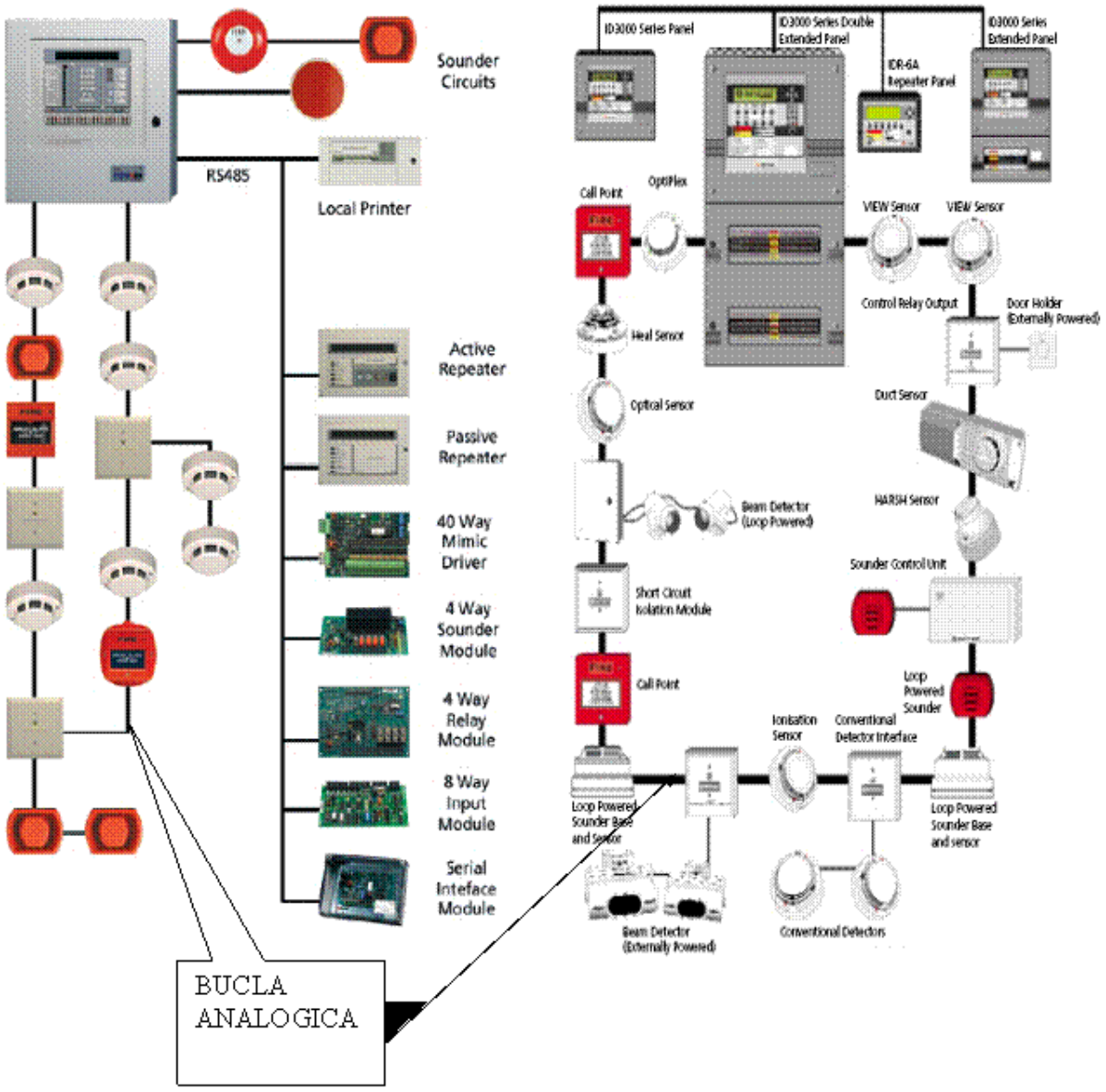
General Indicator Section		
Indicator Description	**Indication Colour**	**Operating Condition**
Power Supply On	Green	Illuminates Steady for Mains or Standby power On.
Fire	Red	Flashes on any new fire alarm condition, changing to a steady indication on operation of Silence Alarms.
Fire Routing Active	Red	Illuminates Steady when the Fire Routing Output is active.
General Fault	Yellow	Flashes for any fault condition.
Power Supply Fault	Yellow	Flashes for mains or standby power supply/charge fault
System Fault	Yellow	Illuminates Steady to indicate Microcontroller or Memory Failure. Flashes to indicate Engineer's Configuration Mode active.
Earth Fault	Yellow	Flashes for any positive or negative power supply earth fault.
Fuse Fault	Yellow	Flashes for any auxiliary supply fuse failure
Repeater Fault	Yellow	Flashes for any Repeater fault or repeater communication fault,
Sounder Fault/Disabled	Yellow	Flashes for any sounder fault. Steady for sounders disabled.
Sounder Test	Yellow	Illuminates Steady while sounder walk test is active.
Fire Protection Fault/Disabled	Yellow	Flashes for a fault on the Fire Protection Output. Steady when Fire Protection Output is disabled.
Fire Routing Fault/Disabled	Yellow	Flashes for a fault on the Fire Routing Output. Steady when Fire Routing Output is disabled.
Fault Routing Fault/Disabled	Yellow	Flashes for a fault on the Fault Routing Output. Steady when Fault Routing Output is disabled.

Exemplu ARHITECTURA ANALOGIC ADRESABILA

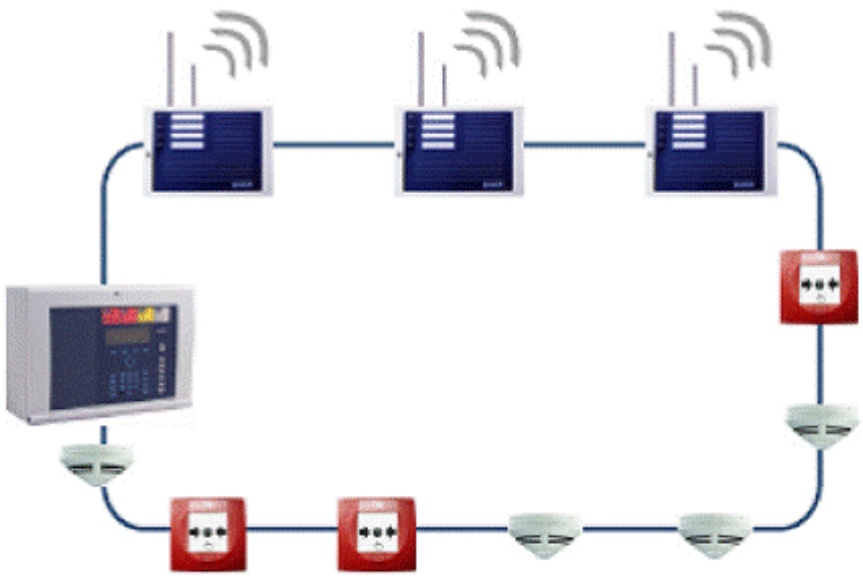


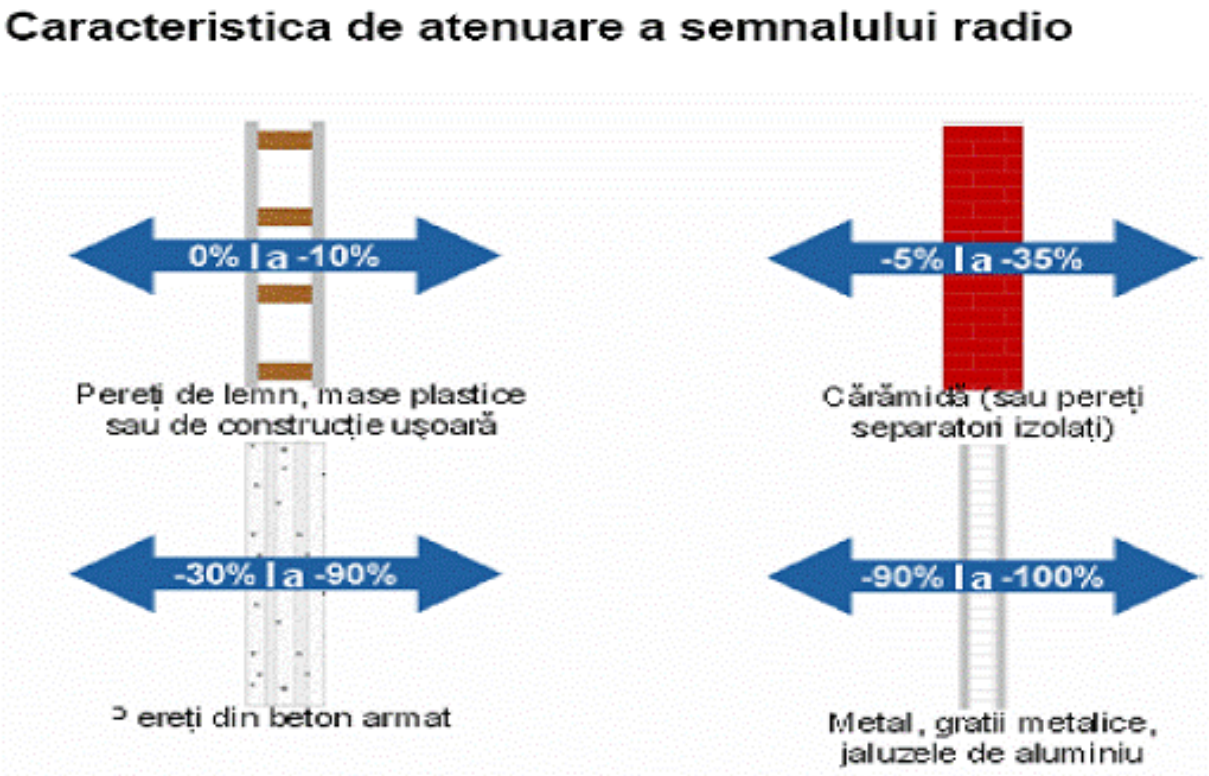


TYPICAL WIRING DIAGRAM



ARHITECTURI UZUALE CENTRALE SEMNALIZARE ANALOGIC ADRESABILA – CAI DE TRANSMISIE CABLATE





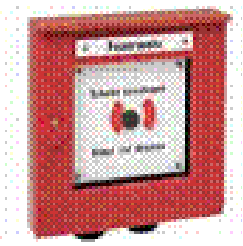
ARHITECTURA UZUAL CENTRALE SEMNALIZARE ANALOGIC ADRESABILA – CAI DE TRANSMISIE RADIO

Declansatoare manuale de alarma (descriere in EN 54-11)

Rolul functional al acestui dispozitiv este initierea unui semnal de alarma la actionarea butonului. Din acest motiv locul de amplasare trebuie sa fie usor accesibil. Normativele in vigoare impun o inaltime de montaj de 1,2 – 1,5 m fata de pardoseala. Pentru a se asigura o buna vizibilitate culoarea rosie si inscriptionarea intuitiva (text si/sau simbol) permit deosebirea de alte dispozitive cu actionare manuala.

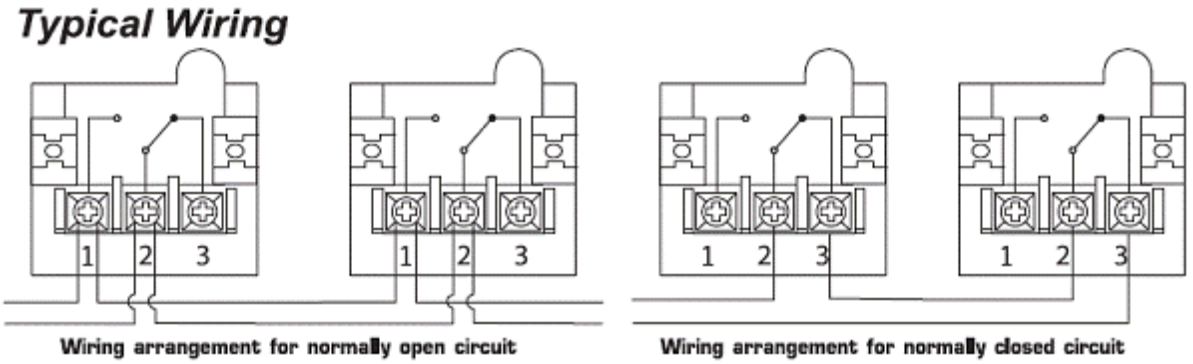
Amplasarea declansatoarelor manuale se face astfel incit sa nu fie nevoie sa se parcurga mai mult de 30 de metri pina la cel mai apropiat buton. Pentru cladiri inalte, foarte inalte, aglomerari de persoane sau pentru cladirile ce gazduiesc persoane cu handicap locomotor distanta maxima pina la cel mai apropiat buton se reduce la 20 de metri. Pozitionarea in cladire se face pe caile de evacuare la interiorul sau exteriorul fiecarei usi, pe scara de evacuare (paliere sau cai de acces la scara) si la fiecare iesire spre exterior. Suplimentar ele pot fi amplasate in apropierea spatiilor cu risc mare de incendiu.

Constructiv declansatoarele manuale sunt realizate astfel incit sa isi pastreze functionalitatea in conditiile de mediu in care sunt amplasate. Conditii de mediu diferite au condus la aparitia unei game constructive variate (de interior, de exterior, pentru medii Ex, pentru medii corozive etc.)

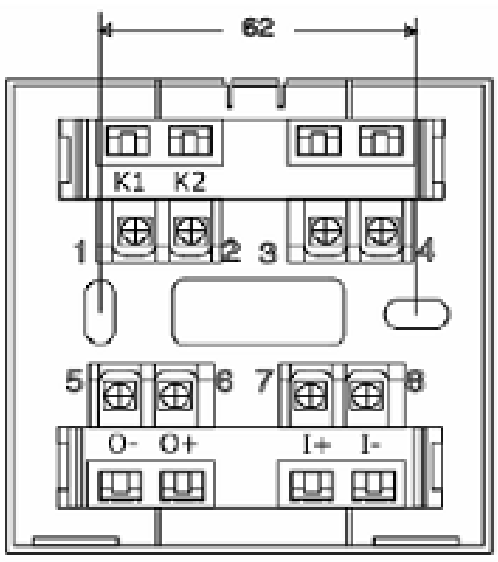




Declansatoarele manuale la care actionarea se realizeaza prin spargerea geamului nu pot fi readuse in starea initiala decit prin inlocuirea acestuia. Din acest motiv vor fi considerate dispozitive neresetabile.

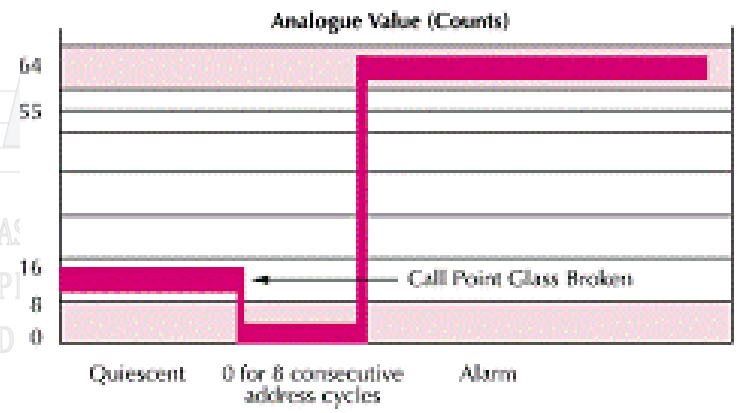
Conectarea la instalatia de semnalizare a incendiilor se realizeaza prin cai de transmisie specifice (uzual cablu sau radio) asigurindu-se transmiterea informatiei de stare in formatul adecvat. Astfel in



instalatiile de detectie conventionale scaderea rezistentei electrice produce initierea starii de alarma. Pentru sistemele analogic adresabile se transmite semnalul ce identifica declansatorul manual si starea sa (normala sau in alarma la actionare).Exemplu de cablare declansatoare manuale (aplicatii conventionale)
Exemplu de cablare declansatoare manuale (aplicatii analogic adresabile)



I+/I- (7-8) conectoare intrare bucla
O+/O- (5-6) conectoare iesire bucla
K1K2 (1-2/3-4) contact suplimentar (nc/no)



Exemplu de semnal transmis analogic

Detectoare automate de incendiu – CLASIFICARE (conf EN 54-1/SR EN 54-1)

Din punct de vedere al formei zonei de detectie detectoarele pot fi:

Detectorul punctual- Detector care raspunde la parametrul sesizat in vecinatatea unui punct fix
Detector multipunctual - Detector care raspunde la parametrul sesizat in vecinatatea mai multor puncte fixe
Detector liniar- Detector care raspunde la parametrul sesizat in vecinatatea unei linii continue

Din punct de vedere al numarului de parametri monitorizati pot fi:
Detector monosenzor – Detector care raspunde la un parametru al incendiului
Detector multisenzor – Detector care raspunde la mai mult de un parametru al incendiului

Din punct de vedere al marimii sau vitezei parametrului masurat:
Detector static – Detector care initiaza o alarma cind marimea parametrului masurat depaseste o anumita valoare pentru un interval de timp suficient
Detector diferential- Detector care initiaza o alarma cind diferenta intre marimile parametrului masurat in doua sau mai multe locuri depaseste o anumita valoare pentru un interval de timp suficient
Detector de rata de crestere (velocimetric) - Detector care initiaza o alarma cind rata de schimbare a parametrului masurat cu timpul depaseste o anumita valoare pentru un interval de timp suficient

Din punct de vedere al parametrului masurat detectoarele pot fi:
Detector de fum cu camera de ionizare – Detector sensibil la produse de combustie capabile sa afecteze curentii de ionizare din interiorul detectorului
Detector optic de fum - Detector sensibil la produse de combustie capabile sa afecteze absorbtia sau difuzia unei radiatii in domeniul IR, vizibil si/sau ultraviolet a spectrului electromagnetic
Detector de gaz - Detector sensibil la produse de combustie si / sau descompunere termica
Detector de flacara - Detector care raspunde la radiatia electromagnetica emisa de flacarile unui incendiu
Detectoare de caldura – detectoare punctuale statice sau velocimetrice definite de EN 54-5

Din punct de vedere constructiv detectoarele pot fi:
Detector resetabil - Detector care dupa raspuns poate fi reanclansat din satrea sa de alarma in starea de veghe din momentul in care conditiile care au declansat intrarea lui in stare de alarma au incetat fara a fi necesara sa inlocuiasca unul din elementele sale.
Detector neresetabil – Detector care nu poate fi reanclansat fara a se inlocui o componenta a sa.

Principalele tipuri de elemente de detectie (senzori sau detectoare) sunt :

1. **Detectoare de fum.**

Cea mai mare parte a incendiilor produc ca urmare a arderii reziduri solide de mici dimensiuni ce sunt antrenate de curentii de aer ascendenti produsi de procesul exoterm. Suspensia acestor particule solide in aer (uzual denumita fum) afecteaza propagarea luminii producind o atenuare direct proportionala cu numarul de particule pe unitatea de volum. Functie de caracteristicile materialului combustibil si de caracteristicile procesului de ardere variaza dimensiunea particulelor si caractertisticile acestora (culoare, indice de reflexie etc.).
Detectoarele de fum pot fi clasificate astfel:

A) Din punct de vedere al arhitecturii sistemului de detectie:
   a) Detectoare conventionale.
   Sistemele conventionale sunt structurate pe linii de detectie radiale ce suporta in mod uzual pina la 30 detectoare /linie. Detectorul conventional « decide » asupra starii proprii (alarma sau normal)

functie de calibrarea si performantele sale interne. Nu exista posibilitatea modificarii pragurilor de alarma sau de identificare univoca a detectorului in alarma fata de restul detectoarelor de pe linia respectiva.

Nota: pentru sistemele conventionale am intilnit si terminologia de zona de detectie ca fiind echivalenta liniei de detectie.

b) Detectoare conventional adresabile

Similare cu cele conventionale insa permit identificarea univoca a detectorului in alarma in baza unei adrese unice pentru fiecare detector.

c) Detectoare analogice.

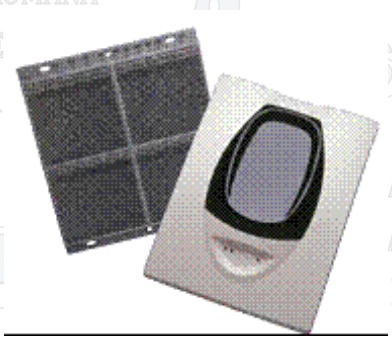
Sistemele analogice permit instalarea pe fiecare bucla analogica a unui detector. Acesta transmite continuu date privind nivelul de fum catre unitatea centrala

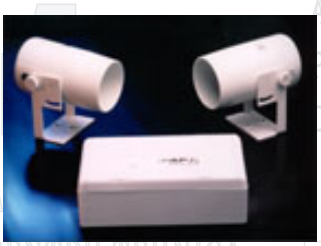
d) Detectoare analogic adresabile – similar dar cu multiple adrese pe fiecare bucla de detectie

B) Din punct de vedere al ariei de acoperire:

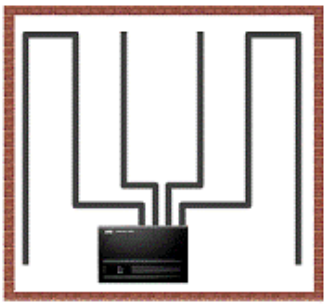
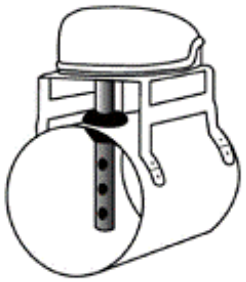
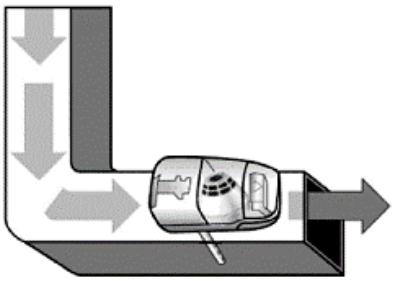
a) Punctuale. Utilizind varii metode de identificare a prezentei fumului transmit informatia (cantitativ sau stare) referitor la punctul unde este amplasat detectorul.

b) Liniare. Transmit informatia referitor la un anume volum aflat intre emitatorul si receptorul detectorului. In literatura de specialitate sunt intilnite si sub denumirea de detectoare spot (beam detector) sau detectoare cu fascicul proiectat (projected beam detector).





c) Cu absorbtie. Prelevind probe din instalatia de ventilatie aceasta clasa de detectoare semnaleaza prezenta fumului in anumite arii de unde sunt prelevate mostrele analizate.



C) Din punctul de vedere al principiului de detectie
- cu camera optica (denumite si detectoare fotoelectrice)
- cu camera de ionizare
-cu dioda laser

2. Detectoare de temperatura

A)Dupa modul de alarmare:
a) cu alarmare la prag de temperatura
b) detectoare velocimetrice (gradient de temperatura - variatie de temperatura/interval de timp)
c) duale – velocimetric si prag

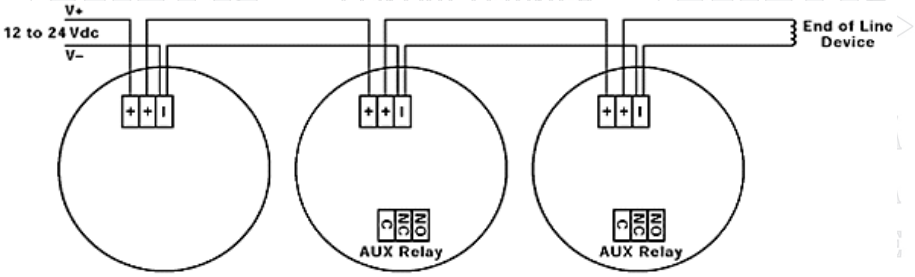
B)Dupa tip constructiv al sistemului:
a) conventionale
b) adresabile analogice

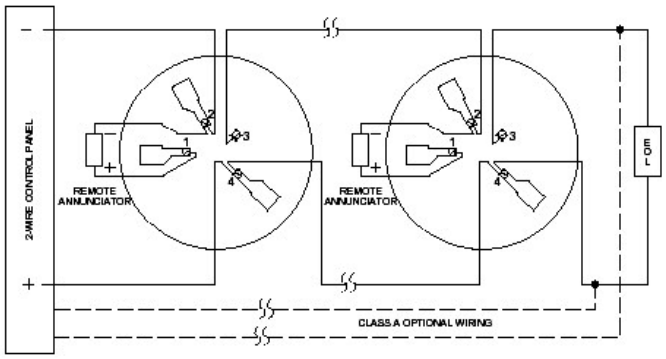
3. Detectoare speciale

In aceasta categorie pot fi incadrate detectoarele atipice (denumite uzual detectoare combinate sau multicriteriale) ce utilizeaza principii fizice si chimice diferite pentru a decela cu o mare acuratete prezenta unui incendiu. Curent ele au microprocesor incorporat si algoritmi de detectie si verificare proprii.

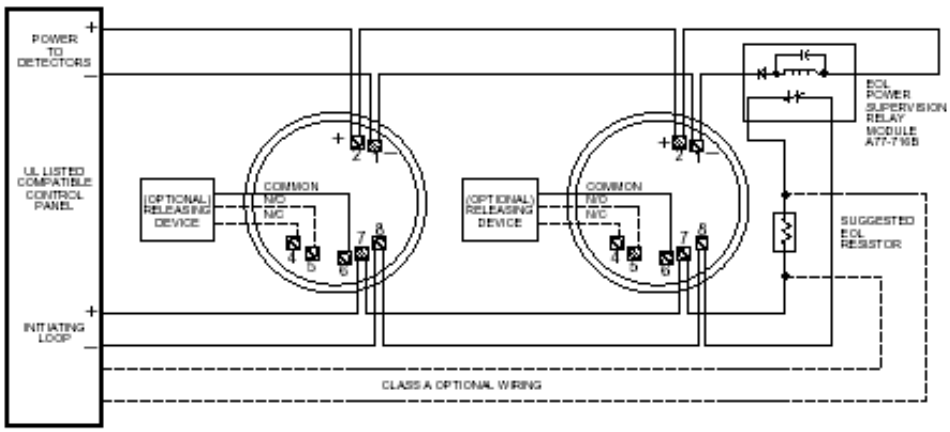
Nota: Nu au fost tratate detectoarele “stand alone” ce nu impun prezenta unei unitati centrale si a unui cablaj.

Cablare- Exemplu de cablaj conventional pe 2 fire (baze diferite)

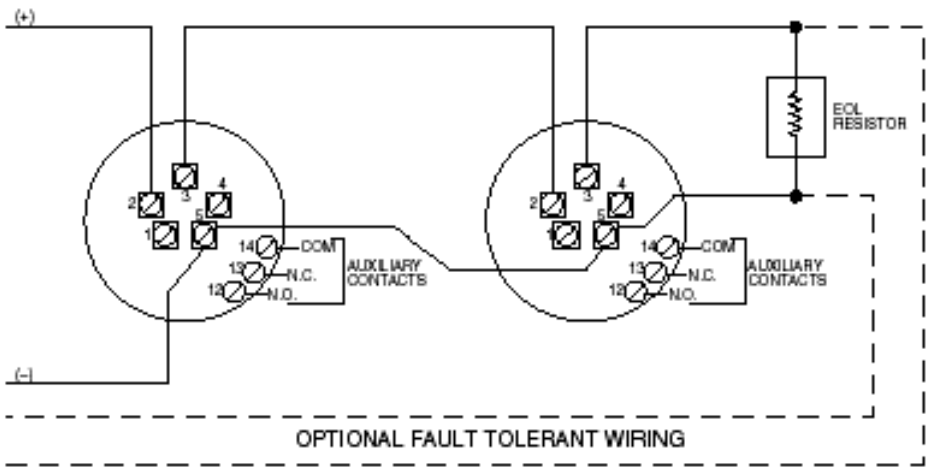




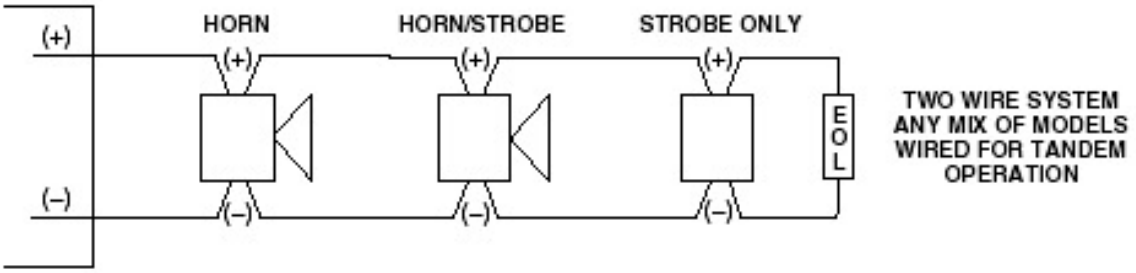
CABLARE PE 4 FIRE



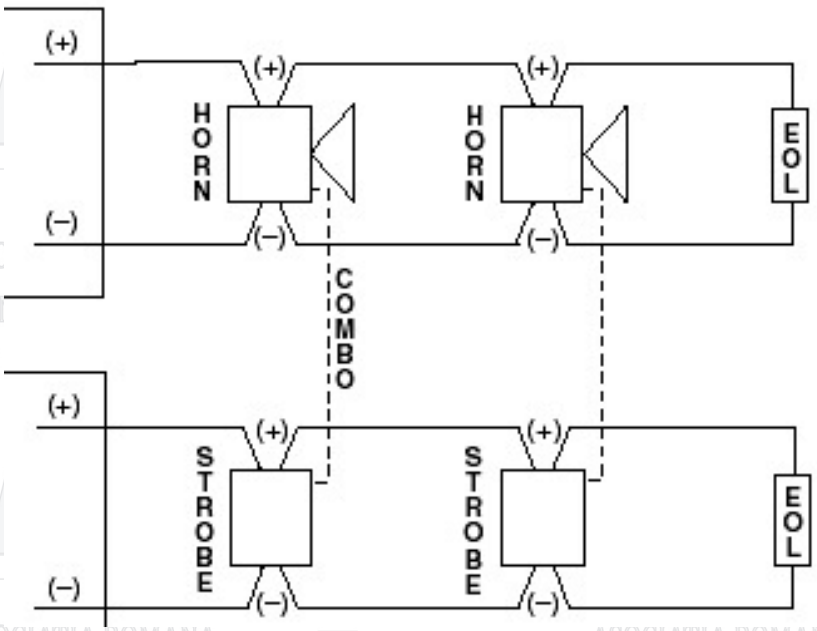
CABLARE CU TOLERANTA LA DEFECTE (intrerupere)



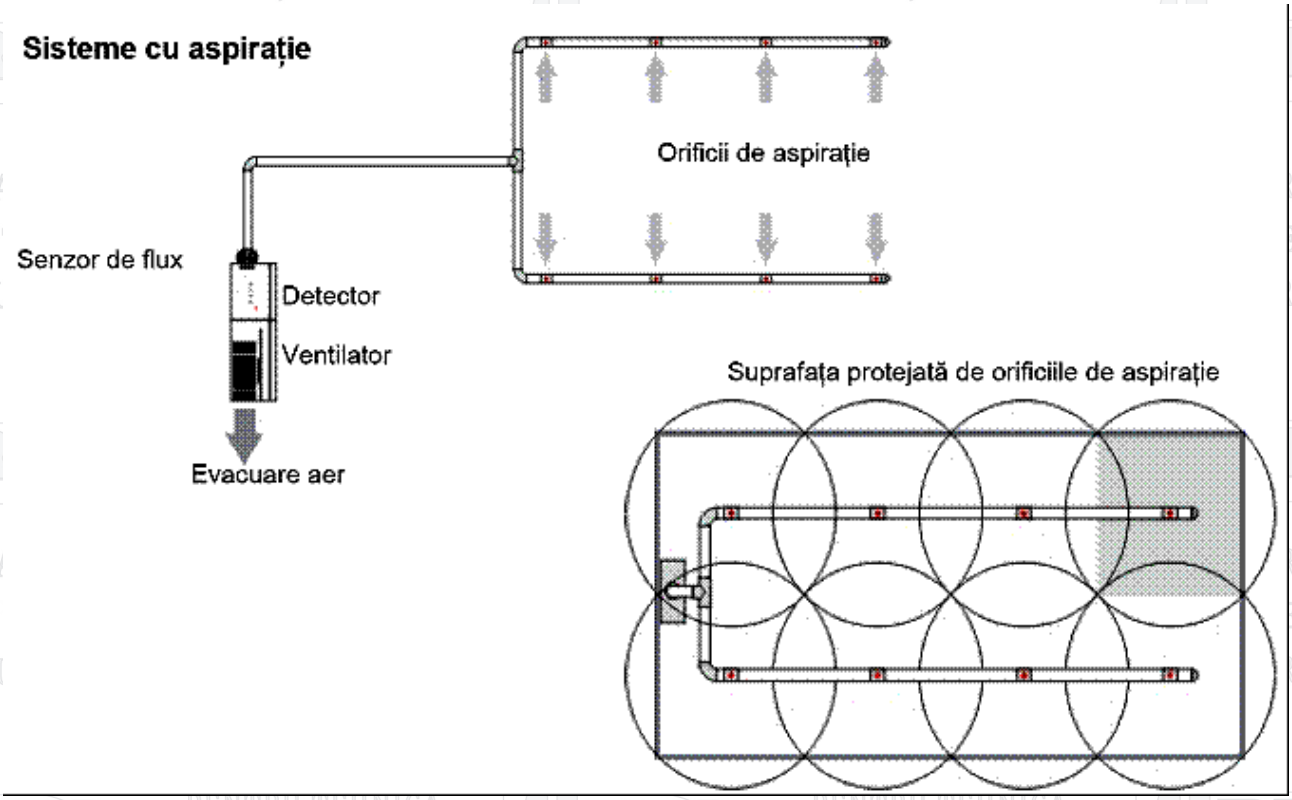
Schema conexiuni circuit de alarmare conventional pe 2 fire cu rezistenta cap de linie



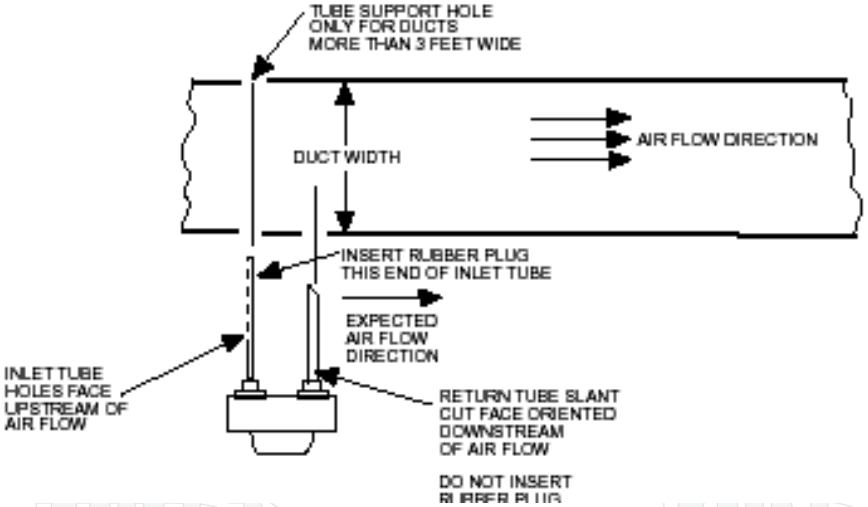
Schema conexiuni circuit de alarmare conventional pe 4 fire cu rezistente cap de linie pe fiecare circuit de alarmare



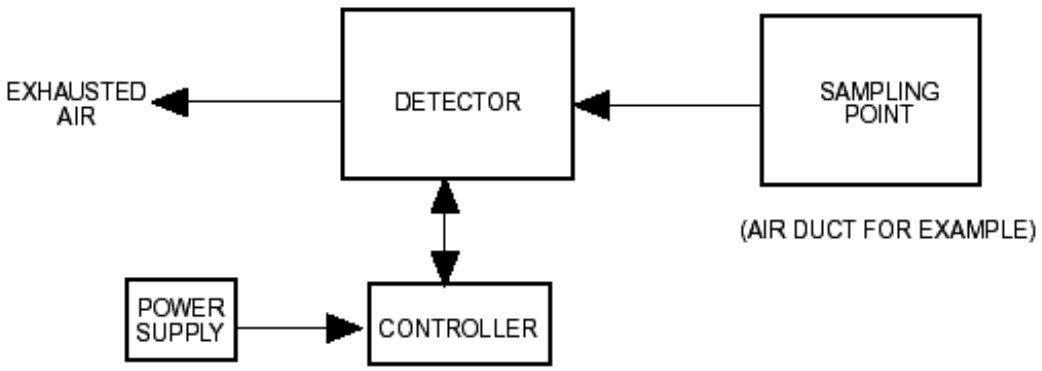
Sisteme cu aspirație



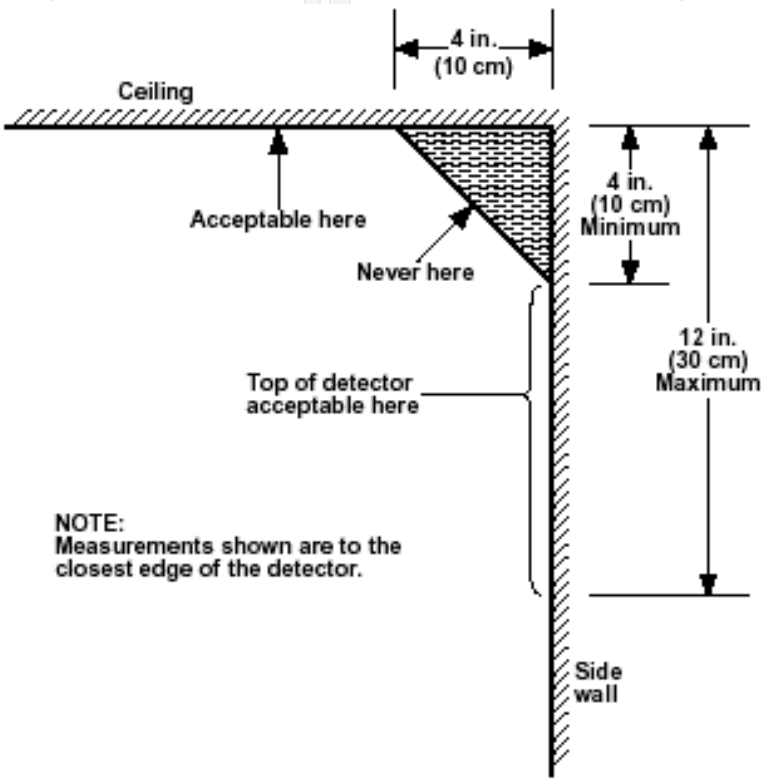
SCHEMA DE PRINCIPIU DETECTOR CU ABSORBTIE – montare pe tubulatura



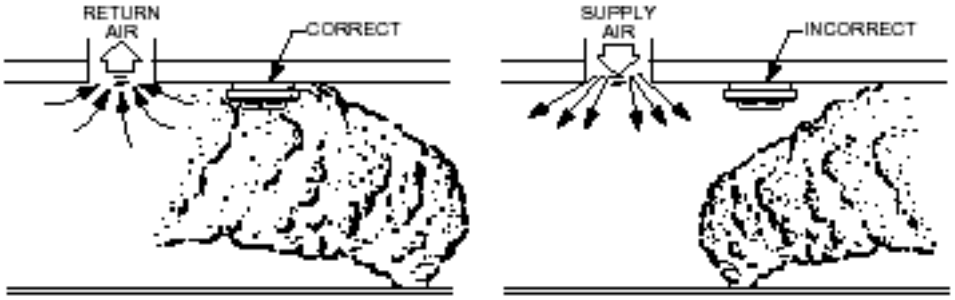
APLICATIE TIPICA DETECTOR CU ABSORBTIE



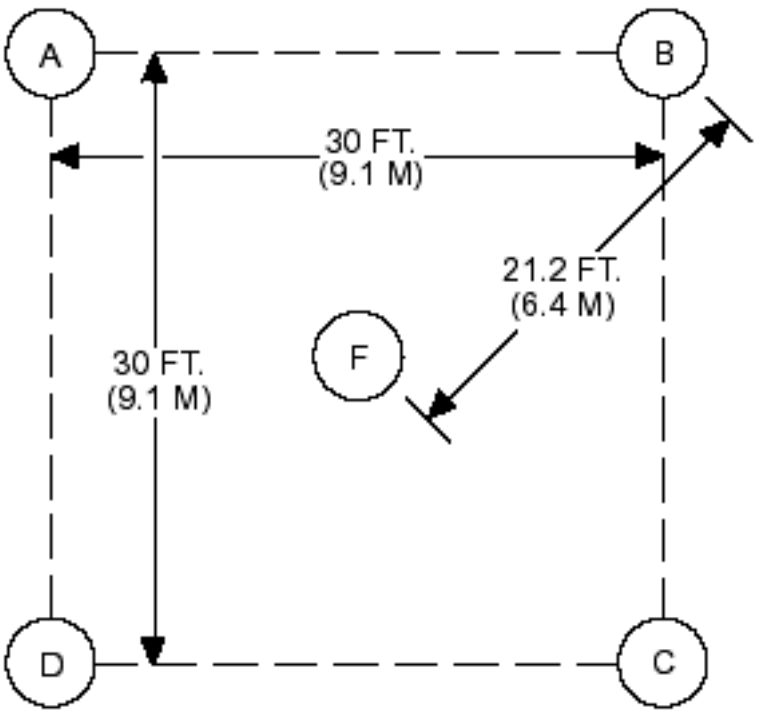
AMPLASARE DETECTOARE PUNCTUALE



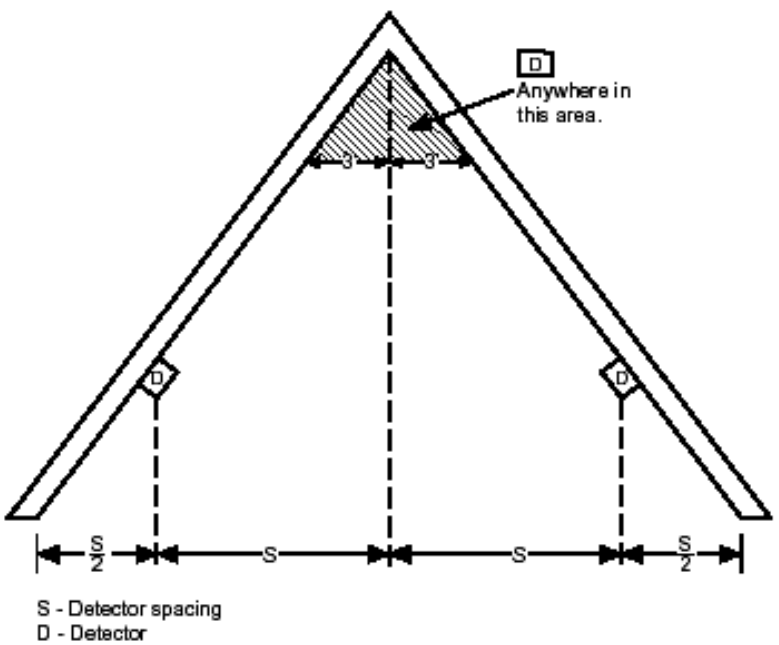
AMPLASARE DETECTOARE PUNCTUALE REFERITOR LA VENTILATIE



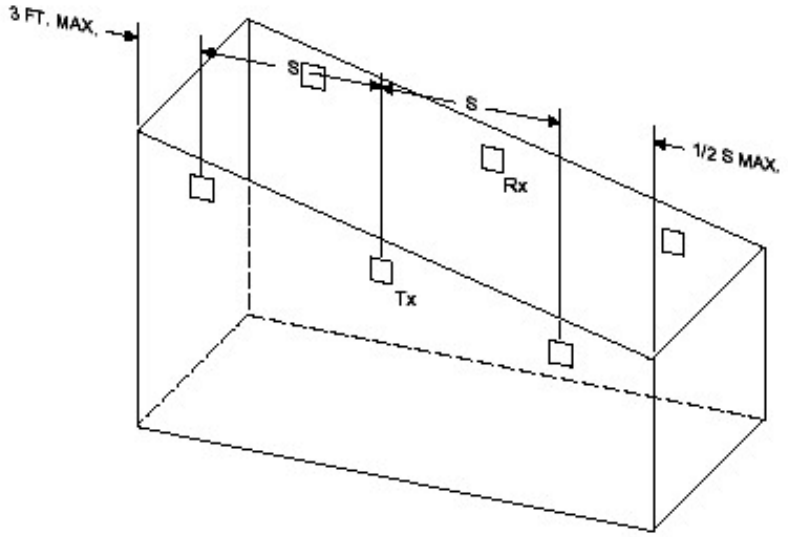
EXEMPLU SPATIERE DETECTOARE (TAVAN PLAN)



EXEMPLU AMPLASARE DETECTOARE PUNCTUALE (TAVAN IN 2 APE)

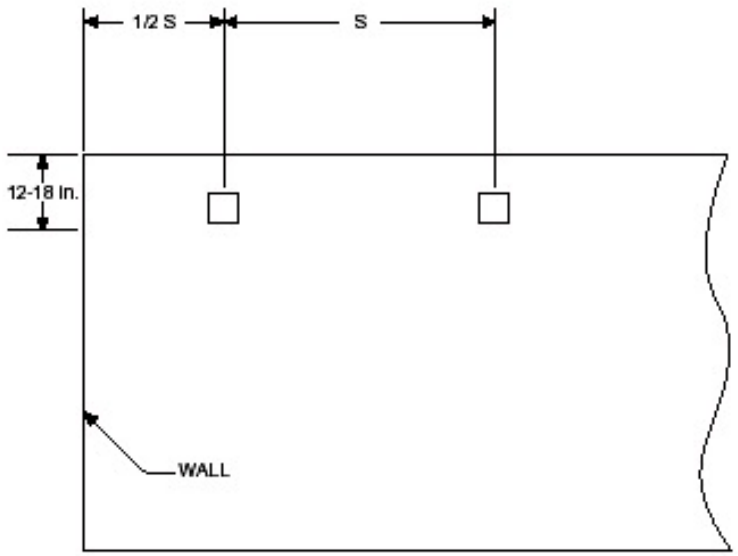


Model de amplasare a detectoarelor liniare pentru tavane inclinate

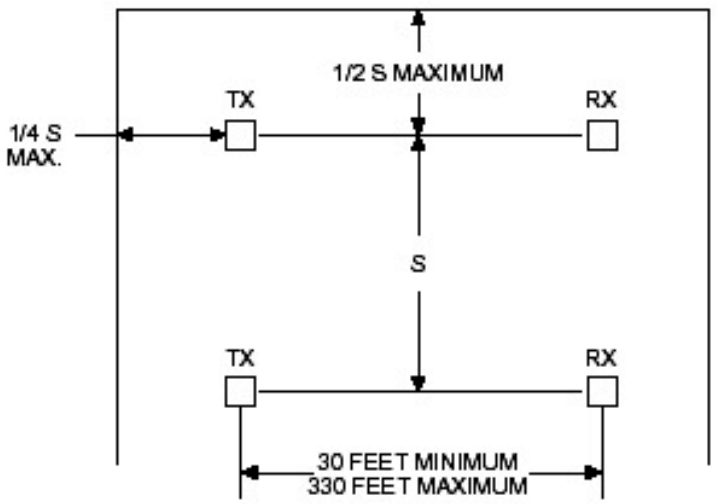


VEDERE IZOMETRICA

Model amplasare detectoarelor liniare pentru tavane plane

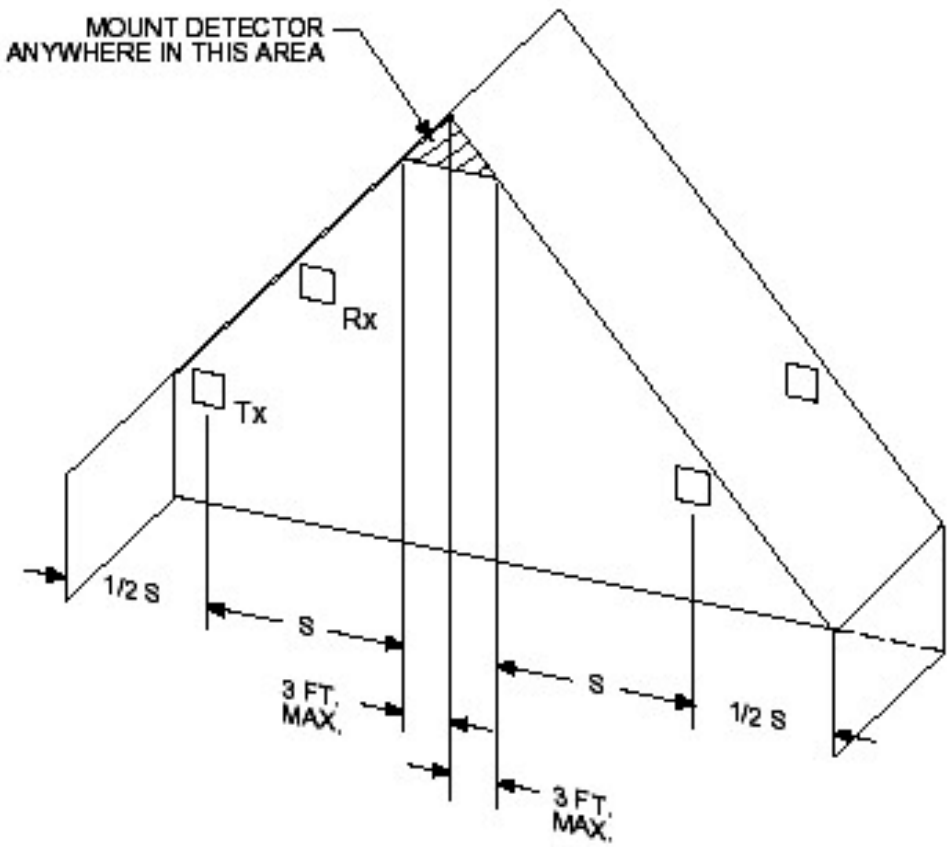


SECTIUNE

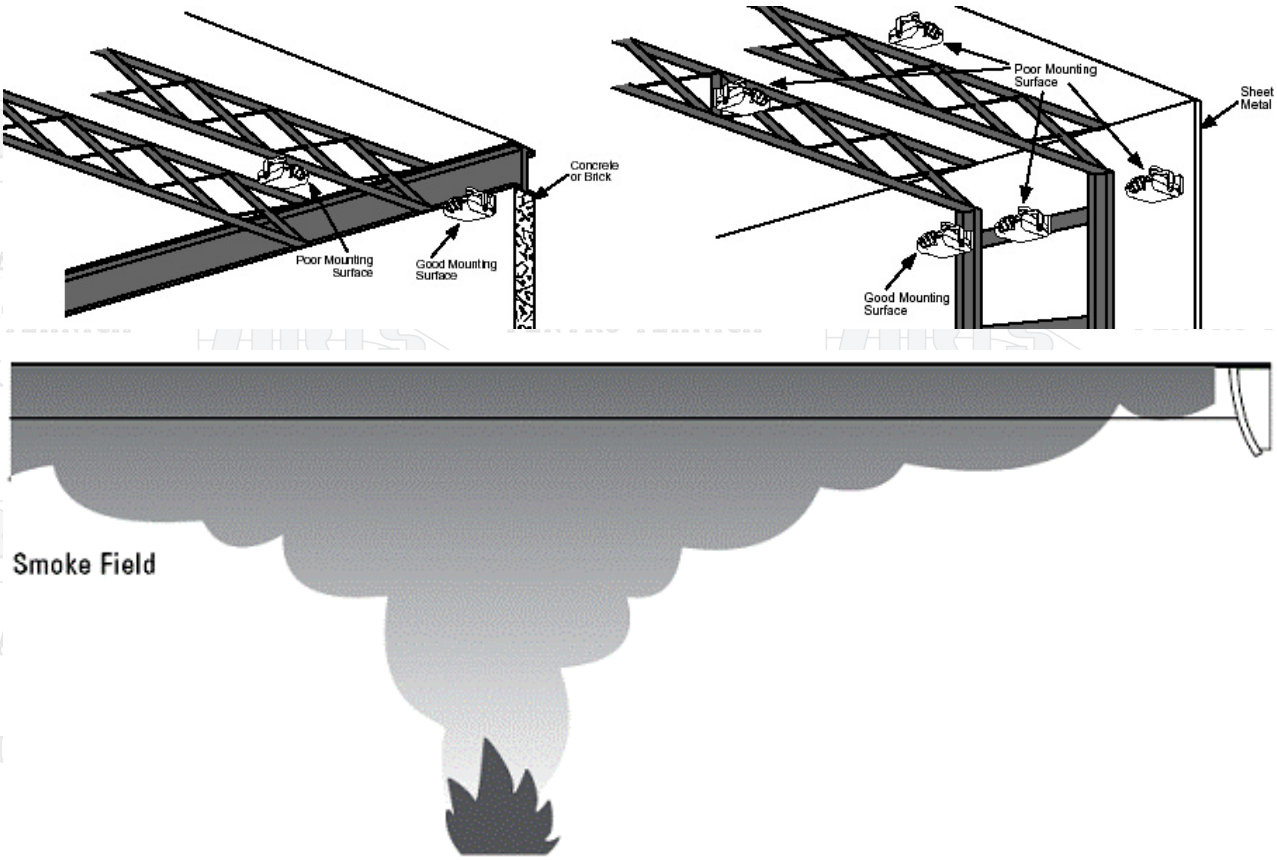


VEDERE DE SUS

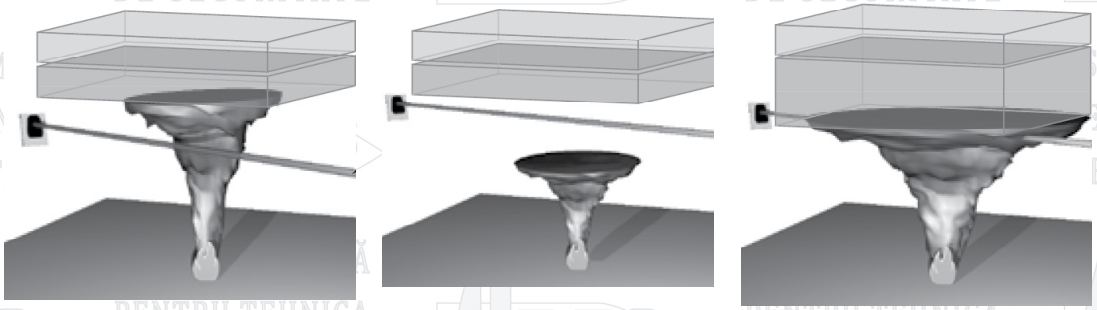
Model amplasare detectoarelor liniare pentru tavane in doua ape



Amplasare corecta/gresita detectoare liniare din punct de vedere mecanic (rigiditate)

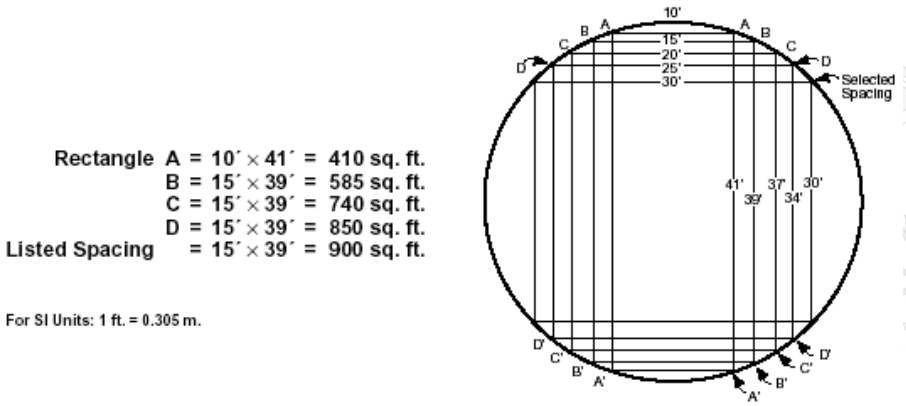


Sectiune prin camera protejata cu detector optic liniar



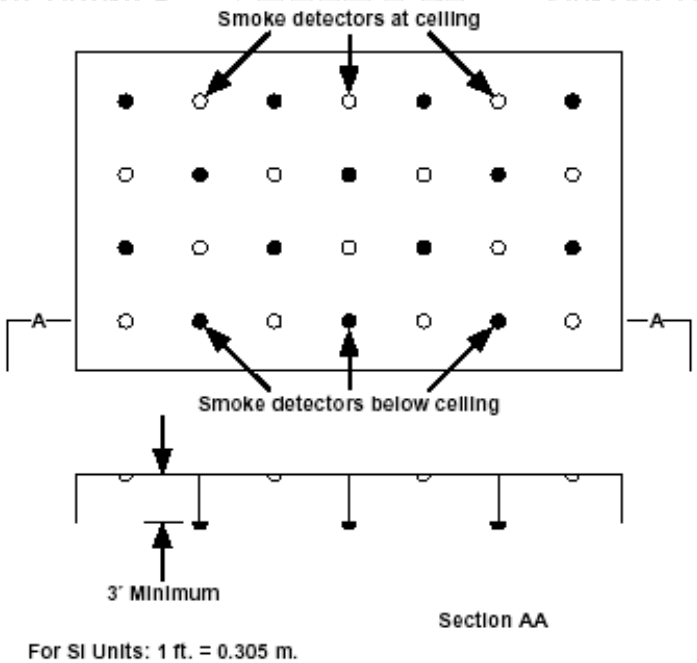
Efectele stratificarii aerului asupra conului de dispersie a fumului. Scenarii de amplasare.

EXEMPLU DE VERIFICARE A ARIEI DE ACOPERIRE



Nota: 1 detector este suficient pentru oricare suprafata inscrisa in cercul de detectie
Aria de detectie a unui detector este specifica fiecarui producator. Uzual este intre 50 si 100 metri patrati.

SPATIERE DETECTOARE DE FUM IN MONTARE ALTERNANTA
(pentru spatii inalte)



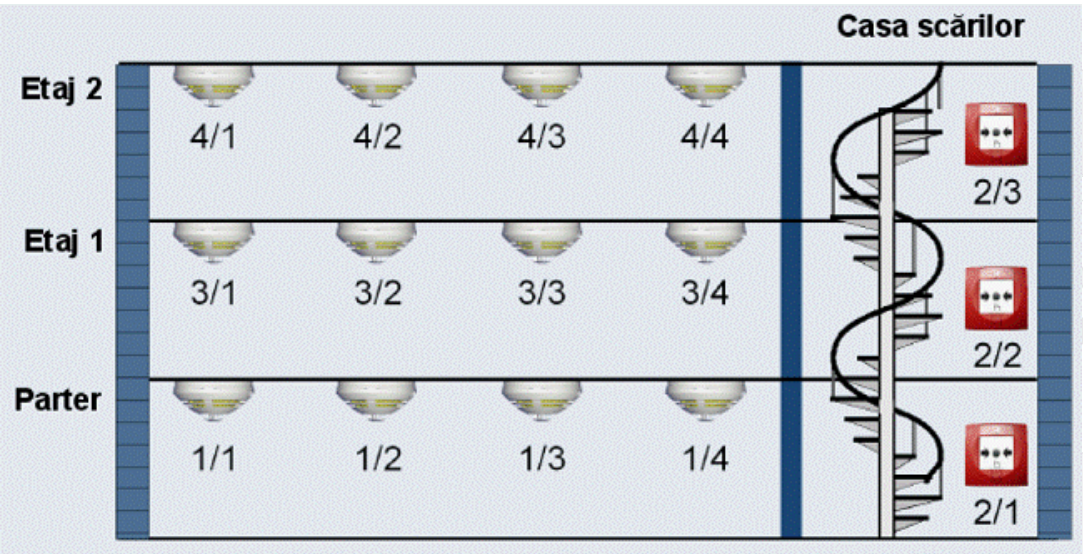
Nota: Acest mod de amplasare este folosit pentru a creste viteza de detectie prin evitarea fenomenului de stratificare termica.

Zonarea Cladirilor

Impartirea unei cladiri in zone are ca scop identificarea rapida a locului de origine al alarmei in baza indicatiilor centralei de semnalizare.

REGULI

1. Aria desfasurata a unei zone trebuie sa fie mai mica sau egala cu 1600 metri patrati
2. Distanta de cautare in interiorul unei zone sa fie mai mica sau egala cu 30 m
3. Intr-o zona pot fi incluse mai multe incaperi daca:
   a) suprafata lor nu depasete 400 metri patrati, numarul lor e mai mic de 5 iar incaperile sunt invecinate
   b) incaperile sunt invecinate cu acces usor intre ele, suprafata totala nu depaseste 1000 metri patrati si in centrala de semnalizare sau in incaperi sunt prevazuti avertizori de alarma pentru spatiul afectat de incendiu
4. Fiecare zona trebuie limitata la un nivel al cladirii exceptind:
   a) zona este casa scarii, putul liftului sau o structura similara ce se intinde pe mai mult de un nivel
   b) suprafata cladirii este mai mica de 300 metri patrati.



Alegerea detectoarelor si declansatoarelor manuale

Selectarea tipului de detector optim a fi utilizat pentru un anumit spatiu trebuie sa tina seama de urmatoarele criterii:

1. Materialele combustibile prezente in spatiul protejat si clasa de reactie la foc a acestora
2. Configuratia geometrica si inaltimea spatiului protejat
3. Prezenta si efectele instalatiilor de incalzire si ventilatie
4. Conditiile de mediu tipice spatiului protejat
5. Riscurile aparitiei alarmelor false

In multe cazuri un singur tip de detector nu poate asigura un raspuns optim la toti parametrii amintiti caz in care se recomanda pentru atfel de cazuri detectoare ce actioneaza pe principii fizice diferite sau cu multsenzor.

Normativul I18 precizeaza ca pentru protectia persoanelor din cladiri publice. detectorul de uz general este detectorul de fum celelalte tipuri de detectoare utilizindu-se suplimentar sau numai in acele spatii in care incendiul se manifesta prin crestere de temperatura, flacari sau are o evolutie rapida.
Caile de evacuare si traseele de circulatie comune in caz de incendiu se protejeaza cu detectoare de fum.

Amplasarea detectoarelor automate

Amplasarea detectoarelor se face astfel incit produsele degajate de incendiu din suprafata supravegheata sa ajunga la detectoare fara dilutie, atenuare sau intirziere. Fieacre compartiment antiincendiu va fi prevazut cu minim un detector. Astfel o incapere prevazuta cu tavan fals si cu podea falsa cu aria inscrisa in aria de supraveghere a unui detector va fi echipata minim cu 3 detectoare.

Cele trei cerinte specificate si legile fizicii dicteaza amplasarea fiecarui tip de detctor. Pentru a demonstra cele afirmate vom analiza cerintele privind amplasarea unui detector de caldura static punctual. Astfel aria supravegheata de un astfel de detector se limiteaza la aria compartimentului antiincendiu in care este montat (schimbul de caldura cu compartimente invecinate fiind neglijabil). Inaltimea de montaj maxima admisa de 7.5 m este in strinsa corelare cu timpul necesar pentru a atinge temperatura de initiere a alarmei. Montajul pe tavan sau la o distanta maxima de 5% de acesta are ca scop patrunderea cit mai rapida in detector a fluxului de aer cald. Distanta fata de pereti de minim 500 de mm sau fata de orice alte obstacole are ca scop evtarea blocarii circulatiei aerului.

Factori ce influenteaza zona de supraveghere a unui detector:

- performanta detectorului (suprafata protejata specificata de producator)
- distanta orizontala dintre orice punct al spatiului supravegheat si detector
- distanta fata de pereti
- inaltimea si configuratia tavanului
- ventilatia si miscarile aerului in aria supravegheata
- obturatiile miscarii de convectie a produselor de ardere

Reguli Generale

1. Detectoarele de fum si caldura se monteaza de regula pe tavan sau cu elementele sensibile la distante mai mici de 5% din inaltimea incaperii de acesta.

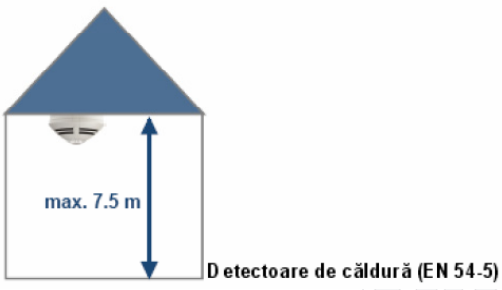
2. Daca exista gradienti de temperatura si inaltimea de stratificare se poate determina se monteaza detectoare **suplimentare** la aceasta inaltime.

DISTANTE ORIZONTALE RECOMANDATE PENTRU DETECTOARE FUNCTIE DE INALTIMEA INCAPERII						
	Inaltimea incaperii h (m)					
TABELUL 1	h<4,5m	4,5m<h<6 m	6m<h<8 m	8m<h<11 m	11m<h<25 m	h>25 m
Detectoare de caldura clasa 1*	5	5	5	Nu se utilizeaza	Nu se utilizeaza	Nu se utilizeaza
Detectoare de caldura clasa 2*	5	5	Nu se utilizeaza	Nu se utilizeaza	Nu se utilizeaza	Nu se utilizeaza
Detectoare de caldura clasa 3*	5	Nu se utilizeaza	Nu se utilizeaza	Nu se utilizeaza	Nu se utilizeaza	Nu se utilizeaza
Detectoare de fum punctuale	7,5	7,5	7,5	7,5	Nu se utilizeaza	Nu se utilizeaza
Detectuare de fum liniare	7,5	7,5	7,5	7,5	7,5 cu al doilea start de detectoare la 1/2 h spatiu	Nu se utilizeaza

Distantele de 5 si 7,5 m sunt distante orizontale considerate intre orice punct al spatiului protejat la cel mai apropiat detector (cu exceptia tavanelor inclinate).

Pe caile de evacuare distantele din tabel se reduc cu 10%.

* Nota - Clasa 1 detectoare de caldura – corespondent clasa A1 EN 54-5
- Clasa 2 detectoare de caldura – corespondent clasa A2 EN 54-5
- Clasa 3 detectoare de caldura cu temperatura de initiere 54-78 grade recomandat de I18 nu are corespondent in EN 54-5



Detectoare de căldură (EN 54-5)

Detectoare de fum (EN 54-7)

3. Daca prin ventilatie se produc mai mult de 4 schimburi de aer pe ora se vor monta detectoare suplimentare fata de numarul necesar fara prezenta ventilatiei

4. Nu se monteaza detectoare in apropierea gurii de refulare a vaentilatiei. Daca ventilarea se produce prin perforatii in tavan se va asigura o arie cu o raza de 600 mm neperforata in jurul detectorului

5 Distanta de la detector fata de orice perete sau obstacol minima neobstructionata trebuie sa fie de 500 mm.

6 Pentru tavanele cu denivelari grinzi sau plansee casetate se aplica urmatoarele:

- grinzi mai inalte decit 5% din inaltimea incaperii vor fi considerate pereti despartitori (exceptie fac cazurile in care se poate demonstar ca acestea nu intirzie apreciabil initierea detectoarelor)
- in cazul planseelor casetate o anumita zona dintre casete poate fi supravegheata de un singur detector. Volumul intern al unei casete acoperite de un singur detector nu trebuie sa depaseasca produsul a 6 metri patrati cu inaltimea grinzii pentru detectoarele de caldura si 12 metri patrati cu inaltimea grinzii pentru detectoarele de fum.
- daca denivelarile tavanului sunt mai mici de 5% din inaltimea incaperii se considera tavan plan.

7. Pentru tavane inclinate o inclinatie de 1 grad a pantei se maresc distantele din tabelul 1 cu 1%.

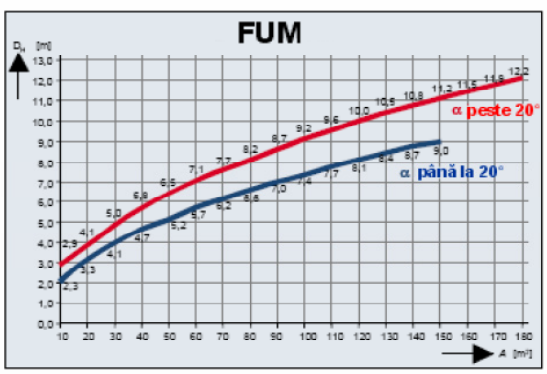
8. Daca acoperisul este in panta sau cu iluminatoare se vor monta detectoare in fiecare virf de coama.

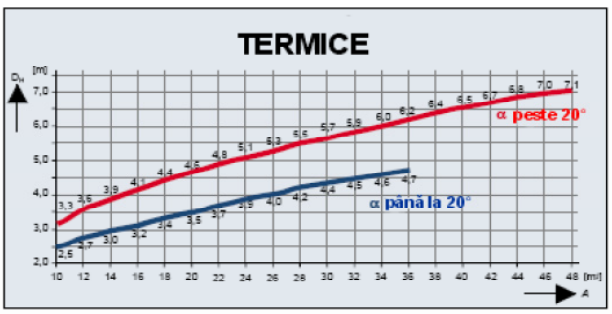
Înălțimea incintei	Detectoare de fum SR EN 54-7	Detectoare de căldură EN 54-5: 1989-09			Detectoare de flacără SR EN 54-10
		Clasa 1	Clasa 2	Clasa 3	
		Detectoare de căldură SR EN 54-5: 2002			
		Clasa A1	Clasele A2, B, C, D, E, F şi G	------	
Până la 45 m	Neadecvat	Neadecvat	Neadecvat	Neadecvat	Adecvat
Până la 16 m	Neadecvat	Neadecvat	Neadecvat	Neadecvat	Adecvat
Până la 12 m	Adecvat	Neadecvat	Neadecvat	Neadecvat	Adecvat
Până la 7,5 m	Adecvat	Adecvat	Neadecvat	Neadecvat	Adecvat
Până la 6 m	Adecvat	Adecvat	Adecvat	Neadecvat	Adecvat
Până la 4,5 m	Adecvat	Adecvat	Adecvat	Adecvat	Adecvat

Dispunerea detectoarelor punctuale de fum şi de căldură

Tipul detectorului	Înălțime *h*	Lungime platformă *l*	Lățime platformă *b*	Suprafață platformă *F*
Detector termic EN 54-5	< 7,5 m	> 2 m	> 2 m	> 9 m^2
Detector de fum EN 54-7	< 6 m	> 2 m	> 2 m	> 16 m^2
	> 6 m p.la 12 m	> 3,5 m	> 3,5 m	> 31,5 m^2

Spații orizontale între detectoare conform SR EN 54-7 (fum) şi SR EN 54-5 (termice)





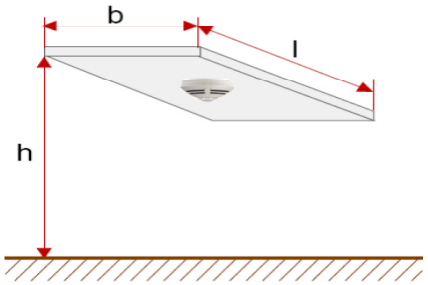
A	Suprafața maximă supravegheată de un detector
D_H	Distanța orizontală maximă de un punct oarecare al tavanului la cel mai apropiat detector
α	Unghiul de înclinare al tavanului/acoperişului. Pentru înclinări diferite se va considera cea mai mică înclinare

Amplasarea detectoarelor in spatii multietajate

Dispunerea detectoarelor punctuale de fum şi de căldură

Tipul detectorului	Înălțime *h*	Lungime platformă *l*	Lățime platformă *b*	Suprafață platformă *F*
Detector termic EN 54-5	< 7,5 m	> 2 m	> 2 m	> 9 m^2
Detector de fum EN 54-7	< 6 m	> 2 m	> 2 m	> 16 m^2
	> 6 m p.la 12 m	> 3,5 m	> 3,5 m	> 31,5 m^2

Echipamentele de alarmare locala pot fi clasificate astfel:



A) Functie de tipul semnalului de avertizare emis

a) optic
b) acustic
c) dual optico-acustic

B) Functie de sistem si mod de conectare

a) conectare pe circuit dedicat de alarmare (cu sau fara monitorizare EOL)
b) conectare prin intermediul unui modul de iesire adresabil (conectare pe bucla adresabila)

Pot exista si alte criterii de clasificare cum ar fi gradul de protectie, tip constructiv al sursei de semnal, intensitate semnal acustic sau optic insa aceste criterii sunt relevante in conditii de utilizare speciale (medii in care se impun anumite restrictii) sau acolo unde exista reglementari specifice (spatii anti-ex, spatii cu vizibilitate redusa sau cu zgomot intens). In majoritatea cazurilor dispozitivele de semnalizare uzuale sunt astfel selectate de catre proiectantul instalatiei incit sa asigure o alarmare locala eficienta pentru spatiul protejat. O nota aparte trebuie acordata redundantei sistemului de alarmare. Astfel toti producatorii unitatilor centrale de avertizare si semnalizare antiincendiu prevad minim doua circuite de semnalizare independente. Pe fiecare circuit se recomanda utilizarea a minim 2 dispozitive de semnalizare distincte astfel incit chiar in cazul in care un dispozitiv se defecteaza sa existe cel putin un dispozitiv functional.

Exceptie de la recomandarea de mai sus fac dispozitivele de semnalizare montate pe bucle adresabile unde chiar in cazul unei intreruperi acidentale dispozitivele vor functiona pe fiecare ramura a buclei. Indiferent de tipul sistemului se recomanda montarea dispozitivelor de semnalizare cu circuite de monitorizare sau cu toleranta la intreruperi.

Alarmarea la distanta se realizeaza in doua moduri:

a) cu suport fizic

In aceasta clasa intra toate dispozitivele de semnalizare la distanta cablate (tip modem comunicator telefonic sau comunicator digital incluzind si dispozitivele de comunicatie in retea)

b) fara suport fizic

Aceasta clasa include gama dispozitivelor de comunicatii wireless (radio, GSM sau pe tehnologii de comunicatii digitale radio criptate)

Esentiala pentru aceste dispozitive de alarmare la distanta este viteza de reactie si disponibilitatea acestuia (functionare in regim S1 24h/24h). Semnalizarea rapida a eventualei intreruperi sau a functionarii defectuoase este un al doilea criteriu de selectie important.

STINGEREA

Instalatiile de stingere au evolut in decursul timpului devenind mai complexe si asigurind o protectie eficienta pentru spatiile asigurate. Este foarte clar ca fiecare instalatie de stingere este destinata a asigura stingerea pentru un caz dat sau pentru o clasa de scenarii de incendiu posibile. Fiecare tip de material combustibil si fiecare tip de incendiu impun o anumita instalatie de stingere sau oricum restring sau interzic anumite solutii tehnice posibile. Astfel unele materiale combustibile (bunuri) pot fi distruse de catre agentul de stingere.

Latura economica are si ea un rol important in selectarea instalatiei adecvate (valoarea bunurilor protejate, costurile instalatiei).

Dimensiunile fizice ale spatiului protejat si forma acestuia pot face ca anumite instalatii de stingere sa fie inaplicabile.

Instalatiile de stingere au si ele dimensiuni diferite functie de agentul de stingere utilizat (caracteristici fizico-chimice) ceea ce restringe aria de aplicabilitate.

Agentul de stingere optim pentru un anumit tip de incendiu sau material combustibil poate fi toxic pentru organismul uman sau nociv mediului ceea ce il va face inutilizabil in spatii ocupate sau va duce la interzicerea utilizarii sale prin legislatie.

Tinind seama de cele de mai sus se observa problematica complexa careia proiectantii de specialitate trebuie sa ii faca fata. In continuare vom prezenta agenti de stingere comuni si aria lor de utilizare.

APA – un agent de stingere eficient ce actioneaza in principal fizic eliminind energia din focar si ridicind punctul de aprindere pentru o gama larga de materiale combustibile.

Avantaje – cost redus agent de stingere, eficienta ridicata in stingerea unei game largi de incendii, 100% nepoluanta – produs ecologic, non toxic – utilizabil in spatii ocupate, necoroziva, disponibilitate ridicata.

Dezavantaje – cost instalatie ridicat, potential distructiva pentru anumite materiale, inadecvata pentru stingerea unor anumite materiale combustibile, conductibilitatea

In stare impura prezinta pericol de electrocutare, nu permite stingerea non distructiva a echipamentelor electronice, dimensiuni instalatie mari, intretinere greoaie

GAZ INERT – AMESTECURI DE GAZE INERTE ATMOSFERICE – aceasta clasa de agenti actioneaza prin reducerea cantitatii de oxigen din spatiul de stins si prin efect fizic de racire la destinderea din recipientii sub presiune.

Avantaje – cost redus agenti de stingere, eficienta ridicata in stingerea unei game largi de incendii, 100% nepoluanta – produs ecologic, non toxic, necoroziv, disponibilitate ridicata.

Dezavantaje – cost instalatie ridicat, cantitate de gaz necesara mare 30-80% din volum, dimensiuni instalatie mari, greutate mare, presiune de stocare ridicata, utilizabil pe perioade limitate in spatii ocupate.

CO2 – actioneaza prin reducerea cantitatii de oxigen din spatiul de stins si prin efect fizic de racire la destinderea din recipientii sub presiune
Avantaje – cost redus, eficienta ridicata in stingerea unei game largi de incendii, 100% nepoluanta – produs ecologic, non toxic, necoroziv, disponibilitate ridicata.

Dezavantaje – cost instalatie ridicat, cantitate de gaz necesara mare, dimensiuni instalatie mari, greutate mare, presiune de stocare ridicata, nerecomandat in spatii ocupate.

HALON – agent extinguant cu actiune fizica chimica ce actioneaza preponderent asupra energiei din procesul de combustie.

Avantaje – eficient in concentratii mici (6.2%), non toxic, necoroziv, stocare la presiune redusa, instalatie ieftina, utilizabil in spatii ocupate.

Dezavantaje – pret ridicat agent de stingere, AFECTEAZA STRATUL DE OZON motiv pentru care a fost interzis prin Conventia de la Montreal.

INLOCUITORI DE HALONI – agenti extinguanti similari HALONULUI insa fara a dauna stratului de ozon. Performantele lor sunt usor mai scazute fata de cele ale halonului insa pastreaza marea majoritate a caracteristicilor pozitive.

Avantaje – eficienti in concentratii mici 7-10% din volum, non toxici, necorozivi, stocare la presiune redusa, instalatie ieftina, utilizabili in spatii ocupate.

Dezavantaje – pret ridicat agent de stingere, disponibilitate redusa.

NOTA: Pentru a compara numarul de butelii cu gaz necesare pentru a stinge un incendiu intr-un volum dat cu diverse gaze putem utiliza HALONUL ca element de referinta. Astfel daca pentru a asigura stingerea am avea nevoie de 2 butelii cu HALON numarul de butelii necesare cu alte gaze ar fi:

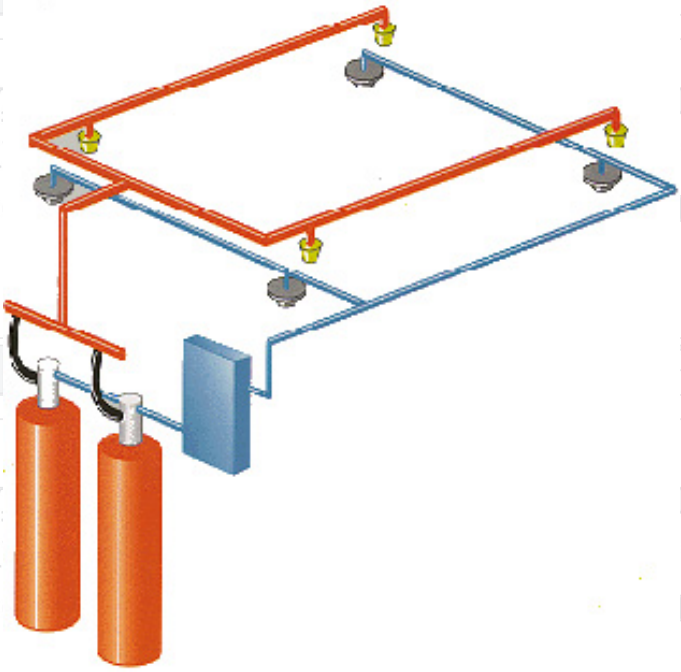
- CO2 – 8 butelii
- GAZE INERTE – 22 butelii
- Inlocuitori de halon – 3 butelii

Mai putin utilizate in instalatiile de stingere fixe pulberile si compusii chimici dedicati (spuma, substante peliculare sau neutralizatori chimici) prezinta interes in cazul in care aplicatiile permit utilizarea acestora fara efecte negative.

Trebuie mentionat faptul ca o instalatie de stingere fara o detectie si o alarmare corespunzatoare nu este eficienta astfel incit sistemul de detectie alarmare si stingere trebuie abordat in mod unitar.

Principial orice instalatie de stingere este compusa din:

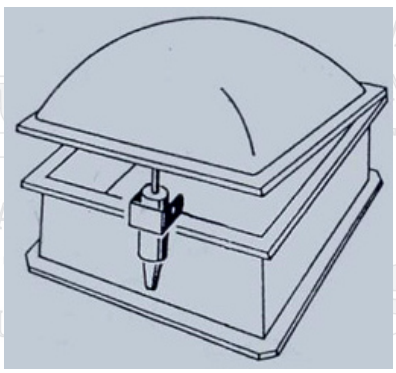
- agent de stingere stocat corespunzator starii sale de agregare
- elemente de transport a agentului din rezervorul de stocare catre elementele de dispersie
- dispozitive de monitorizare a starii instalatiei si a parametrilor functionali
- elemente regulatoare si de control al deversarii
- sisteme electronice de detectie/alarmare si comanda pentru actionarea dispozitivelor deversoare



Special Hazard - Clean Agent Suppression Systems

Actionari si automatizari

In caz de incendiu sunt prevazute unele actionari automate cu rol direct in stingere (cum ar fi instalatiile de stingere sau de limitare a propagarii incendiilor) sau cu rol de protectie a vietii (desfumare, ventilarea cailor de evacuare etc.).



Comenzile pentru acestea se realizeaza in mod direct din releele de comanda ale centralei conventionale sau din dispozitive de comanda (module de iesire) instalate pe bucla analogica. Indiferent de tipul comenzii aceasta este supervizata cu rezistenta EOL garantind integritatea circuitului.

Din punct de vedere fizic conexiunile se fac de preferinta cu cabluri rezistente la foc dimensionate corespunzator din punct de vedere al consumului dispozitivelor actionate. Se va acorda o atentie deosebita actionarilor de trape unde consumul insumat al unui grup de trape devine important.

Inspecția şi întreținerea sistemului (prEN 54-14:1996)

Verificarea lunară

- Utilizatorul va efectua lunar:
  - Proba generatoarelor care asigură cu energie sistemul de detectare şi alarmare la incendiu şi asigurarea unei cantități suficiente de combustibil pentru acestea
  - Declanşarea cel puțin a unui detector automat sau a unui declanşator manual (în fiecare lună din altă zonă) şi verificarea recepționării corecte a informației la centrala de detecție a incendiilor, a declanşării alarmării şi a celorlalte dispozitive de protecție la incendiu
  - Verificarea transmisiei către Pompieri sau către alte dispecerate – dacă este permisă
- Fiecare abatere va fi menționată în registrul de control şi va fi remediată în cel mai scurt timp posibil

Verificarea trimestrială

- La un interval de maxim 3 luni, utilizatorul asigura verificarea sistemului de către o persoană autorizată în următoarele privințe:
  - Înregistrările din registrul de control sunt corecte, iar lucrările necesare au fost executate
  - Conexiunile la acumulatoare sunt în pozițiile corecte
  - Funcționarea corectă a alarmării, semnalizării defectelor şi a acționărilor centralei de detecție a incendiilor
  - Inexistența (control vizual) pătrunderii condensului în interiorul centralei şi nemodificarea situației de mediu
  - Executarea tuturor celorlalte verificări prescrise de instalatorul, producătorul sau distribuitorul echipamentului
  - Păstrarea structurii şi destinației construcțiilor protejate, care ar putea influența utilizarea declanşatoarelor manuale, a detectoarelor automate sau a dispozitivelor de alarmare; în caz contrarse va executa o vizitare a locațiilor în cauză, conform pct. (d) de la "Verificarea anuală".
- Fiecare abatere va fi menționată în registrul de control şi va fi remediată în cel mai scurt timp posibil

Verificarea anuală

- Cel puțin odată pe an, utilizatorul va asigura verificarea sistemului de către o persoană autorizată în următoarele privințe:
  - Executarea corectă a verificărilor zilnice, lunare şi trimestriale
  - Funcționarea corectă a fiecărui detector, conform datelor fabricantului
  - Vizitarea sistemului, în scopul verificării conexiunilor şi echipamentelor în privința fixării, integrității şi a protejării
  - Vizitarea sistemului pentru descoperirea eventualelor locații unde – din cauza modificării structurii sau destinației spațiilor – există influențe asupra poziționării declanşatoarelor manuale, a detectoarelor automate şi/sau a dispozitivelor de alarmare. Această vizitare va avea drept scop şi verificarea păstrării unui spațiu liber de minim 500 mm până la fiecare detector şi păstrarea neobturată şi vizibilă a tutror butoanelor de incendiu
  - Funcționarea corectă a acumulatoarelor sistemului
- Fiecare abatere va fi menționată în registrul de control şi va fi remediată în cel mai scurt timp posibil

Intervale mai mari de timp pentru operațiile de mentenanță

- Anumite componente ale sistemelor dispun de verificarea ciclică automată a unor funcții. Producătorul poate prescrie în acest caz o mărire a intervalelor succesive de verificare manuală a acestor funcții

Documentare

- După încheierea întreținerii anuale a sistemului se va completa un document (care va constitui din acel moment parte integrantă din registrul de control al sistemului) care va fi predat persoanei răspunzătoare din partea utilizatorului.

REGISTRU DE CONTROL
pentru instalațiile de detectare, semnalizare, alarmare, alertare, limitare și stingere a incendiilor

Nr. crt. (fișă) .....

Denumirea instalației

Producător/importator/furnizor

Caracteristici principale (loc amplasare, zone protejate, componente etc.)

Certificat CE/Certificat de conformitate al produsului/Agrement

Documentație tehnică aferentă certificatului

Persoana fizică/juridică ce a executat proiectarea
Certificat atestare

Persoana fizică/juridică ce a executat montarea
Certificat atestare

Persoana fizică/juridică ce execută verificarea, întreținerea, repararea
Certificat atestare
Contract nr. .....
Perioada contractului

Solicitare service deranjamente
Telefon, e-mail, fax

Personal responsabil
Data

Date evenimente

Nr. crt.	Data	Locul	Evenimentul	Cauza	Acțiune corectivă	Numele în clar - Semnătura -

Conform Ordinului nr. 163/2007,
pentru aprobarea Normelor generale de apărare împotriva incendiilor
Anexa 7

1. În registrul de control pentru instalațiile de detectare, semnalizare, alertare, alarmare, limitare şi stingere a incendiilor se consemnează toate datele relevante privind:
a) executarea controalelor stării de funcționare, a operațiunilor de verificare, întreținere şi reparații;
b) executarea de modificări;
c) acționările în situații de incendiu;
d) evenimente produse: alarme de incendiu, alarme false de incendiu, defecte, întreruperi, declanşări intempestive, teste, dezactivări temporare - cu menționarea cauzelor care le-au determinat şi a acțiunilor corective efectuate.

2. Datele consemnate trebuie să indice clar şi precis data (anul, luna, ziua, ora, după caz, minutele şi secundele) şi locul de producere a evenimentului.
3. Toate evenimentele trebuie înregistrate corespunzător.
4. Registrul se completează pentru fiecare instalație din dotare.
5. Se numeşte un responsabil pentru completarea registrului; numele responsabilului este trecut în registru.
6. Se notează componentele înlocuite şi cauzele înlocuirii.

Conform Ordinului nr. 163/2007,
pentru aprobarea Normelor generale de apărare împotriva incendiilor
Anexa 8

EVIDENȚA
exercițiilor de intervenție efectuate la .....

Nr. crt.	Data şi ora executării exercițiului	Tipul exercițiului	Locul/Sectorul de activitate	Cine a organizat exercițiul Numele, semnătura şi funcția	Observații

Un document important in domeniul mentenantei si serviceului sistemelor de detectie si alarmare la incendiu este CEN TS 54-14 INSTRUCTIUNI PENTRU PLANIFICARE, PROIECTARE, INSTALARE, PUNERE IN FUNCTIUNE, UTILIZARE SI INTRETINERE – GHID DE APLICATII.

Acest document aflat in stadiul de dezvoltare si aprobare ofera solutii concrete pentru o gama larga de aplicatii intilnite in practica curenta armonizate la legislatia europeana intr-un mod asemanator celui prezentat de NFPA 72-2002 – Ghid de buna practica, pentru continentul nord american. La ratificarea acestui document instalatorul va fi instruit in realizarea unor proceduri corecte de proiectare, instalare si service pentru sistemele de detectie si alarmare la incendiu

CONCLUZII

In finalul acestui curs voi mentiona ca a fost tratata in special problematica uzuala din domeniul protectiei antiincendiu specifica instalarii, utilizarii si mentenantei. Domeniul este vast iar aprofundarea unui singur capitol necesita un timp indelungat. Scopul acestui curs consta in familiarizarea cu elementele de baza, fundamentind studiile individuale si permitind insusirea unor deprinderi practice corecte. Cunoasterea modului de manifestare si a principiilor ce stau la baza unui anumit fenomen ofera raspunsuri la care in mod uzual se ajungea dupa o indelungata experienta individuala in domeniu.

Legislatie

In cadrul acestui curs au fost abordate in special aspecte teoretice iar exemplele date au caracter consultativ. Pentru aplicatii specifice legislatia in vigoare la momentul elaborarii documentatiilor si/ sau instalarii echipamentelor si instalatiilor poate avea reglementari diferite care vor avea prioritate absoluta fata de specificatiile din prezentul curs.
Unele echipamente sau produse pot diferi constructiv sau ca mod de utilizare – amplasare fata de descrierea principiala din curs caz in care se vor respecta cu strictete prevederile producatorului acestora. Autorul nu isi asuma responsabilitatea pentru utilizarea fara discernamint a datelor sau informatiilor din prezentul material.

Legislație națională

L 307/2006	Lege privind apărarea împotriva incendiilor
O 163/2007	Ordin pentru aprobarea normelor generale de apărare împotriva incendiilor
O 130/2007	Ordin pentru aprobarea metodologiei de elaborare a scenariilor de securitate la incendiu
O 252/2007	Ordin pentru aprobarea metodologiei de atestare a persoanelor care proiectează, execută, verifică întreţin şi/sau repară sisteme şi instalaţii de apărare împotriva incendiilor, efectuează lucrări de termoprotecţie şi ignifugare, de verificare, întreţinere şi reparare a autospecialelor şi/sau a altor mijloace tehnice destinate apărării împotriva incendiilor
L 608/2001 (rep. 2006)	Lege privind evaluarea conformităţii produselor
HG 1490/2004	Hotărâre pentru aprobarea regulamentului de organizare şi funcţionare şi a organigramei Inspectoratului General pentru Situaţii de Urgenţă
HG 259/2005	Hotărâre privind înfiinţarea şi stabilirea atribuţiilor Centrului Naţional pentru Securitate la Incendiu şi Protecţie Civilă

*Lista are un caracter informativ, indicând doar câteva din actele normative de bază care conţin referiri la sistemele de detecţie a incendiilor, actuale la data editării prezentei documentaţii. În practica curentă se vor consulta şi respecta versiunile actualizate şi republicate, precum şi toate celelalte legi, standarde, normative şi reglementări aplicabile.

Bibliografie

SR ISO 8421-x

Partea 1: Termeni generali şi fenomene ale focului
Partea 2: Protecția structurală împotriva incendiului
Partea 3: Detectare şi alarmă la incendiu
Partea 4: Echipamente si mijloace de stingere
Partea 5: Controlul fumului
Partea 6: Evacuare şi mijloace de evacuare
Partea 7: Mijloace de detectare şi de inhibare a exploziilor
Partea 8: Termeni specifici luptei împotriva incendiilor, serviciilor de salvare şi manipulării produselor periculoase

EN/TR 14568:2003

EN 54 - Fire detection and fire alarm systems - Interpretation of specific clauses of EN 54-2:1997

Normativ I18/1 – 01

Proiectarea şi executarea instalațiilor electrice interioare de curenți slabi aferente clădirilor civile şi de producție

Normativ I18/2 – 02

Proiectarea şi executarea instalațiilor de semnalizare a incendiilor şi a sistemelor de alarmare contra efracției din clădiri

P118-99

Normativ de siguranță la foc a construcțiilor

NT 030-01

Ghid pentru evaluarea riscului de incendiu şi a siguranței la foc la săli aglomerate

NT 049-02

Ghid pentru evaluarea riscului de incendiu şi a siguranței la foc pentru clădiri de spitale

NT 050-02

Ghid pentru evaluarea riscului de incendiu şi a siguranței la foc la căminele de bătrâni şi persoane cu handicap

NP 063-01

Ghid pentru proiectarea, executarea şi exploatarea dispozitivelor şi sistemelor de evacuare a fumului şi a gazelor fierbinți din construcții în caz de incendiu

EN VDE 0815

Conexiuni şi cabluri pentru echipamente de detecție şi semnalizare

EN VDE 0823 p1 & 2

Echipamente de semnalizare a pericolului de incendiu, efracție şi atac

EN 14675

Echipamente de semnalizare a incendiilor; construcție şi utilizare

EN 14034

Simboluri grafice pentru instalații de semnalizare a incendiilor

Alte normative conexe

(US) NFPA 72 -National Fire Alarm Code

NFPA12 - Standard on Carbon Dioxide Extinguishing Systems
NFPA12 A - Standard on Halon 1301 Fire Extinguishing Systems

NFPA 13 - Standard for the Installation of Sprinkler Systems

BS 5446 Part 1: 1990 -Specification of Self-Contained Smoke Alarms and Point-Type Smoke Detectors

BS 5839 Part 1: 1988 -Code of Practice for System Design, Installation and Servicing

BS 5839 Part 2: 1983-Specification for Manual Call Points

BS 5839 Part 3: 1988-Specification for Automatic Release Mechanisms for Certain Fire Protection Equipment

BS 5839 Part 4: 1988-Specification for Control and Indicating Equipment

BS 5839 Part 5: 1988-Specification for Optical Beam Smoke Detectors

BS 5306 Part 4: 2001
Requirements for Carbon Dioxide Systems

BS 5306 Part 5.1: 1992
Specification for Halon 1301 Total Flooding Systems

BS 5306 Part 5.2: 1984
Halon 1211 Total Flooding Systems

BS 6535 Part 1: 1990
Fire Extinguishing Media - Part 1: Specification for Carbon Dioxide

BS 6535 Part 2.1: 1990
Fire Extinguishing Media - Part 1: Specification for Halon 1211 and 1301

EN 12094 Part 1:
Fixed Firefighting Systems: Components for Gas Extinguishing Systems - Part 1: Requirements and test methods for electrical automatic control and delay devices

BS ISO 14520-9: 2000
Gaseous fire-extinguishing systems – Physical properties and system design Part 9: HFC 227ea extinguishant

BS ISO 14520-12: 2000
Gaseous fire-extinguishing systems – Physical properties and system design Part 12: IG-01 extinguishant

BS ISO 14520-13: 2000
Gaseous fire-extinguishing systems – Physical properties and system design Part 13: IG-100 extinguishant

BS 5306 Part 2: 1990
Specification for Sprinkler Systems

EN 12259 Part 1: 1999
Fixed Firefighting Systems: Components for Sprinkler and Waterspray Systems:Part 1: Sprinklers

EN 1568 Part 1: 2001
Fire extinguishing media. Foam concentrates. Specification for medium expansion foam concentrates for surface application to water-immiscible liquids

EN 12416 Part 2: 2001
Fixed firefighting systems. Powder systems. Design, construction and maintenance

BS 5588-8:1999, *Fire precautions in the design, construction and use of buildings — Part 8: Code of practice for means of escape for disabled people.*

BS 5839-8, *Fire detection and alarm systems for buildings — Part 8: Code of practice for the design, installation and servicing of voice alarm systems.*

BS 7807, *Code of practice for design, installation and servicing of integrated systems incorporating fire detection and alarm systems and/or other security systems for buildings other than dwellings.*

Lista standardelor si normelor utilizate nu este limitativa aplicatii specifice impunind utilizarea normelor sau standardelor specifice aplicatiei in cauza. Intodeauna se va verifica revizia si se va utiliza ultima versiune disponibila.

Întocmit:
Ing.Cristian Şoricuț/Ing.Carol Șamu

Capitolul 1

PREZENTARE GENERALA

Sistemele de supraveghere video au devenit, cu timpul, o componente cheie pentru asigurarea sigurantei si securitatii pentru foarte multe organizatii. Odata cu cresterea riscului de securitate, nevoia de monitorizare video si de inregistrare a evenimentelor a devenit din ce in ce mai importanta. Ca rezultat multe organizatii implementeaza astfel de sisteme pentu o gama larga de aplicatii si nu doar in domeniul strict al sistemelor de securitate. Trebuie spus de la inceput ca aceste sisteme vin sa completeze sistemele « traditionale« de securitate si siguranta – detectie efractie, control acces, detectie incendiu- sistemele de supraveghere functionand in relatie de colaborare cu acestea, asigurand elementul de monitorizare in timp real si posibilitatea de vizualizare post-eveniment precum si inregistrare, afisarea si transmisia informatiei video catre diversi beneficiari ai acesteia. Datorita progreselor tehnologice inregistrate de a lungul timpului in industria electronicii si, in principal, in domeniul tehnologiei informatiei industria TVCI si-a schimbat foarte multe din principiile de baza, trecand de la sistemul complet analogic la cel complet digital, centrat pe transmisia de date in retea.

Capitolul 2

ECHIPAMENTE TVCI.
STRUCTURA SI FUNCTIONAREA COMPONENTELOR SISTEMELOR TVCI

2.1 CONSIDERATII GENERALE

Un sistem de supraveghere video cu circuit inchis este format din camere video, medii de transmisie, echipamente de inregistrare si coumtare, afisare si prelucrare a imaginilor achizitionate de la camerele video. Aceste imagini sunt folosite doar in scopul asigurarii functiilor specifice.
Procesele principale ce au loc intr-un sistem de supraveghere video pot fi descrise ca fiind :

- procesul de achizitie a imaginii si de producere a semnalului video
- transmisia semnalului video, folosind diverse medii de transmisie
- procesul de inregistrare, conversie, distributie a semnalului video.
- procesul de afisare

Intr-un sistem de supraveghere video se pot distinge, conform cu procesele mentionate anterior urmatoarele elemente componente:

- echipamente de achizitie a imaginii – obiectiv-ul (lentila) si camera video
- mediul de transmisie a semnalului video : cablul coaxial, perechea torsadata, fibra optica, wireless
- echipamente de achizitie si prelucrare. Aici gama de echipamente este extrem de larga si diversa : digital video recordere-DVR, matrici video, multiplexoare, distribuitoare, amplificatoare, Network video recordere, unitati de arhivare etc.
- echipamente de afisare a semnalelor video : monitoare CRT, LCD, software de gestiune

Folosirea luminii este, practic, un element cheie in implementarea unui sistem video. Acest lucru, pe langa altele, influentand in mod direct calitatea imagini afiasate si/sau inregistrate. Lumina este o forma de energie formata din sapte componente de baza. Aceste componente formeaza un spectru, din care ochiul uman poate percepe doar o portiune cuprinsa intre aprox. 400nm si 700 nm. Aceata lumina este folosita pentru « sensibilizarea« elementelor fotosensibile (senzorul de imagine) Pe langa radiatia vizibila o alta forma de radiatie este folosita de camerele de tip zi/noapte pentru preluarea imaginilor in conditii slabe de iluminat. Radiatia infrared se situeaza in afara spectrului vizibil. Acest tip de radiatie este emisa de catre toate obiectele, oameni, animale etc. Obiectele « calde » apar evidentiate pe un fundal « rece« in conditii slabe de iluminat, de exemplu noaptea.

2.2 CAMERA VIDEO

Principiul de baza de functionare al unei camere video consta in transformarea luminii reflectate de catre « scena » supravegheata in semnal electric. La baza acestui proces sta senzorul de imagine. Senzorul de imagine este un circuit integrat specializat care are rolul de a transforma « informatia« luminoasa in semnal electric. Acest semnal electric este apoi prelucrat de circuitele de procesare digitala a semnalului (DSP-Digital Signal Processor). Semnalul video rezultat la iesirea camerei este asa numitul semnal video compozit. Pana de curand circuitele de procesare a semnalelor erau circuite analogice dar, odata cu dezvoltarea circuitelor specializate de procesare a semnalelor, majoritatea camerelor de astazi folosesc « chip set«-uri specializate – Digital Signal Procesor - care ofera facilitati si optiuni ce permit o mai usoara instalare, reglare si cu rezultatul final –calitatea imaginii- mult mai buna decat precedenta serie de camere analogice. Senzorul de imagine este format dintr-o « matrice « de elemente fotosensibile numite elemente de imagine sau pixeli. Pixel-ul este elementul de baza al imaginii, care transforma lumina cazuta pe el in semnal electric, intensitatea acestui semnal este direct proportionala cu cantitatea de lumina care cade pe elementul de imagine. CCD-ul este scanat de la stanga la dreapta de 312,5 de 50 de ori pe secunda. Intensitatea luminii ce cade pe CCD este « translatata« intr-o mixtura de culori : rosu, verde si albastru din care se obtin valorile de luminanta (Y) si diferenta de culoare (U, V) ce compun semnalul video complex. In specificatiile camerelor numarul de pixeli ai unui CCD este specificat ca numar de pixeli orizontalaXnumar de pixeli pe verticala (De exemplu :752HX582V).

Senzorul de imagine tip CCD (Charged Coupled Device) :Tehnologia senzorilor tip CCD este una dezvoltata special pentru industria camerelor video. Principalul avantaj, comparativ cu tehnologia CMOS, consta in sensibilitatea ridicata in conditii de iluminare scazuta ceea ce inseamna imagini de calitate mai buna pentru conditii de iluminat scazut. Tehnologia CCD presupune un proces mai complex de producere si incorporare in camerele video.

Senzorul de imagine tip CMOS (Complementary Metal Oxide Semiconductor) :Tehnologia CMOS este una larg raspandita pentru componentele electronice. Senzorii tip CMOS pot fi produsi in dimensiuni variabile, de la camere miniaturale pana la camere tip megapixel. In ultimul timp distanta intre cele doua tipuri de tehnologii s-a redus, astfel incat calitatea imagini se apropie de cea a celor CCD, totusi – atunci cand cea mai buna calitate este dorita- tehnologia tip CCD este recomandata. Principalul dezavantaj al acestui tip de senzor de imagine este sensibilitatea scazuta pentru conditii de iluminat scazut. In conditii de iluminat constant acest lucru nu este o problema dar in conditii de iluminat scazut imaginea rezultata este intunecata sau de calitate slaba (perturbata de « zgomot«).

Formate de CCD

Standardul de imagine folosit in industria CCTV este 4:3 (H :V). Cele mai des intalnite formate pentru senzorii de imagine CCTV sunt urmatoarele : 1”, 2/3”, 1/2”, 1/3”, 1/4”. Cu cat dimensiunea CCD-ului este mai mare cu atat imaginea rezultata va avea o calitate mai buna. Totusi, din motive economice, cele mai des folosite sunt cele de 1/3” si 1/4”.

Semnalul video complex (composit)

Semnalul video composit este semnalul obtinut din camera video folosind circuite de procesare a semnalului (DSP-Digital Siganal Processor). Se numeste semnal video composit (sau complex) deoarece este compus din informatia video, un puls de sincronizare si un semnal de referinta. Amplitudinea maxima a acestui semnal este de 1 V varf–la-varf (1V peak-to-peak).

Pentru standardul PAL o imagine este formata din 625 linii scanate la o frecventa de 50Hz. Exista doua moduri de afisare a informatiei video :

Modul intretesut (2 :1 Interlaced): In acest mod o imagine completa (frame) este formata din doua treceri (scanari), fiecare trecere (scanare) formand un field. Prima trecere este pentru field-urile impare (313 linii) si urmatoarea trecere pentru field-urile pare (312). Acest mod se mai numeste si

2:1 Interlaced (2 field-uri : 1 frame).

Modul progressiv scan (1 :1 Non-interlaced): este modul de formare al imaginii prin scanarea progresiva de la linia 1 la linia 625 cu o frecventa de 25 frame-uri/secunda
Interlaced scan este mostenit de la sistemele TV si este inca larg folosit astazi.. Progressive scan este folosit de noile monitoare tip LCD, TFT pentru a afisa imaginea in ordinea aparitiei liniilor. Pentru afisarea unui semnal Intrelaced aceste echipamente au nevoie de un circuit de de-interlaced, pentru a afisa imaginile in modul progresiv.

Caracteristici generale ale camerelor video

Rezolutia: Rezolutia este o masura foarte importanta a calitatii imaginii pe care acea camera o poate reda. Rezolutia unei camere reflecta capacitatea acelei camere de a reda detaliile unei scenei. Aceasta marime se exprima uzual in termeni de linii TV orizontale. In specificatiile unei camere valoarea rezolutiei se bazeaza pe numarul de elemente distincte, dintr-o linie orizontala, care pot fi capturate de catre camera. Acest lucru se reflecta in mod direct asupra numarul de linii verticale care pot fi distinse, pentru echivalentul de proportie 4/3 (H/V). Numarul de linii verticale, adica numarul elementelor distincte dintr-o linie orizontala, se obtine din rezolutia orizontala inmultita cu valoarea 4/3. Acest lucru se face pentru a pastra proportiiile naturale ale imaginii. Cu cat numarul de elemente individuale dintr-o linie orizontala este mai mare, cu atat in imaginea rezultata vom putea distinge mai multe detalii. De exemplu o camera cu rezolutia de 520 linii TV va avea intr-o singura linie 520 x (4/3) elemente distincte de imagine.
O clasificare tipica a camerelor color este, din punctul de vedere al rezolutiei, urmatoarea :
- rezolutie normala: in jur de 330-380 linii TV
- rezolutie medie: mai mica de 480 linii TV
- inalta rezolutie: peste 520 linii TV

Pentru camerele monocrome se foloseste aceeasi clasificare dar rezolutia este, in medie, cu 80 de linii TV mai mare. O masurare a rezolutiei camerei se poate face folosind chart-ul de test EIA. Acest parametru, rezolutie, este extrem de important in alegerea unei camere care sa corespunda cu cerintele de vizualizare, identificare si recunoastere a detaliilor necesare aplicatiei. De mentionat ca rezolutia intregului sistem este data de cea mai mica rezolutie a elementelor componente (camera video, monitor, DVR).

Sensibilitatea: sensibilitatea unei camere este o masura a performantei camerei in conditii slabe de iluminat, se mai intalneste un specificatii ca fiind iluminarea minima. Acest parametru este influentat de mai multi factori, printre acestia se includ, apertura (deschiderea) irisului, calitatea obectivului, dimensiunea si calitatea CCD-ului, amplificarea camerei, timpul de expunere, modalitate de procesare a semnalului video.
Sensibilitatea mai poate fi descrisa ca fiind iluminarea minima necesara, la o deschidere data a lentilei, pentru ca sa avem la iesirea camerei un semnal video util.
Masura acestei valori este exprimata ca fiind « canitatea » de lumina necesara in anumite conditii, raportata la apertura irisului (pentru o distanta focala fixa). De exemplu : 0.1 lux@f1.2 Aceasta valoare exprima cantitatea minima de lumina necesara pentru a reda un semnal util. In capitolul dedicat obiectivului va fi explicata semnificatia marimii f-stop.

Raportul Semnal Zgomot (Signal Noise Raport - SNR) : Este un parametru care descrie, din punct de vedere dinamic, comportamentul camerei si capacitatea ei de a compensa influenta perturbatoare a « zgomotului«, a semnalului parazit, care se suprapune peste semnalul util. Nicio camera nu poate rejecta acest « zgomot«, influenta acestuia putand fi doar redusa. Masura acestui parametru este data in decibeli (dB). O camera cu un raport semnal zgomt cat mai mare are o capacitate mai mare de a reduce « zgomotul« si de a furniza imaginii de calitate mai buna, decat o camera cu SNR mai mic.

Compensarea Luminii din Spate (Back Light Compensation - BLC): Aceasta functie are un rol major in situatiile in care obiectul supravegherii se afla pe un fundal luminos, ori cand cea mai mare parte a luminii vine din spatele obiectului. Sistemul de expunere al camerei se seteaza automat pentru o medie a cantitatii de lumina din scena. Daca in scena apare o cantitate mai mare de lumina, atunci sistemul de expunere reactioneaza la aceasta prin ajustarea (inchiderea) irisului (sau a irisului electronic) acest lucru avand ca efect o imagine mai intunecata. Pentru a compensa acest efect, prin activarea BLC-ului, camera va calcula timpul de expunere bazandu-se pe nivelul de iluminare doar dintr-o parte a imaginii, uzual in centrul imaginii, care este de interes pentru vizualizare. Orice modificare a iluminatului in afara acestei ferestre este ignorata de catre sistemul de expunere.

Automatic Gain Control : Circuitul care realizeaza aceasta functie are rolul de a compensa fluctuatiile de iluminat care duc la scaderea semnalului video. Daca valoarea semnalului este adecvata circuitul nu va aplica nicio amplificare, totusi daca semnalul video continua sa scada (pe masura scaderii iluminatului) atunci circuitul va aplica din ce in ce mai multa amplificare pana ce semnalul video atinge valoarea de 1V p-p. Trebuie mentionat ca acest circuit nu poate face minuni si in scena trebuie sa exista lumina pentru a se putea produce un semnal video. Trebuie mentionat ca amplificarea unui semnal slab presupune si amplificarea zgomotului din acel semnal, de aceea semnalul video preluat in conditii slabe de iluminat si amplificat va produce o imagine de proasta calitate, dar acest lucru este de preferat in schimbul lipsei totale de imagine. Este recomandat ca aceasta functie sa fie activata, daca exista lumina suficienta in scena AGC nu functioneaza. Cand se regleaza o camera trebuie setat AGC OFF astfel incat semnalul obtinut sa nu fie influentat de amplificarea camerei, dupa reglaj se seteaza AGC ON.

Electronic Iris : In contrast cu functia AGC aceasta functie compenseaza valorile crescute ale semnalului video prin controlul timpului de expunere in concordanta cu nivelul de iluminat. Shutter-ul este circuitul care controleaza timpul de expunere a senzorului de imagine la fluxul luminos care este focalizat de lentila. Cu cat acest timp este mai mic cu atat timpul necesar senzorului pentru a « acumula » lumina este mai mic si, in acest fel, se evita supra expunerea la lumina. Circuitul de Electronic Iris asigura ca semnalul video de iesire sa fie la valaoarea de 1 Vp-p. Irisul electronic are limitele sale, daca prea multa lumin cade pe senzorul de imagine poate rezulta fenomenul de « smearing« .

Shutter Speed : Shutter-ul are rolul de a controla timpul de expunere a senzorului la lumina. Un shutter cu viteza mare (adica cu timp redus de expunere) este recomandat pentru redarea imaginilor in care avem obiecte in miscare rapida. Totusi un shutter rapid inseamna un timp de expunere mic, adica mai putina lumina ajunge pe senzorul CCD si are ca rezultat o imagine mai intunecata. Daca este necesar un shutter rapid atunci trebuie sa ne asiguram ca avem suficienta lumina. Valoarea shutter-ului poate fi setata manual sau poate fi lasata pe regimul automat..

OSD - On Screen Display : Este o functie intalnita la camerele digitale. Datorita complexitatii si numarului mare de functii prezente la o astfel de camera trebuia sa existe o metoda de a putea seta acesti parametrii, metoda gasita presupune actionarea unor butoane de pe camera si intrarea in meniurile de configurare care apar suprapuse pe semnalul de iesire din camera atunci cand camera este conectata la un monitor.

Detectie de miscare : Este o functie ce permite detectarea miscarii in campul vizual al camerei prin analiza de imagine la nivelul camerei video.

*Zone de mascare :*Aceasta functie permite eliminarea unor zone din campul vizual al camerei, zone care nu trebuie sa apara in imaginea rezultata de la aceea camera, permitand protejarea anumitor obiecte.

2.3 OBIECTIVUL (LENTILA)

Alegerea obiectivului este una din alegerile care influenteaza in mod direct performanta unui sistem de televiziune cu circuit inchis. Acesta alegere depinde de mai multi factori, ca de exemplu: pozitia fizica a camerei, nivelul de iluminare existent, cerinte privind tipul de imagine dorit, ce anume se doreste a se monitoriza, identifica etc.

Lentila (obiectivul) este un element optic-electronic-mecanic ce realizeaza functia de preluare si focalizare a luminii pe senzorul de imagine. Punctul de pe axa lentilei unde se focalizeaza (converg) razele luminoase se numeste punct focal. Distanta de la acest punct la planul de formare a imaginii se numeste distanta focala. Distanta focala determina « campul de vizualizare » - field of view – sau unghiul de vizualizare, la o distanta data, adica ceea ce "vede" acea camera. Cu cat distanta focala este mai mare cu atat campul de vizualizare devine mai ingust. O distanta focala mica inseamna ca acea lentila « vede« o arie mai mare (larga) atat in plan orizontal cat si in plan vertical, din acest motiv obiectele din campul vizual apar departate si de dimensiuni mici.

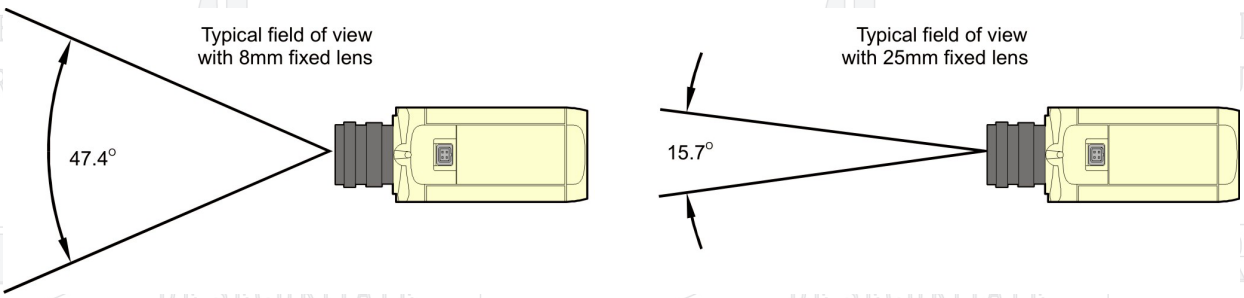


Figura 2.11 Campul de vizualizare si distanta focala

In figura de mai jos este reprezentata schematic relatia dintre distanta focala si dimensiunea in plan orizontal a scenei/ariei supravegheate.

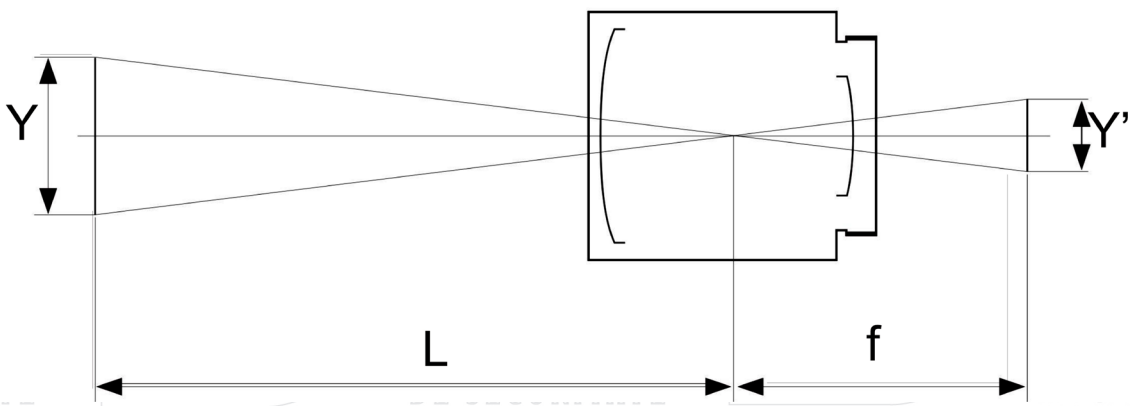


Figura 2.12 Relatia dintre distanta focala si campul de vizualizare

$Y = Y' \times L/f$

Daca stim ce dimensiuni are obiectul pe care vrem sa-l supraveghem putem deduce distanta focala necesara pentru lentila. In mod obisnuit producatorii de lentile asigura instrumente de calcul pentru distanta focala, astfel incat sa putem alege de la inceput tipul de lentila necesara unei aplicatii. Pentru a identifica corect detaliile unui obiect trebuie ca acesta sa ocupe cel putin 50% din imagine.

Din punctul de vedere al distantei focale obiectivele se impart in :

- obiective cu distanta focala fixa
- obiective cu distanta focala variabila – varifocale
- obiective cu zoom motorizat

Obiectivele cu distanta focal fixa sunt folosite din considerente de economie dar, avand distanta focala fixa, atunci si campul de vizualizare este fix, acest lucru presupune ca trebuie luate in calcul inca de la inceput distantele de montaj precum si marimea obiectelor supravegheate pentru a putea alege lentila cu distanta focala corecta. Orice schimbare a cerintelor aplicatiei presupune, de cele mai multe ori schimbarea lentilei ori a locului de amplasare a camerei.

Obiectivele varifocale sunt mai scumpe dar au avantajul de a putea fi folosite intr-o gama extrem de larga de aplicatii, mai ales atunci cand nu stim de la inceput care sunt cerintele aplicatiei, in termeni de camp de vizualizare, cerinte de identificare etc. Acest tip de lentila permite reglarea distantei focale intr-o gama fixa, relativ mica (de ex : 3.5 – 8 mm, 5 – 50 mm etc). Fixarea distantei focale se face la instalarea camerei, in mod manual, folosind controlul Wide/Tele aflat pe lentila.

Obiectivele cu zoom motorizat sunt un pas inainte in ceea ce priveste obiectivele varifocale, oferind cea mai mare functionalitate. Aceste obiective sunt comandate de la distanta prin modificarea distantei focale si, implicit, a campului de vizualizare, realizandu-se focalizarea automata (autofocus) sau manuala. Astfel se permite operatorului sa examineze amanuntit anumite detalii ale scenei. Prin modificarea distantei focale se modifica si adancimea campului de focalizare. Uzual aceste lentile se folosesc pentru camerele de tip Pan&Tilt&Zoom, acele camere atasate la un dispozitiv electromecanic ce permite deplasarea in plan vertical si in plan orizonatal a camerei, comenzile pentru zoom fiind trimise direct obiectivului.

Pentru a descrie calitatile acestui tip de obiectiv se foloseste raportul dintre distanta focala maxima si cea minima (Zoom Ratio – raportul de zoom sau zoom optic). De exemplu pentru un obiectiv avand distanta focala intre 10 mm si 100 mm acest raport este de 10X, iar pentru un obiectiv care are distanta focala intre 18 mm si 144 mm raportul de zoom este de 8X. De observat ca un zoom optic mare nu inseamna o distanta focala mare, in exemplul de mai sus o camera cu obiectivul avand zoom optic 8X poate sa « vada » mult mai departe decat cea cu zoom optic de 10X.

Formatul obiectivului. Ca si pentru senzorul CCD obiectivele au formatele de : 1”,2/3”,1/2”,1/3”,1/4”, aceste fiind rezultate din diametrul lentilei, raportat la dimensiunile imginii produse. Practica uzuala este de a folosi acelasi format atat pentru lentila cat si pentru senzorul de imagine al camerei, dar este posibil sa se foloseasca si obiective cu format mai mare pe camere cu senzor de imagine mai mic decat al lentilei (de exmplu se poate folosii o lentila de ½” pe un senzor de 1/3”). Ca principiu, se alege o lentila care poate furniza o imagine mai mare decat cea a senzorului camerei.

Daca se alege o lentila cu un format mai mic decat al senzorului atunci imaginea rezultata va avea colturile negre, daca se va alege o lentila cu un format mai mare atunci nu toata energia luminoasa ajunge pe senzor, iar o parte din unghiul de vizualizare (o parte din campul de vizualizare) se va pierde. Formatele mari de lentila ofera cateva avantaje comparativ cu cele mici : o mai mare adancime a campului de focalizare si imagini cu mai putine efecte de distorsionare la margini.

Irisul (Diafragma)

Cantitatea de lumina care cade pe senzorul de imagine trebuie sa fie intre anumite limite pentru o performanta optima a camerei. Prea multa lumina duce la fenomenul de supraexpunere sau albire, prea putina lumina inseamna o imagine mai intunecata si pierderea detaliilor in zonele aflate in umbra. Irisul (sau diafragma) are rolul de a controla cantitatea de lumina ce ajunge pe senzorul de imagine. Irisul consta dintr-un numar de pale metalice aranjate astfel incat produc o deschidere circulara in centrul lor. Deschiderea (apertura irisului) se poate mari sau micsora in incremente numite f-stops.

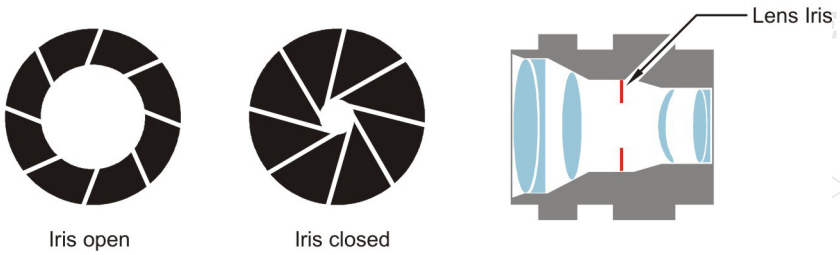


Figura 2.19 Irisul

Un alt rol al irisului, in afara controlului lumini ce ajunge pe senzor, este acela de a controla adancimea campului de focalizare. Practic irisul este cel mai bine definit de F-stop (Numarul F sau F.No).
Acest parametru este o masura a « luminozitatii« obiectivului. Valoarea acestui numar se calculeaza cu formula F.No= f/D (f-distanta focala a lentilei si D-diametrul irisului)
Cu cat F.No este mai mare cu atat mai putina lumina ajunge pe senzorul CCD. O valoare mica a numarului F.No inseamna mai multa lumina care ajunge pe CCD.
Acest parametru este luat in calcul la masurarea sensibilitatii camerei (de exemplu **0.1lux@F1.2).**
In tabelul de mai jos sunt date cateva valori privind procentul de lumina ce ajunge pe CCD pentru diverse valori ale numarului F.

F. No	F1.0	F1.2	F1.4	F1.7	F2.8	F4.0	F5.6
% lumina ajunsa pe CCD	20	14.14	10	7.07	2.5	1.25	0.625

Din punctul de vedere al irisului incorporat obiectivele pot fi :
- obiectiv cu iris fix
- obiectiv cu iris manual
- obiective cu iris automat (autoiris)

Obiectivul cu iris fix este un tip de iris care nu poate sa se adapteze la conditiile variabile de iluminat, deschiderea acestuia ramanand constanta. Obiectivul cu acest tip de iris este recomandat doar pentru conditii de interior unde nivelul de iluminat ramane constant. Parte din functiile irisului sunt realizate de camera prin folosirea functiilor Electronic Iris si Automatic Gain Control.

Obiectivul cu iris manual permite reglarea deschiderii irisului la momentul instalarii, astfel incat sa corespunda conditiilor de iluminat existente, totusi, la fel ca si la obiectivele cu irisul fix, conditiile de iluminat trebuie sa fie relativ constante pentru a avea o imagine buna. Pentru astfel de obiective se recomanda gasirea unei valori “medii” care sa corespunda cat mai multor variatii ale luminii.

Obiectivul cu autoiris este, practic, cel mai folosit si cel mai util pentru marea varietate de aplicatii in care conditiile de iluminat nu sunt constante, in special pentru aplicatiile de exterior unde conditiile de iluminat se schimba continuu. Acest tip de obiectiv, cu autoiris, este controlat in mod automat si constant de catre camera pentru obtinerea unui nivel de iluminare optim pe senzorul de imagine. Controlul iris-ului se poate face prin mai multe metode. Astfel, obiectivele cu iris automat se pot clasifica in mai multe tipuri.

*Video Drive Iris*Acest tip de obiectiv contine toata partea electronica de analiza a semnalului video obtinut de la camera. Un semnal video de referinta se preia de la camera iar lentila incearca sa mentina acesta valoarea de tensiune la 1V p-p prin inchiderea sau deschiderea diafragmei. De exemplu daca nivelul de iluminare incepe sa scada atunci si valoarea semnalului video va scadea, in acel moment circuitul de analiza a semnalului va da o comanda catre servo-motorul inglobat de deschidere a diafragmei, pana cand se atinge din nou valoarea optima de 1V p-p a semnalului de referinta.

Direct Drive Iris Pe masura ce circuitele de analiza a semnalelor TV si de comanda au fost incorporate pe scara din ce in ce mai larga direct in camerele de supraveghere video, au aparut din ce in ce mai mult obiective mai mici si mai ieftine – numite Direct Drive. Aceste obiective controleaza diferit iris-ul printr-un procedeu numit – galvanic drive. Obiectivele Direct Drive nu contin circuite de analiza a semnalului ele fiind comandate direct de catre camera video prin doua semnale : drive signal si damping signal. Drive signal este semnalul de control al lentilei iar damping signal este folosit pentru prevenirea situatiilor cand lentila reactioneaza prea repede la schimbarile de iluminat din campul vizual. Acest semnale sunt furnizate de catre camerele video care accepta acest tip de lentile.

Adancimea campului de Focalizare Este momentul sa vorbim acum despre un parametru important al lentilelor si anume adancimea campului de focalizare. Uzual o lentila se focalizeaza, la o anumita distanta, pe un obiect. Acel obiect va aparea in imagine foarte clar, totusi, pe o anumita distanta in fata si in spatele lui si celelalte obiecte vor aparea foarte clar. Suma acestor doua distante, din fata si din spatele obiectului, se numeste adancimea planului de focalizare. Impreuna formeaza asa numitul « camp de focalizare ». Obiectele care nu sunt in acest »camp de focalizare », pe toata adancimea lui, vor pierde din claritate. Adancimea campului de focalizare depinde de numarul F.No (« luminozitatea » lentilei, care depinde invers proportional de deschiderea irisului). Asadar, adancimea campului de focalizare depinde de deschidera irisului. Pe masura ce irisul se inchide adancimea campului de focalizare va creste, ceea ce inseamna ca mai multe obiecte vor intra in campul de focalizare.- adică vor aparea mai clar in imagine. Un dezavantaj al cresterii acestei adancimi prin inchiderea irisului este ca pe senzorul de imagine va ajunge mai putina lumina, iar imaginea va fi mai intunecata. Adancimea campului de focalizare este dependenta de distanta defocalizare, obiectivele « wide angle«, cele care au unghiul de vizualizare mare - adica distanta focala mica- vor avea o adancime mai mare decat cele de tip « telephoto« - adica cele cu o distanta focala mica. Obiectivele autoiris, prin natura lor putand sa-si modifice deschiderea irisului, vor face ca si adancimea campului de focalizare sa se modifice.

2.4 TIPURI DE CAMERE

Asa cum am aratat mai sus tipologia camerelor este foarte diversa, o clasificare a acestora se poate face din punctul de vedere al mobilitatii lor in : camere fixe si camere mobile.
Camerele fixe au diverse forme constructive si dimensiuni care merg de la cele tip «pin hole« , camere de tip mini-dome, camere cu obiectiv incorporat in carcasa camerei, camere la care se adauga, separat, obiectivul etc. Pentru camerele fixe exista posibilitatea de a avea montat un obiectiv cu zoom motorizat astfel incat sa existe controlul asupra unghiului de vizualizare. Uzual acest tip de camere se folosesc atasate intr-un echipament de tip Pan&Tilt& Zoom (PTZ).
O categorie de camere mobile cu functii deosebite o constiuie asa numitele camere de tip « dome » sau « speed dome«. Aceste camere sunt folosite intr-o laraga gama de aplicatii in care exista cerinte de supraveghere deosebite :

- arii mari de supravegheat
- este necesara urmarirea unor obiecte/persoane aflate in miscare
- se cere preluarea unor imagini din momentul producerii unor evenimente
- se cere interconectarea cu alte sisteme (control acces, efractie, building managemet, detectie incendiu)
- usurarea muncii de supraveghere video a operatorilor
- costuri reduse, pentru supravegherea unor suprafete mari, unde ar fi necesar un numar mai mare de camere fixe

O camera de tip speed-dome este compusa dintr-o camera video, in general de mare rezolutie, cu obiectiv auto-iris, cu zoom motorizat si autofocus, actionata de un set servo-motoare, comandate de un echipament de control. Toate aceste componente se afla intr-o carcasa comuna avand, in partea inferioara, un capac de sticla de forma unui dome (semisfera). Modalitatile de montaj sunt multiple : tavan, perete, stalp, coltul unei cladiri, in atarnare de diversi suporti etc.

Aceste camere au cateva caracteristici deosebite dintre care enumeram :

- zoom optic mare (30X, 36X)
- lentila autofocala
- rotatie in plan orizontal de 360 grade
- rotatie in plan vertical de aprox. 180 grade
- numar mare de prepozitii (presets) care pot fi memorate
- posibilitatea de executie a tururilor
- intrari de alarma (care pot declansa tur-uri sau "sarirea" la prepozitii)
- iesiri de alarma pentru activarea unor echipamente auxiliare
- zone de mascare
- protocoale de comunicatie multiple

In plus, exista astfel de camere care au si functia de auto-tracking, sau urmarirea unei tinte. Aceasta functie este utila pentru spatii care, in general, nu au obiecte in miscare si cand se doreste urmarirea oricarei miscari in acel loc.

Camerele de tip speed-dome pot functiona total autonom, independent de operatorii sistemului de supraveghere. Camerele pot fi programate sa execute automat tururi sau pot fi interfatate cu alte sisteme de la care sa primeasca comenzi. De exmplu o astfel de camera de tip speed-dome folosita intr-un sistem de paza perimetrala poate primi, in caz de alarma pe un anumit segment, comanda de comutare la o anumita prepozitie care este memorata in camera, acea prepozitie fiind alocata segmentului respectiv.

Comanda camerelor mobile speed dome se face de la un echipament care poate fi : DVR, matrice video, PC cu un software adecvat, tastaturi dedicate, sau alt tip de controller.

In general comunicatia acestor speed –dome-uri are la baza un protocol serial de distanta mare (RS-485, RS-422). Aceste protocoale, de nivel fizic (care definesc din punct de vedere electric interfetele de comunicatie), sunt protocoale diferentiale de distanta mare (1200m) ce folosesc perechea torsadata ca mediu de transmisie. Pe langa acest mediu de transmisie, in ultimul timp un alt mediu si-a facut aparitia, este vorba de fibra optica. Sunt camere speed-dome care vin gata echipate cu interfata de fibra optica astfel incat pe acelasi mediu –fibra optica- se transmit atat semnalul video cat si semnalul de comanda (date). Evident, in dispecerat exista echipamentul de conversie a semnalului luminos folosit pentru transmisia in fibra optica in semnalul video composit necesar echipamentelor de comutare/ inregistrare afisare.

De mentionat ca peste protocolul serial de nivel fizic fiecare camera foloseste un protocol de nivel inalt, specific producatorului respectiv sau folosind standard-ul de facto protocolul PELCO-D. Pe piata exista o multitudine de camere de tip speed-dome care pot folosi mai mult de un protocol, uzual cel proprietar si PELCO-D. Pentru rezolvarea problemelor de compatibilitate dintre elementul de comanda si camera mobila se pot folosi convertoare de protocol. Totusi este posibil ca din protocolul « sursa » sa nu poata fi traduse toate comenzile in protocolul « destinatie », acest lucru ducand la anumite limitari ale functionalitatii camerei.

O alta clarificare a camerelor este data de tipul de semnal video : camere color, camere alb/negru si camere de tip day/night.

Camere Zi/Noapte (Day/Night) :

O gama aparte de camere o constituie camerele de tip Zi/Noapte. Aparitia acestor camere are la baza comportamentul diferit al camerelor monocrome si al celor color in conditii slabe de iluminat (in general noaptea, dar pot fi si alte conditii, de exemplu camere slab iluminate etc.). Camerele color, raportate la cele monocrome, aduc in plus informatia de culoare, extrem de utila pentru ochiul uman, totusi camerele monocrome sunt mult mai sensibile decat cele color in conditii slabe de iluminat, cele color avnd nevoie de mai multa lumina pentru a furniza un semnal util. Asa cum s-a aratat mai sus lumina este un factor foarte important in functionarea unei camere video. Fara lumina nici-o camera nu poate furniza un semnal video util. Din spectrul de radiatie, prezentat in paragraful referitor la

lumina, o camera color poate percepe mai mult decat ceea ce poate percepe ochiul uman (radiatia vizibila), intrand in gama de radiatie infra-red pana la aproximativ 1000 nm. Totusi, pe timp de zi, a percepe aceasta radiatie IR inseamna a distorsiona culorile, asa cum sunt ele percepute de ochiul uman. De aceea toate camerele color sunt echipate cu un asa numit « IR-cut filter », filtru de eliminare a radiatiei IR. Acest filtru elimina radiatia IR si permite afisarea culorilor in mod natural. Filtru poate fi mecanic –o piesa de sticla plasata intre lentila si senzorul de imagine - sau electronic – aceasta apare ca o functie a chip-set-ului camerei. La scaderii iluminarii sub o anumita valoare, intr-o camera de tip Day/Night, acest filtru este scos, astfel incat lumina IR sa ajunga pe senzorul de imagine, iar camera trece in modul de functionare monocrom.

2.5 MEDII DE TRANSMISIE A SEMNALULUI VIDEO

Cablul coaxial

Cablul coaxial este cel mai raspandit mediu de transmisie a semnalului video.
Componenta acestui tip de cablu este aratata in figura de mai jos.

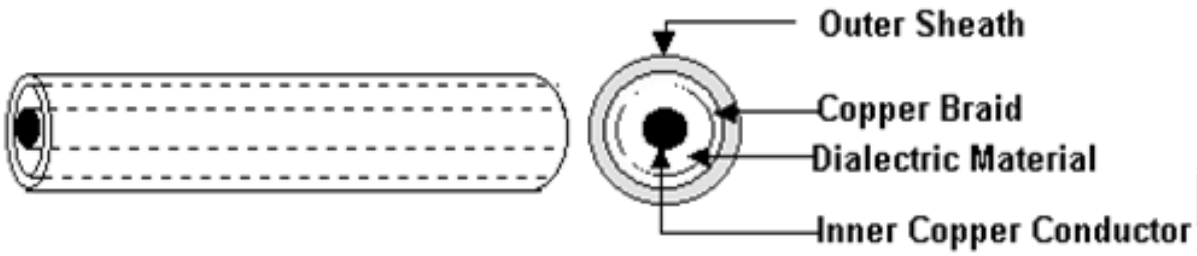


Figura 3.1 Cablul coaxial

Printre carcteristicile de baza se numara :

- impedanta de 75 Ohmi
- imunitate relativ buna la perturbatii de frecventa inalta
- varietate de tipuri
- latime de banda suficienta pentru tipul de semnal video composit

In tabelul urmator sunt exemplificate diferitele tipuri de cablu coaxial folosite des in sistemele CCTV :

Tip cablu	Lungime maxima recomandata (metri)	Atenuare (dB/100m @ 5 MHz)
RG59	250-300	2.2
RG6	500-700	1.8
RG11	800-1000	1.2

Optiunea pentru cablul coaxial trebuie sa aiba in vedere atat distantele de transmisie cat si atenuarile de semnal. Se pot obtine distante mai mari folosind echipamente de amplificare a semnalului. Un sistem de televiziune cu circuit inchis foloseaste semnale in banda de 5Mhz. In conditii reale cablul are o anumite carcteristici de rezistivitate care duc la atenuari ale semnalului. Atenuarea creste cu lungimea cablului si se masoara in decibeli (dB).

Perechea torsadata (UTP –Unshielded Twist Pair)

O optiune din ce in ce mai folosita pentru distante mari (ce depasesc 300m, dar nu numai) este cea de a transmite semnalul video folosind perechea torsadata si echipamente intermediare de conversie.
Acest tip de transmisie are cateva avantaje :
- distante mai mari de transmisie (folosind echipamente active)
- costuri mai mici de instalare comparativ cu fibra optica

- folosirea unor echipamente care au izolare galvanica
- imunitate crescuta la pertrubatii de joasa frecventa, datorate modului de transmisie

Fibra optica

Fibra optica este un mediu de transmisie relativ nou pentru sistemele de supraveghere ce se bazeaza pe transmisia luminii printr-o fibra de sticla de dimensiuni foarte mici. Acest mediu de transmisie a devenit o alternativa viabila si extrem de eficienta la mediile bazate pe cupru folosite in diverse sisteme de telecomunicatii, instrumentatie si control, broadcast, sisteme de securitate etc. Capacitatea fibrei optice de a transmite volume mari de informatie la viteza luminii a revolutionat industria de comunicatii si nu numai. In acelsi timp cu volumul mare de informatii ce se pot transmite se diversifica si tipul de semnale transmise, acest lucru ducand la aplicatii mai sofisticate.

Avantajele fibrei optice sunt :

- dimensiuni si greutate reduse
- latime de banda foarte mare, acest lucru ducand la posibiliotatea folosirii unui singur mediu de transmisie pentru mai multe scopuri/ aplicatii.
- atenuare scazuta (pentru fibra single-mode 0.3dB/Km, multi-mode 0.35dB/Km), acest lucru duce la acoperirea de distante mari fara alte echipamente intermediare de amplificare
- imunitate la zgomot, spre deosebire de cablul de cupru ce necesita ecranare pentru atenuarea perturbatiilor electromagentice, fibra contine un material dielectric ce nu este afectat de radiatia electromagnetica sau de interferente radio
- transmisie securizata, fibra nu radiaza nicio forma de energie care poate fi interceptata, iar bresele in fibra duc la pierderea semnalului
- nu exista scurt-circuite, este folosita in medii explozive sau industriale fara pericol de foc
- performante stabile in timp si pentru diferite configuratii

Cateva din dezavantajele fibrei optice sunt :

- costul componentelor, conectorilor, cablurolor, echipamentelor de testare si de conectare
- refacerea conexiunilor este mai dificila, odata sistemul instalat este dificil de montat noi conectori si/sau echipamente indermediare

2.6 ECHIPAMENTE DE ACHIZITIE, PRELUCRARE SI AFISARE

Sub aceasta denumire am incadrat o mare varietate de tipuri de echipamente ce au functii si caracteristici diverse, toate folosite pentru aplicatii diverse : monitorizare, inregistrare, comutare, afisare semnale video, comanda echipamente etc.

Digital Video Recorder-ul a fost evolutia fireasca a sistemelor de inregistrare video cand s-a trecut de la VCR (Time Lapse Recorder) care folosea banda magnetica pentru inregistrare, la solutia de inregistrare pe Hard Disk. Principalele roluri ale unui DVR sunt :

- inregistrarea semnalelor video furnizate de catre camere, pe hard disk-urile interne
- redarea (playback-ul) acestor inregistrari
- arhivarea informatiei digitale pe diverse suporturi (DAT, matrice de hard disk-uri RAID, LAN, USB, CD, DVD-RW)
- afisarea semnalelor video in timp real pe monitoarele atasate
- comunicatia cu un software client pentru furnizarea de informatii video si/sau setari

Toate aceste functii se pot executa simultan (de unde si denumirea de DVR pentaplex).

Inregistratoarele video digitale se impart in doua mari clase : inregistratoare de tip « stand-alone« si cel de tip « PC-based« .

Inregsitratoarele de tip stand-alone sunt echipamente dedicate. Ele au doar rolurile specificate anterior si nu pot fi folosite in alte scopuri. Acest tip de echipament este bazat pe o structura hardware dedicata ce contine o placa de baza in care sunt inglobate functiile de conversie analog digitala, compresie, stocare, interfata cu utilizatorul. In fapt, este o structura de calcul dedicata,

bazata pe un procesor de tip industrial, pe aceasta structura este instalat un sistem de operare (kernel) tip Linux Embedded, avand doar functiile strict necesare functionarii acestui echipament. Modul de operare al acestui tip de echipament este bazat pe o interfata de operare prin butoane sau telecomanda, dar se poate opera si prin intermediul unui software client de gestiune.

Inregistratoarele PC-based, asa cum le spune si numele, sunt echipamente de calcul de larg consum (PC-uri, eventual cu specificatii mai bune), care au in dotare un numar de placi de achizitie a semnalelor video si un software dedicat care permite integrarea acestor placi pe structura de PC si operarea sistemului ca un inregistrator video. Sistemul de operare al acestor DVR-uri este unul de tip Windows. Majoritatea functiilor inregistratoarelor video sunt comune ambelor tipuri de sisteme.

Inregistrarea este principalul rol al acestor echipamente. Semnalul video preluat de catre sistemul (placa) de achizitie video este transferat la circuitele de conversie analog-digitala, unde au loc procesele de esantionare si cuantizare. Apoi semnalul digital intra in circuitul de compresie. Acest circuit, si functiile implementate in el, joaca un rol important in performanta globala a sistemului. Deoarece semnalul digital obtinut in urma digitizari nu poate fi folosit ca atare (din cauza dimensiunilor foarte mari ale imaginii rezultate) acest semnal digital trebuie compresat pentru a putea fi stocat pe hard-disk. Procesele de compresie video care au loc in circuitele specializate (compresor) vor fi descrise in capitolul referitor la compresia video in sistemele digitale IP. Pe scurt, semnalului video digital de intrare i se aplica un procedeu de compresie video in urma caruia are loc o scadere considerabila a dimensiunilor imaginii rezultate. Imaginea rezultata va putea fi apoi trimisa la sistemul de stocare (HDD). Orice inregistrator foloseste o tehnica de compresie conform unui standard. De exemplu : JPEG, MPEG, Wavelet, MPEG4, MPEG2, H.264 etc. Fiecare din aceste standarde este particularizat de producatorul echipamentului respectiv. Acest lucru insemnand ca nu este posibil sa « citesti« informatia de pe un DVR cu un software de la alt producator. In general producatorii isi parametrizeaza si protejeaza propriul format, tocmai pentru a adauga elemente de securitate, nefiind posibil sa modifici inregistrarile, care pot fi folosite ca probe. Stocarea informatieo video se face pe hard-disk-uri in format proprietar, aceasta putand fi apoi exportata sau arhivata in alte formate proprietare sau standard (AVI de exemplu). Problema stocarii este una deosebit de importanta.

Astazi toate inregistratoarele video digitale au facilitati ce au devenit standard de-facto pentru orice sistem de supraveghere video :

- inregistrare bazate pe evenimente (intrari de alarma, detectie de miscare) programata, continuua
- selectare individuala a ratei de inregistrare si a calitatii imaginii pe fiecare canal
- cautare inteligenta bazata pe tip de eveniment, data&ora, detectie de miscare intr-o anumita regiune a imagini (ROI)
- interfatare cu tastaturi/controllere de comanda a camerelor mobile
- conectivitate in retea LAN/WAN, RS-232, RS-485
- porturi USB, unitati de arhivare CD/DVD-RW, interfata SCSI pentru matrici RAID
- posibilitate de setare software sau prin telecomanda (pentru cele stand-alone)

Matricea video

Este un echipament care are drept principal rol controlul unui numar mare de camere existent intr-o aplicatie. Exista aplicatii in care numarul mare de camere (uzual peste 100), face ca procesul de monitorizare a acestora sa fie destul de dificil. Partea umana a acestui proces, operatorul de supraveghere video, poate fi coplesit de numarul mare de informatii video, astfel incat atentia lui scade dramatic. Matricea video permite controlul unui numar mare de camere video, preluarea acestor semnale video pe intrari, si afisarea lor pe un numar relativ mic de iesiri de monitor. Afisarea pe iesirile de monitor se poate face in mod automat sau manual.

Pentru modul automat se programeaza asa numitele secvente, care sunt constituite din perechi <camera, monitor, timp de afisare>. O astfel de secventa de perechi poate fi « rulata« in mod manual, daca operatorul comanda acest lucru sau se poate activa automat atunci cand se porduce un eveniment in sistem. Uzual operatorul poate sa selecteaze pe orice monitor (iesire din matrice) orice camera video (intrare in matrice). Matricea se opereaza prin intermediul unor tastaturi, pentru sistemele mari (numar mare de camere) fiecare operator are propria tastatura si set de monitoare pe care urmareste aria alocata. Matricea video poate sa aiba si module de intrari de alarma pentru a putea primi informatii de la alte sisteme si sa decida, automat, actiunile ce se executa la un anumit eveniment. Un exemplu ar fi urmatorul : operatorul urmareste pe monitoarele sale un grup de camere din zona publica a unui Mall, daca o usa de urgenta de pe un hol tehnic se deschide, atunci in matrice se va activa o intrare de alarma (contactul magnetic de pe usa de urgenta), iar pe monitoarele de alarma vor fi afisate camerele de pe holul tehnic si camera de exterior care supravegheaza usa de urgenta.
La fel ca si DVR-urile si matricile video pot fi integrate in sisteme complexe, comanda catre matrice putand fi data pe baza unor evenimente din alte sisteme (control acces, efractie, building management etc.).

Monitoare video

Odata cu procesul de digitizare a sistemelor si monitoarele au cunoscut o evolutie de la cele analogice CRT (Catode Ray Tube) la cele de tip TFT, LCD, plasma. Un tip aparte de sistem de afisaj este cel numit Video Wall, destinat dispeceratelor de dimensiuni mari, unde exista multa informatie de afisat.

Amplificatoare/Convertoare video

Amplificatoarele video sunt folosite pentru imbunatatirea calitatii semnalului atunci cand avem pierderi de semnal sau se doreste atingerea unei distante mai mari de transmisie. In ceea ce priveste convertoarele video acestea sunt folosite in principal cand se doreste transmisia semnalului video pe diferite medii de transmisie, de exemplu Coaxial-UTP, coaxial – fibra optica etc. Convertoarele video coaxial-UTP sunt folosite la transmiterea semnalului video pe perechea torsadata. Aceste convertoare se impart in

- active : necesita alimentare separata
- pasive : nu au nevoie de alimentare separata.

3. ALIMENTAREA SISTEMELOR TVCI

Alimentarea sistemului de televiziune cu circuit inchis se va face, pe cat posibil, dintr-o singura faza a tabloului principal de alimentare. In acest scop se va folosii un circuit dedicat acestui subsistem. Sunt situatii in care acest lucru nu este posibil. In acest caz trebuie evitate problemele cauzate de diferentele in sincronizarea camerelor alimentate din faze diferite.
Un element important este cel privind impamantarea. In majoritatea cazurilor acesta exista in obiectiv, dar sunt si situatii in care se cere realizare unei prize de pamant,. Toate echipmanetele trebuie sa fie conectate la impamantare pentru a permite o cale de eliminarea descarcarilor electrostatice si a protectiei personalului. De mentionat ca aceasta impamantare este diferita de masa de alimentare si de masa de comunicatie (RS-485 COMUN).

Pentru a a sigura un consum neintrerupt se recomanda utilizare de surse cu acumulatorii pentru camerele cu alimentare in 12/24VDC sau asigurarea de surse UPS cu durata de pana la 24 de ore pentru camere si pentru echipamentul de inregistrare, alimentate in cuernt alternativ.

4. DEFECTIUNILE SISTEMULUI TVCI

Notiunea de defectiune este strans legata de fiabilitatea sistemului TVCI. Fiabilitatea este unul dintre parametrii principali ai calitatii unui sistem de securitate si, in particular, al unui sistem de televiziune cu circuti inchis. Fiabilitatea se realizeaza/ calculeaza/ modeleaza tinand cont de toate fazele prin care trece sistemul: conceptie, proiectare, instalare si exploatare. Din punct de vedere calitativ fiabilitatea este aptitudinea (capacitatea) sistemului, aflat in conditii date de utilizare, de a-si indeplinii functiuni specifice o anumita perioada de timp. Din punct de vedere cantitativ fiabilitatea este probabilitatea ca, la un anumit moment, un dispozitiv (sistem), aflat in conditii date de utilizare, sa isi indeplineasca functiunile specifice. Prin caracteristicele calitative pe care le are, si in special cea de fiabilitate, se poate considera ca fiabilitatea sistemului inseamna “calitatea in timp”. O analiza de fiabilitate poate duce la imbunatatirea calitatii in proiectare, instalare si asigura o functionalitate cu o probabilitate mica de defect critic a sistemuluil TVCI. Aceaasta analiza va duce deasemenea la o planificare a activitatilor de mentenanta si o planificare a stocurilor de piese de schimb si accesorii necesare proceselor de mentenanta preventiva si corectiva.. Scopul final Il constituie reazlizarea si furnixzarea unui sistem TVCI cat mai fiabil pentrui o anumita perioada de timp.

Defectiunea reprezinta o pierdere partiala sau totala a capacitatii de functionare a unui dispozitiv sau sistem precum si orice modificare a valorilor parametrilor sai constructivi si functionali in afara limitelor prevazute in documentatie.

Putem clasifica defectele folosiind mai multe criterii:

1 In raport cu cauzele care le-au produs:
- de proiectare
- de fabricare
- de instalare
- de utilizare
- accidentale

2 In functie de corelarea cu alte defectiuni
- Primare (cauza este intrinsecsa dispozitivului, sistemului)
- Secundare (a fost cauzata ca urmare a defectarii unui alt dispozitiv sistem cu care acesta interactioneaza)

3 Dupa viteza de aparitie
- Bruste
- Progresive (uzare, corodare, imbatranire etc)

4 Dupa frecventa de aparitie a defectelor
- Sporadice <30% - nesemniicative <10%
  - de importanta mica 10%-30%
- Cronice >30%

5 Dupa consecintele defectiunii:
- Minore - nu impiedica functionarea sistemului in ansamblu (functii considerate secundare nu sunt realizate)
- Majore - impiedica realizarea functiilor pirncipale ale sistemului
- Critice – pot provoca distrugeri/pierderi de bunuri/valori sau vieti omenesti

6 dupa volumul operatiilor de restabilire a starii tehnice initiale:

- Dereglari- necesita setarea, reprogramarea unor piese/dispozitive, fara a le inlocuii
- Caderi – necesita remedierea su inlocuuirea unor piese/dispozitive
- Avarii –necesita interventii la nivelul intregului sistem si operatii complexe de inlocuire si/ sau reporgramare

7 Dupa durata manifestarii defectiuni:

- Temporare – aparitie rara si de scurta durata
- Intermitente – aparitie frecventa si de scurta durata
- Permanente – aparite rara dar de lunga durata

8 Dupa usurinta depistarii:

- Evidente
- Ascunse

9 Dupa perioada din viata dispozitivului/sistemului in care se produc defectiuni:

- Precoce
- Alaeatoare
- De imbatranire

Defectiuni datorate etapelor de proiectare, instalare, montaj.

Probleme de sincronizare.

Una din cele mai dese probleme este lipsa sincronizarii echipamentelor cu transmise/receptie de semnal analogic.

Figura. exemplu de imagine cu probleme de sincronizare

Acest tip de probleme se datoreaza unor factori precum:
- *bucla de impamantare*

O problema ce poate sa apara atunci cand se foloseste cablul coaxial ca mijloc de transmisei a semnalelor video, este cea a impământarilor diferite pentru camera si pentru echipamentul de preluare a semnalului video. Daca la nivelul camerei exista o impamantare iar la nivelul DVR-ului (monitor, matrice etc) alta impamantare apare asa numitul fenomen de bucla de impamantare, care consta in producerea/aparitia unei diferente de tensiune intre cele doua impamantari si aparitia unui curent ce poate duce la distrugerea echipamentelor. Eliminarea acestui fenomen se face prin folosirea unei singure impamantari (daca este posibil) sau introducerea unor echipamente numite izolatoare de impamantare, care separa din punct de vedere electric cele doua echipamente.

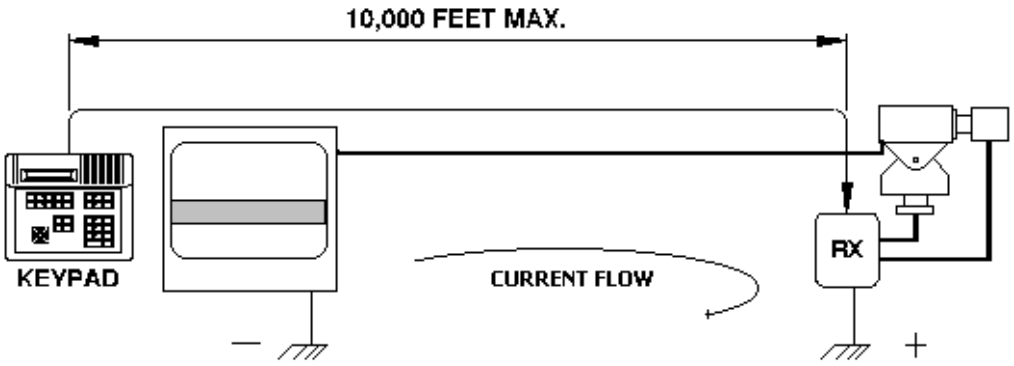


Figura: Aparitia unui diferente de potential intre cele doua impamantari

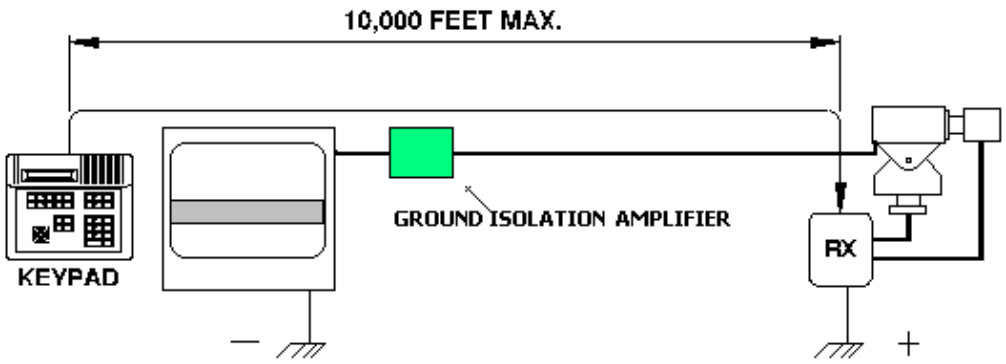


Figura: Eliminarea curentului datorat buclei de impamantare

- *interferente electomagnetice sau radio* (RFI – radio frequence interference sau EMI – electromagnetic interference)

In cablul coaxial se pot induce perturbatii electromagnetice (EMI - ElectroMagnetic Interference) daca acest tip de cablu este instalat in apropierea unor surse de inalta tensiune sau alaturi de cabluri cu curenti tari. In final perturbatiile pot avea drept rezultat o calitate proasta a semnalului.

- *lungimi de cablu mari*

Atunci cand se folosesc peste limitele recomandate sau se folosesc alte tipuri de cablu decat cele recomandate de producator pentru atingerea distantelor necesare aplicatiei respective.

Probleme de terminator semal video

Pentru a evita scaderea valorii semanlului si aparitia distorsiunilor in imaginea video rezultata se recomanda utilizarea asa numit-ului terminator de 75Ohm. Acest terminator impiedica aparitia distorsiiunilor, Lipsa acestui terminator sau un terminator impropriu (sau dublu terminator) provoaca afisarea de imagini duble, imagini intunecate sau fade

Probleme de comunicatie

Sunt specifice camerelor mobile si echipamentelor care sunt folosite pentru a comunica cu acesta. Intrefata electrica cea mai folosita pentr pentru aceasta comunicatie este RS-495 sau RS-422. Aceste interfete permit atingerea unor distante mari, 1200m sau chiar maim mari daca se folosesc si echipmanet de amplificare / conversie date.

Cateva din cauzele comune ale problemelor de comunicatie sunt:

- lipsa terminatorilor de linie,
- folosirea de cabluri de proasta calitate
- folosirea de cabluri nerecomandate pentru lungimea dorita
- conectarea masei de comunicatie la masa de alimentare
- adresarea incorecta

Un aspect important este cel privind folosirea protectiilor la supratensiune pe liniile de comunicatie, mai ales in aplicatii de exterior si de distanta mare.

6. CERINTE DE INSTALARE

Pe parcursul capitolelor precedente s-au facut cateva precizari privind conditiile de instalare si modalitatile de a realiza un sistem de supraveghere video eficient si performant. Pentru a realiza un astfel de sistem se impune ca proiectarea si alegerea unor componente sa se faca dupa o analiza generala, care sa raspunda cat mai multor cerinte. Punctul de plecare il constituie cerintele impuse sistemului. Aceste cerinte trebuie sa raspunda la urmatorul gen de intrebari :

- ce se doreste prin instalarea sistemului de supraveghere ?
- pentru supravegherea in timp real, la ce calitate ?
- pentru inregistrare, la ce calitate ?
- care sunt conditile de inregistrare si arhivare ? cat timp se pastreaza informatia video ?
- cum este operat sistemul ? este supravegheat continuu sau doar din cand in cand?
- se doreste exportul inregistrarilor ? daca da, in ce format ?
- care sunt conditiile de instalare ? (montaj, iluminat, locatie)
- care sunt condtiile de transmisie a semnalelor video si ale semanlelor de date?
- se doreste interconectarea cu alte sisteme ?

Toate aceste intrebari, si multe altele, conduc in final la stabilirea unor specificatii pentru elementele componente si pentru sistem in ansamblu.

Conditiile de iluminat. Asa cum am mai precizat pentru a avea imagini de calitate buna trebuie ca sa avem cat mai multa lumina. O cauza comuna pentru calitatea slaba a imaginilor o constituie lipsa lumini. In general cu cat avem mai multa lumina cu atat avem o imagine mai buna. Cand se folosesc camere de exterior se recomanda folosirea unor surse suplimentare de lumina – eventual iluminatoare in IR. Este important de ales o camera care sa aiba o sensibilitate cat mai mare astfel incat sa poata reda imagini cat mai bune pentru conditii slabe de iluminat. Invers, prea multa lumina poate duce la fenomenul de suprailuminare, de aceea se recomanda evitarea luminii directe a soarelui si folosirea de incinte cu parasolar. Daca o camera este montata intr-o incinta este posibil sa apara fenomene de reflexie cauzate de geamul incintei, acest lucru se poate elimina prin montarea lentilei cat mai aproape de geamul incintei.

Lentila. Pentru aplicatii de interior unde iluminatul este constant se pot alege lentile cu iris manual dar pentru aplicatii de exterior se va alege intotdeauna o lentila cu autoiris. Lentilele varifocale sunt recomandate pentru marea majoritate a aplicatiilor intrucat au o mai mare flexibilitate si pot fi folosite pe o gama mai larga de aplicatii mai ales cand nu se stiu de la inceput toate condtiile de montaj.
Pentru conditii de exterior se vor folosii camere de tip Day/Night care pot sa-si foloseasca sensibilitatea sporita in condiile slabe de iluminat.
Conditiile de montaj trebuie asigurate astfel incat camerele sa fie bine ancorate pe stalpi, suporti, ziduri si sa nu fi e afectate de vant puternic sau alte condiit meteo.
Modalitatea de transmisie trebuie aleasa in functie de lungimea traseului, conditiile de cablare si de vecinatate cu eventuale surse de perturbatii electromagnetice sau radio. Chiar daca este mai scump la inceput, alegerea fibrei optice, de exemplu, poate sa rezolve o serie de probleme care, in timp, pot sa coste mai mult decat costul initial al folosirii unui astfel de mediu. (de mentionat problemele de impamantare si perturbatii).
Alegera echipamentelor de comutare, inregistarea si afisare se face tinind cont de factorii precizati la descrierea fiecarui echipament in parte. Solutia aleasa trebuie sa asigure, in acelasi timp, scalabilitatea, posibilitatea de extindere si de interfatare cu alte sisteme.

7 SERVICE SI MENTENANTA

In cadrul operatiunilor de service si mentenanta (intretinere) se executa acele operatii care duc la pastrarea si prelungirea starii de buna functionare precum si a remedierii defectelor, conform cu cele descrise in capitolul DEFECTIUNILE SISTEMELOR TVCI.
Operatiile de service care se executa pe baza unui contract de service se incadreaza in operatii de mentenanta preventiva si corectiva,

VERIFICARI GENERALE / MENTENANTA PREVENTIVA

- Examinarea aspectului exterior al camerelor video si al echipamentelor de comutare, inregistrare si afisare
- Repozitionarea camerelor datorita modificarii in timp a pozitiei din cauza slabirii elementelor de prindere/orientare;
- Verificarea calitatii imaginilor transmise de camere si eventual reglarea celor care au imaginea alterata; In cazul in care alterarea imaginii unei camere de exterior este produsa de aburirea geamului incintei termostatate se va verifica si inlatura cauza care a produs efectul mentionat mai sus. Alterarea imaginii mai poate proveni si datorita oxidarii mufelor, ceea ce impune inlocuirea lor;
- Verificarea calitatii imaginilor afisate de monitoare;
- Verificarea calitatii inregistrarilor video;
- Indepartarea prafului si a murdariei de pe monitoare, inregistratoare, matrici video si orice alt echipament ce constituient al sistemului TVCI.
- Verificarea tensiunilor de alimentare si a incarcarii acumulatorilor.

VERIFICARI SPECIFICE LA REVIZII PERIODICE

Sunt incluse operatiuni de amploare si intensive ce urmaresc verificarea unor functii si, eventual, remedierea unor defecte, precum si cautarea si eliminarea cauzelor care au dus la modificarea sau lipsa unor parametrii/ functii specifice sistemelor TVCI.
Aceste operatii includ :

- Verificarea si reglarea camerelor video din punct de vedere al calitatii imaginii si al pozitiei ;
- Verificarea parametrilor specifici monitoarelor;
- Verificarea functiilor si setarilor echipamentelor de comutare, inregistrare si afisare
  Verificarea tensiunilor de alimentare ale tuturor echipamentelor;
- Verificarea arhivarii si a calitatii suporturilor de arhivare;
- Verificarea calitatii inregistrarilor si a arhivei ;
- Verificarea elementelor de interactiune cu alte sisteme (comutare camere video la evenimente de tip intrari de alarma, detectie de miscare incendii, cutremure,etc.) ; Verificarile includ memorarea prepozitiilor, a tururilor.

Întocmit

Ing. Viorel TULEŞ

SISTEME DE CONTROL AL ACCESULUI

CAPITOLUL 1

PREZENTARE GENERALA

Sistemele electronice de control acces sunt sisteme complexe formate din componente mecanice, electromecanice, electronice (hardware) si software, interconectate astfel incat sa asigure functiile de protectie si control impuse anumitor tipuri spatii. Practic sistemele de control acces asigura necesarul de siguranta si securitate ce trebuie avut in vedere indifernt daca vorbim de aplicatii de paza perimetrala, acces in parcari, spatii de birouri, aplicatii militare, cladiri de birouri sau zone de inalta securitate. Gama de aplicatii in care sistemele de control acces isi au un rol bine definit este foarte mare. In aceasta gama se includ si aplicatii care nu sunt strict legate de securitate ci, folosind aceleasi tehnici si sisteme, asigura functii de accesare la nivel logic, interfatare cu sisteme de baze de date si sisteme de pontaj si resurse umane, controlul resurselor, identificare automata etc.

Sistemele electronice de control acces au devenit o componenta de baza a oricarui sistem de securitate integrat atat la nivel fizic, hardware, cat si la nivel logic, software. Sistemele de control acces se pot interconecta la sisteme existente sau pot asigura infrastructura pentru sisteme viitoare. Rolurile si functiile asigurate de catre aceste sisteme s-au diversificat de-a lungul timpului astfel incat astazi avem o paleta extrem de mare de functii ce pot fi realizate folosind facilitatile oferite de diversi producatori ai sistemelor de control acces.

In termeni reali sistemele de control acces se bazeaza pe tehnologii diverse care, practic, cuprind toata gama de sisteme de securitate, dar in special detectia la efractie si TVCI, sisteme cu care practic formeaza un « sistem integrat de securitate« , in care orice eveniment de securitate este abordat intr-o maniera unitara si tratat prin mijloace specifice : detectie, avertizare, restrictionare, vizualizare, inregistrare.

Principalele functii ale unui sistem de control acces constau in :

- identificare/autentificare
- restrictionarea accesului
- blocarea accesului folosind elemente electromecanice
- aplicarea politicilor de securitate intr-un anumit spatiu
- monitorizarea elementelor din sistem si a utilizatorilor
- detectia si inregistrarea evenimentelor precum si luarea deciziilor aferente
- raportarea, audit

Spre deosebire de un sistem de detectie a efractiei, care are ca scop protejarea intregului spatiu securizat un sistem de control acces se concentreaza pe caile de intrare/iesire din spatiul securizat. Modelul de securitate aplicat este unul bazat pe nivele de securizare fizica si logica. Spatiul securizat este, in general, ierarhizat pe diferite nivele de securitate, pentru fiecare nivel aplicandu-se metode specifice acelui tip de spatiu, care indeplinesc cel mai bine cerintele de securitate impuse.

Odata cu cresterea nivelului de securitate masurile de identificare si control devin mai riguroase.
Pentru controlarea accesului perimetral/exterior se folosesc : bariere auto, cititoare de raza mare, porti de acces de inalta securitate pentru pietoni, tururi de garda, identificarea automata a vehiculelor etc. Pentru controlarea accesului in spatii comune/publice se folosesc : porti de acces de viteza mare, turnicheti, controlul lifturilor si al usilor de urgenta, gestiunea vizitatorilor etc. Pentru controlarea zonelor de inalta securitate se folosesc cititoare de diverse tehnologii, (proximitate, smart card, biometrie), bariere infrared, terminale de pontaj si acces, functii speciale (anti-passback, two-cards, visitor escort, card tracking) etc. Odata cu cresterea riscului de securitate cresc si masurile de identificare si autentificare. Daca pentru zonele cu risc scazut se foloseste o singura masura de autentificare

(cod PIN, cartela de proximitate sau biometrie) pentru zonele cu risc mare de siguranta se folosesc metode de autentificare multiple (multi-factor - cod PIN si biometrie, smartcard si biometrie etc,). Acesti factori pot sa difere in functie de locatie, momentul in care se cere autentificarea, permisiunile persoanei care cere autentificarea si de alti factor impusi prin procedurile de securitate.

In practica orice sistem trebuia sa aiba o combinatie echilibrata intre permisiune si restrictie. O serie de reguli se aplica oricarui sistem de control acces: cu cat un spatiu este mai slab securizat cu atat este mai susceptibil de a fi accesat de persoane neautorizate si, invers, cu cat un spatiu este mai bine securizat cu atat va fi mai susceptibil de a interzice accesul unei persoane autorizate.

CAPITOLUL 2

ELEMENTE COMPONENTE

Pentru un utilizator obisnuit un sistem de control acces este constituit din trei elemente :

- o cartela/un cod PIN/un tag – care se prezinta unui cititor/tastatura
- un cititor/tastatura – care autentifica cartela/PIN-ul
- o usa/bariera/poarta de acces – care se deschide cand se autorizeaza intrarea

In spatele acestei scene se afla un numar de echipamente interconectate, folosind tehnologii diverse, ce comunica in vederea realizarii functiilor de control acces.

Din punct de vedere al structurii unui sistem de control acces se disting urmatoarele nivele pe care sunt distribuite elemntele componente ce au roluri distincte in functionarea sa:

- nivelul echipamentelor de camp
- nivelul echipamentelor hardware de achizitie si control
- nivelul de programare/gestionare software

In tabelul de mai jos sunt exemplificate cateva din tipurile de echipamente existente intr-un sistem de control acces si nivelul la care sunt intalnite.

Nivel	Tipuri de echipamente	Tip resurse
Echipamente de camp	Bariere auto, usi de control acces, turnicheti, porti de acces, incuietori electrice/ electromagnetice, contacte magnetice, butoane de comanda, fotocelule, surse de alimentare etc	Mecanice, electromecanice, electrice sau electronice
Echipamente de achizititie si control	Cititoare diverse tehnologii, tastaturi, unitati de control acces, controllere de lift, interfete de intrari/iesiri, interfete de comunicatie, terminale de pontaj etc.	Electronice, hardware, firmware
Nivel de aplicatie	Calculatoare de gestiune, software de management, retele de comunicatii etc.	Hardware, software, networking

Dupa cum se poate vedea un sistem de control acces este, in general, o combinatie de diverse tehnologii de la cele mecanice pana la cele de tip software si retelistica. Intotdeauna un sistem de control acces va avea realizate primele doua nivele, nivelul de programare/gestionare software poate sa lipseasca in anumite tipuri de sisteme, unde cerintele de securitate sunt mai reduse, aceste functii fiind asigurate pe echipamentele de la nivelul de achizitie si control (de exemplu tastaturile/cititoarele stand-alone). Pentru fiecare dintre aceste nivele se va face o descriere a tipurilor de echipamente si a principiilor functionale.

Nivelul echipamentelor de camp

La acest nivel se afla elemente mecanice si electromecanice care asigura functiile de blocare/ restrictionare a accesului in spatiul securizat. Gama de echipamente utilizate pentru blocarea accesului este foarte larga incluzand atat echipamente de exterior cat si de interior, pentru persoane si autovehicule. In aceasta gama de echipamente se gasessc : usi, porti, bariere, turnicheti etc.

Bariere de acces auto

Acest tip de echipament este folosit pentru controlarea traficului auto in punctele de acces si este, de obicei, primul contact cu un sistem de control acces. Bariera este un echipament electromecanic echipat cu o unitate de control electronica, un element de actionare si bratul barierei. Pentru o functionare in siguranta se foloseste o fotocelula de siguranta, care permite blocare bratului barierei in conditiile prezentei unei masini sau persoane in spatiul de actionare al barierei. In multe aplicatii se folosesc si sisteme de semaforizare care regleaza in timp accesul la bariera. In mod uzual bariera poate fi folosita si fara o comanda dintr-un sistem de control acces, in acest scop folosindu-se doar o telecomanda radio sau butoane de comanda (inchis, deschis). Barierea poate functiona in mai multe moduri

- regim manual – comenzile de deschidere/inchidere sunt date direct de un operator folosind o cheie, butoanele de comanda sau telecomnda radio. In acest regim comenzile de inchidere si deschidere sunt date separat, intre cele doua comenzi bariera ramane deschisa.
- regim automat – comenzile sunt date dintr-un sistem de control acces In acest regim comanda este data de la un echipament de control suplimentar. In acest regim timpul de deschidere este programat in unitatea de control a barierei.

Barierele difera din punctul de vedere al tipului de aplicatie – de trafic intens sau trafic redus, primele avand un timp de deschidere mai mic, in functie de lungimea bratului (2m-6m), de tipul constructiv (brat dintr-o bucata sau din doua parti) sau rezistenta.

Metodele automate de accesare a barierelelor includ :

- tichete de parcare bazate pe banda magnetica sau jetoane de parcare - sunt folosite in parcarile cu plata
- bucla inductiva – un cablu metalic ingropat, conectat la un controller, ce actioneaza ca o antena inductiva, sensibil la prezenta unor obiecte metalice (masini). Acest echipament este foarte util pentru parcari unde iesirea se face fara a fi necesara alta forma de control (card, tag, telecomanda radio, actionare manuala)
- cititor de proximitate de distanta mare si tag-uri active – acesta este un cititor special pentru aplicatii de acces auto. Datorita dimensiunilor mari ale antenei si a curentului indus in antena acest tip de cititor are o raza de citire de pana la aproximativ 70 cm., daca este folosit cu card-uri pasive, si pana la aproximativ 2m daca este folosit cu carduri active (carduri ce incorporeaza o baterie)
- cititor de tag-uri auto, de distanta mare, folosind microunde. Acesta este un cititor de un tip special, functionand pe microunde la frecvente in jur de 2.4GHz. In conjunctie cu tag-urile active instalate pe autovehicol se atinge o distanta de apx 10 m de citire a tag-ului, astfel incat comanda barierei se poate da inaintea ajungerii masini in dreptul acestei bariere. Acest cititor se monteaza in apropierea barierei la o inaltime cuprinsa intre 2 si 4 m astfel incat sa asigure o raza de citire potrivita aplicatiei.
-

Orice zona cu restrictii de acces auto impune folosirea unor astfel de bariere. De mentiont ca barierele asigura o foarte scazuta securizare a spatiului pentru pietoni. Pentru pietoni urmand sa se foloseasca alte tipuri de echipamente de blocarea accesului.

Porti de acces

Un tip aparte de « bariera » o constituie portile metalice de acces auto. Acestea, spre deosebire de barierele auto, asigura o securitate marita atat pentu vehicule cat si pentru pietoni.
Portile metalice sunt clasificate din punctul de vedere al modalitatii de deschidere in :

- porti batante - se deschid in lateral
- porti culisante - culiseaza pe o sina metalica, sau au o roata de deplasare.

Ambele tipuri de porti sunt actionate folosind elemente de automatizare comandate prin intermediul unei unitati de control. Ca si barierele auto si aceste unitati pot fi conectate la echipamente de control acces pentrru a primi comenzile de deschidere/inchidere. O particularitate a acestor porti o constituie timpul de deschidere/inchidere care este mult mai mare decat cel al barierelor. Acest lucru face ca acest tip de echipament sa fie folosit in aplicatii unde numarul de vehicule este redus.

Sisteme de intrare pentru persoane. Turnicheti

Atunci cand se doreste comtrolul strict al persoanelor care patrund intr-o anumita zona cu acces restrictionat cea mai buna metoda este folosirea unor sisteme de intrare care pot fi : turnicheti, porti rapide (speed-gate sau porti de intrarare de flux mare), turnicheti industriali etc. aceste sisteme au rolul de a permite accesul doar in conditiile in care accesul se face individual (spre deosebire de usi, unde mai multe persoane pot trece doar cand una singura a prezentat cardul la cititor). Termenul folosit atunci cand mai mult de o persoana trece printr-un punct de acces, atunci cand s-a prezentat un singur card, este tail-gating. Folosind astfel de sisteme se poate calcula cu precizie numarul persoanelor aflate intr-o anumita arie, acest lucru determinand functionarea corecta pentru Muster Report (raportul persoanelor aflate intr-o arie in caz de urgenta) sau Anti-passback.
Turnicheti tip tripod : acesti sunt cei mai uzuale sisteme de intrare. Asigura o separare simpla a persoanelor care doresc sa acceseze puncte de interior sau de exterior. Sunt dotati cu trei brate metalice ce se rotesc in plan vertical, bidirectional, iar in caz de urgenta pot fi rabatati astfel incat sa se asigure o cale de evacuare.

Fig. Exemplu de instalare turnicheti tip tripod

Turnicheti rotativi : acestia sunt un tip de turnicheti folositi in general pentru spatii interioare, au in componenta un ax central in jur caruia se rotesc trei placi de sticla sau bare metalice care separa persoanele ce solicita accesul. La un acces, axul executand o rotatie de 120 de grade, in sensul cerut.

Fig. Exemplu de instalare turnicheti rotativ

Porti de acces : aceste sisteme de intrare mai sunt numite speed gate sau turnicheti tip alee. Acest tip de sistem de intrare este folosit unde se doreste un acces rapid si o verificare sigura a faptului ca doar o singura persoana trece la un moment dat. O cale de acces este formata din doua corpuri de lungime mare (peste 1m) intre care exista calea de acces ce este blocata de doua panouri de sticla ce se retrag cand primesc comanda de deschidere, in interiorul corpurilor. In aceste corpuri se afla echipamentele de comanda si fotocelulele de control a prezentei in spatiul dintre corpuri. In plus aceste echipamente au ca dotari, contoare de persoane, indicatoare luminoase pentru evenimente tip : prezentare card, acces permis, acces interzis, alarma. In plus pot accepta direct intrari de la alte sisteme pentru deschiderea in caz de urgenta si cate o intrare de comanda pentru ambele sensuri de deschidere.

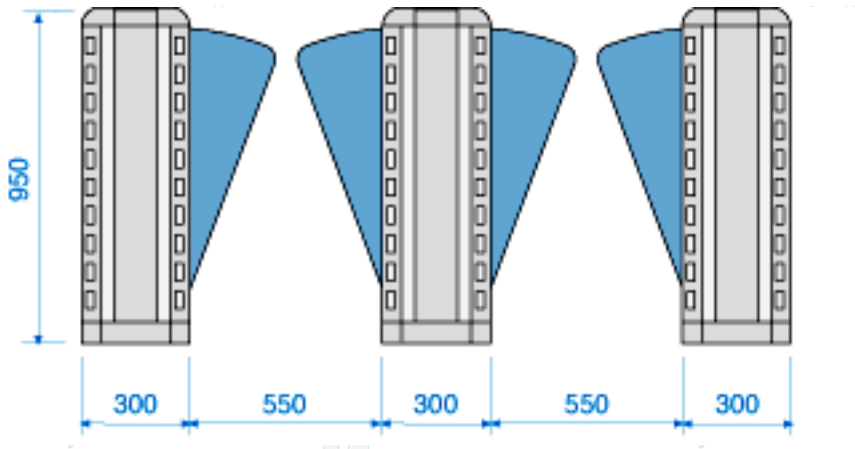


Fig. Exemplu 2 cai de acces cu porti de acces tip « speed-gate »

Porti de urgenta : sunt sisteme de blocare a accesului ce au in componenta un ax central in jurul caruia se roteste o placa de sticla sau un cadru metalic ce blocheaza intrarea. Rolul lor este de asigura un acces pentru situatii de urgenta unde se impune realizarea unei cai de acces suficient de largi. Aceste porti sunt folosite in conjunctie cu celelalte tipuri de porti pentru asigurarea cailor de evacuare in caz de urgenta sau pentru accesul persoanelor cu handicap.

Fig. Exemplu instalare poarta de urgenta

Porti de inalta securitate : aceste echipamente sunt destinate accesului pietonal in spatii externe unde trebuie asigurata o mare securitate fizica a spatiului protejat. Sunt compuse din elemente metalice masive, bare, ce se rotesc in jurul unui ax central, aflat intr-o « carcasa« metalica de protectie. Mai sunt denumite turnicheti tip full-size sau full-high.

Fig. Exemplu instalare turnichete de inalta securitate

Porti de tip « man-trap« : acest tip de echipament este dedicat aplicatiilor de inalta securitate, in care accesul in zonele protejate se face dupa criterii de greutate nu doar de drept de acces. Este compusa dintr-un « tub » in care accesul se face prin doua usi, cate una pentru fiecare parte a zonei protejate, acestea fiind interblocate. Accesul inspre/dinspre zona securizata se face dupa masurarea greutatii persoanei si compararea cu greutatea de referinta (+/- o marja) stocata in sofware-ul de control. Daca este indeplinita conditia atunci se poate face trecerea.

Usa de control acces

Majoritatea spatiilor securizate sunt protejate de o usa si exista multe tipuri de sisteme ce asigura protectia acestora. Exista o varietatea de usi, pentru fiecare dintre ele fiind necesara o atenta selectie a tipului de incuietoare ce va asigura maxima protectie a cai de acces in spatiul securizat.

Un aspect important al unui sistem de control al accesului consta in monitorizarea starii usii. A monitoriza starea usii insemna a cunoaste in fiecare moment daca usa este inchisa sau nu, daca usa s-a deschis in mod normal - prin utilizarea

cititorului sau butonului de iesire-, daca usa s-a deschis normal dar a fost lasata deschisa, daca usa a fost deschisa altfel decat prin mijloacele normale - usa fortata. Deasemenea starea usii este importanta atunci cand se doreste numararea persoanelelor dintr-o arie anti-passback sau executia unor comenzi bazate pe tipul de eveniment "usa deschisa" (de.exemplu interblocarea unor usi de tip SAS). Monitorizarea stari usii se face prin instalarea unui contact magnetic. Acesta poate fi aparent sau ingropat, poate avea diverse marimi, deasemenea se poate folosi contactul magnetic al incuietorii electrice. Ezista variante de contacte magnetice pentru usi de garaj, de tip industrial (heavy-duty). Practic nu se poate spune ca exista control al accesului fara a avea informatia despre starea usii. In functie de starea usii se pot lua deciziile corecte pentru fiecare tip de eveniment. Toate unitatile de control acces au intrari dedicate pentru astfel de contacte de monitorizare a starii usi.

Incuietori electrice si electromagnetice

Spre deosebire de incuietoarea mecanica obisnuită o incuietoare electrica are elementul de actionare al boltului comandat de o bobina in care se induce un curent electric, campul electromagnetica astfel creeat actioneaza asupra elementului de blocare/deblocare a boltului. Incuietorile electrice/ electromagnetice se adapteaza tipului de usa existand multe variante constructive si modalitati de alimentare.

Tipuri de incuietori:

- Electrice ; electric strike, electric drop-bolt
- Electromagnetice: electromagnet tip Maglock
- Electromecanice: cu actionare electrica dar si mecanica

Incuietorile electrice (strike) pot fi de doua tipuri

- Fail-safe (fail-unlock) –acest tip de incuietoare este alimentata pentru a bloca usa, in cazul in care alimentarea este intrerupta strike-ul este deblocat si usa se va deschide
- Fail-secure (fail lock) – acest tip de incuietoare este blocat atat timp cat este nealimentata, pentru a fi deschisa trebuie sa fie alimentata.

Incuietorile electromagnetice (maglock) sunt, prin natura lor, incuietori tip fail-safe. Ele au nevoie de alimentare pentru a produce campul electromagnetic.

Eliminarea tensiuni reziduale asociate cu incuietorile electrice

Una din componentele unei incuietori electrice este bobina ce actioneaza ca un electromagnet asupra elementului de blocare/deblocare a incuietorii. Aceasta bobina actioneaza ca un dispozitiv inductiv de valoare mare. Cand tensiunea continuua este aplicata pe bobina, in bobina se « inmagazineaza« o cantitate de energie care, atunci cand circuitul de alimentare este intrerupt, se transfera pe circuitul de alimentare, sub forma unei descarcari de tensiune, spre unitatea de cotrol sau sursa. Daca nu se aplica o metoda de a elimina aceasta tensiune, de la sursa producerii, este posibil ca ea sa provoace defectarea anumitor componente din sistem. O metoda uzuala pentru incuietorile electrice alimentate in tensiune continuua consta in instalarea unei diode de uz general pe bornele de alimentare ale strike-ului. Catoul este conectat la borna pozitiva a strike-ului astfel incat energia acumulata sa se disipe in strike.

Strike-urile alimentate in curent alternativ nu permit utilizare de diode pentru eliminarea tensiunii reziduale. Pentru acestea se folosesc supresori MOV (Metal Oxide Varistor), deseori acestia sunt inclusi in incuietoare.

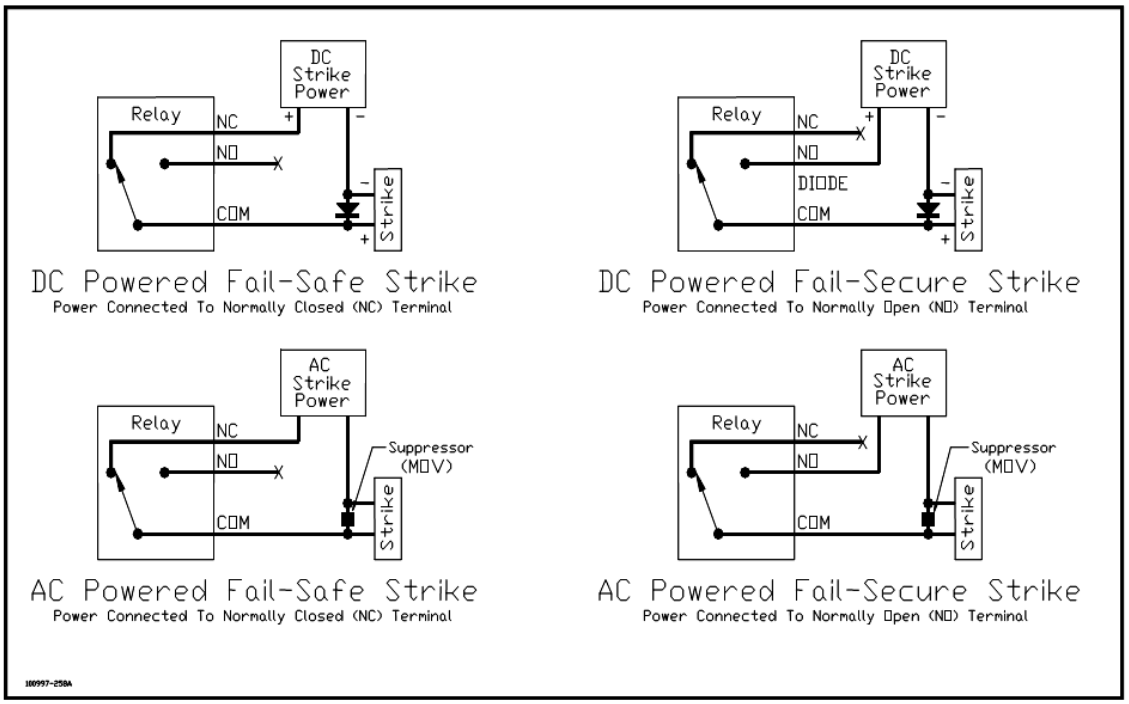


Figura. Metode de protectie ale incuietorilor

Cai de evacuare. Usi de evacuare. Situatii de urgenta

Un sistem de control al accesului trebuie sa asigure restrictionarea accesului intr-un spatiu securizat, totusi exista situatii cand siguranta este predeominanta securitatii. In situatii de urgenta (incendiu, panica, echipamente defecte etc.) se impune evacuarea cat mai rapida a persoanelor aflate in spatiul protejat. Pentru acest lucru trebuie gandite inca de la faza de proiectare mijloacele tehnice ce vor asigura deschiderea usilor desemnate ca usi de urgenta. Usile controlate trebuie sa poata fi deschise cat mai simplu in caz de urgenta.

O cale simpla de a asigura cerinta de deschidere manuala in caz de urgenta consta in instalarea unui buton de urgenta (emergency button) pe calea de iesire din spatiul protejat. Acest echipament permite intreruperea alimentarii incuietorilor electrice / electromagnetice fail-safe sau, pentru cele de tip fail-secure, alimentarea lor. Butonul de urgenta este de fapt un micro-switch, un contact NO/NC, intercalat intre sursa de alimentare si incuietoare. Se recomanda folosirea incuietorilor fail-safe penrtru spatiile publice astfel incat lipsa alimentarii sa nu afecteze functionarea in caz de urgenta a incuietorii. Butonul de urgenta trebuie sa fie de culoare alba sau verde dar nu rosu pentru a nu fi confundate cu cele de incendiu. O alta metoda uzuala pentru deschiderea usilor este cea automata, prin intermediul unei comenzi preluate de la sistemul de detectie incendiu, de exemplu, care permite deschiderea controlata a usilor corespunzator cu scenariul la foc pregatit de proiectant. Majoritatea unitatilor de control acces au intrari ce pot fi programate ca intrari de urgenta.

Nivelul echipamentelor de achizitie si control

La acest nivel se gasesesc echipamentele care realizeaza identificarea utilizatorului si controlul echipamentelor de la nivelul inferior. Acestea se impart in cititoare si unitati de control acces, dar exista si echipamente (numite unitati de tip stand-alone) in care ambele functii sun inglobate in acelasi echipament. Echipamentele de identificare – cititoarele - preiau informatia de la un dispozitiv (cartela, tag, keyfob, PIN code, caracteristica biometrica etc.) si o transfera la unitatea de control care va decide daca acea persoana este autorizata sau nu.

CAPITOLUL 3

PRINCIPII DE IDENTIFICARE. METODE DE IDENTIFICARE

Una din principalele probleme ale unui sistem de control acces consta in definirea identitatii si recunoastrea acesteia (autentificare/verificare) pentru luarea deciziilor. Exista diverse metode si tehnici de identificare. In control acces ne bazam pe trei tipuri de identificare :

- Cunostinta : Ce stii? Se bazeaza pe o informatie stiuta de persoana care cere autentificare. (PIN codul folosit la o tastatura de acces)
- Posesia : Ce ai? Se bazeaza pe prezentarea unui card/tag la un cititor
- Caracteristici fizice personale: Cine esti?Se bazeaza pe caracteristicile biometrice ale unei persoane.

Fiecare dintre metode are avantaje si dezavantaje. Cand se cere realizarea unei aplicatii de inalta securitate se folosesc combinatii de metode identificare. Fiecare dintre factorii de identificare trebuie autentificat pentru ca persoana sa fie autorizata. Tehnologiile de identificare mai pot fi clasificate in tehnologii bazate pe contact – tehnologii care presupun un contact fizic intre cartela si cititor, si tehnologii contactless (fara contact) – in care nu exista vre-un contact intre cititor si cartela.

Tehnologii de identificare uzuale

Sisteme bazate pe cunoastere

Sistemele bazate pe cunostinte sau sisteme de identificare pe baza unui cod (PIN-Personal Identification Number) sunt foarte raspandite mai ales pentru aplicatii de mici dimensiuni sau de securitate scazuta.

Codul PIN poate fi folosit impreuna cu alte tehnici de identificare dar este folosit ca si metoda independenta de acces. Aceasta tehnologie se bazeaza pe utilizator pentru introducerea corecta a informatie in sistem (PIN-ul) dar prezinta si dezavantajul de a putea fi « spionat« de catre persoane neautorizate. Sistemele de acces cu cod PIN sunt usor de instalat si programat, uzual exista un cod master ce permite gestionarea parametrilor gen: timp de deschidere, adaugare/stergere/modificare utilizatori/coduri. Codul PIN poate fi de dimensiuni de la 4 pana la 10 digiti. Cu cat codul este format din mai multi digiti cu atat scade probabilitatea de a « ghici« codul prin incercari succesive.

De exemplul pentru un cod PIN format din 4 digiti la o tastatura cu 10 cifre exista posibilitatea de a seta 10.000 de coduri, iar pentru un sistem bazat pe 5 digiti pot fi introduse 100.00 de coduri PIN.

Sisteme bazate pe posesia unui card

Aceste sisteme se bazeaza pe prezentarea unui card, tag, breloc (keyfob) – se mai numesc si ID credential - unui cititor. In aceasta categorie de sisteme sunt folosite tehnologii cu grade diferite de securitate si operabilitate, Aceste carduri sunt codate folosind echipamente speciale si au un grad de rezistenta mediue/mare privind modalitate de transfer/copiere a informatiei stocate.

Bar code – Tehnologia codurilor de bare este foarte folosita in sisteme adiacente sistemelor de control acces (sisteme de gestiune, vanzari, identificare automata a produselor). Pentru sistemele de control acces aceasta tehnologie este de o securitate foarta scazuta. Codul de bare este format dintr-o serie de linii paralele de dimensiuni variabile, astfel incat formeaza o succesiune de intervale luminoase/ intunecate care, atunci cand sunt citit de de un scanner sau bar code reader, sunt transformate in succesiuni de 1 si 0, informatia fiind trimisa la sistemul de control. Practic informatia este vizibila desi este intr-o forma neuzuala. Acest lucru duce la o replicare destul de usoara. Bar codurile pot

fi imprimate direct pe diverse materiale si pot fi cititte destul de usor cu un software dedicat sau cu scannere de coduri de bare de raspndire larga. Din cauza nivelului scazut de securitate aceasta tehnologie este rar folosita in sistemele de control acces, doar pentru acces tempor, de scurta durata, in arii putin protejate.
Exista o tehnica de codare care permite codurilor de bare sa fie invizibile ochiului uman. Este vorba de asa numitele carduri infra red, in care codul de bare este citit doar folosind lumina infra-red. Sunt de o securitate mai mare decat cea anterioara si sunt folosite in aplicatii speciale.

Banda magnetica – magnetic stripe sau magstripe - este una din cele mai utilizate tehnologii, in special pentru cardurile bancare dar nu numai. Acest tip de card este ieftin, usor de produs si codat si poate contine date de tip alfanumeric. Inca exista o gama de aplicatii de control in care acest tip de tehnologie este larg folosita.
Cardurile magnetice sunt compuse dintr-un card de PVC pe care se suprapune o banda de plastic ce contine mici particule metalice cu proprietati magnetice. Codarea binara (1 si 0) se produce prin magnetizarea acestor particule. Pentru a putea fi citita aceasta banda magnetica trebuie sa fie trecuta printr-un cititor de carduri astfel incat exista un contact intre banda si capul de citire, modificarile campului magnetic al cititorului sunt transformate apoi in semnale electrice si transmise la unitatea de control acces folosind un protocol de tip Clock & Data sau Wiegand.
Capacitatea de a rezista in timp actiunilor unor campuri magnetice este exprimata prin coercivitate. Aceasta exprima forta campului magnetic necesar pentru stergerea informatiei de pe card. Exista doua mari categorii de carduri magnetice, cele cu coercivitate mare, pentru care este necesara o forta de 4000 Oe (Oersted) sau cele de joasa coercivitate (300 Oe). Toate cardurile bancare sunt de mare coercivitate.
Pentru stocarea informatiei pe banda exista 3 track-uri. Track-ul 1 (sau Track1/IATA) a fost folosita pentru Industria Aeronautica, Track 2 (ABA - Asociatia Bancara Americana) este folosita de industria bancara iar Track 3 este nestandardizata si nu este folosita decat pentru aplicatii speciale. Informatia stocata pe aceste track-uri si modul cum este stocata este referita ca formatul tack-ului. Track-ul 1 este singurul care poate contine informatie alfanumerica (este folosita de banci pentru stocarea numelui proprietarului cardului).
Deaorece este una din cele mai raspandite tehnologii de carduri, aceasta este foarte strict standardizata. ISO are mai multe standarde care se refera la aceata tehnologie ISO-7810, ISO-7811, ISO-7812, ISO-7813. Acestea definesc proprietatile fizice ale cardului (incluzand dimensiunea cardului, pozitionarea, dimensiunile si caracteristicile magnetice ale benzii) dar si carcteristicile logice (track-ul folosit, formatul, alocarea numerotarii emitatorilor de carduri etc).
Pentru cardurile magnetice exista doua mari tipuri de cititoare : cele cu trecere (swipe reader) prin care cardul este trecut de catre utilizator si cele cu insertie (insertion reader), in care cardul este introdus de catre utilizator si apoi preluat de un mecanism care-l trece cu viteza constanta peste capul de citire. Un dezavantaj al acestei tehnologii este dat de necesitatea contactului fizic intre card si cititor. Pentru aplicatiile de control acces aceasta tehologie este una de securitate medie, datele de pe card putand fi citite relativ usor. Acest tip de tehnologie poate fi folosit in aplicatii care impun folosirea unor carduri magnetice pentru mai multe aplicatii, nu doar pentru control acces.

Cardul Wiegand – este bazat pe efectul Wiegand. Acest efect este generat intr-un un tip special de conductor feromagnetic de diametru redus. Acest conductor este un aliaj de otel, cobalt si vanadiu prelucrat prin procese speciale care il fac sa aiba un « miez » - core- si o membrana cu proprietati magnetice diferite. La aplicarea unui camp magnetic in acest tip de conductor se induce un puls Wiegand, ce actioneaza ca un generator de semnal pentru cititorul de carduri. Intr-o cartela Wiegand sunt folosite doua conductoare wiegand, unul pentru 1 si celelalt pentru 0, aranjate astfel incat la o trecere print cititor sa se produca codul cu care cartela a fost codata. Cititorul wiegand are doua componente de baza : generatorul de camp magnetic si capul de citire al pulsurilor Wiegand generate de cele doua conductoare (1 si 0)..

Avantajele acestei tehnologii sunt :

- acest tip de card nu poate fi contrafacut deoarece tehnologia de producere a conductorilor Wiegand este patentata, iar sursele de conductori strict controlate.
- durabilitate foarte mare
- este o tehnologie bazata pe un camp magnetic mai puternic decat cel necesar benzii magnetice
- este imuna la interferente radio sau electromagnetice.

Acest tip de card nu poate fi re-scris, informatia fiind codata la momentul fabricarii acestuia. In momentul actual acest tip de card a fost inlocuit de noile tehnologii de proximitate.

Tehnologii fara contact. Proximitate

Tehnologia fara contact este cea mai folosita tehnologie de identificare pentru sistemele de control acces, in acest moment. Aceasta tehnologie presupune absenta contactului fizic dintre cartela si cititor, cartela trebuie doar apropiata de cititor pentru a se face transferul de informatie. Acest tip de tehnologie se mai numeste si RFID (Radio Frequency Identification), deoarece se bazeaza pe transmisia radio. Cititorul este de fapt un transmitator de unde radio (RF), in jurul acestui existand un camp radio de forma elipsoidala, ce se exitnde atat in fata cititorului cat si in spatele lui. Un cititor este compus dintr-un circuit numit antena si o unitate electronica de control care are rolul de converti semnalele primite de la cartela prin intermediul antenei si a face conversia de la RF la protocolul de comunicatie specific (Wiegand, RS-232, RS-485 etc.). Un parametru important al acestor cititoare este cel numit *raza de citire* (read range). Aceasta este definita ca fiind distanta maxima la care acel cititor face o citire corecta a unui card. Acest parametru nu are o valoare fixa. Campul radio al cititorului (read range) este influentat de mai multi parametri : dimensiunea cititorului (a antenei), numarul de spire ale antenei, tensiunea de alimentare si conditiile de instalare. Orice obiect metalic aflat in preajma cititorului va avea ca efect reducerea acestei raze de citire. O cartela de proximtate este formata dintr-un material plastic in care se incapsuleaza un chip (trasnponder) conectat la o antena. Cand aceasta antena intra in campul RF al cititorului in antena se induce un curent ce este folosit pentru alimentarea chip-ului care va transmite codul programat, ca semnal modulat.

Sunt doua tipuri de carduri/taguri folosite in aceasta tehnologie :
- cele pasive – care se folosesc doar de energia furnizata de cititor, nu au nici-o sursa suplimentara de alimentare
- cele active – care au, in plus, o sursa auxiliara, o baterie, ce asigura sursa de energie pentru circuitul tag-ului.

Cardurile pasive sunt de dimensiuni mai mici, mai usoare si au un ciclu de viata extrem de mare. Cardurile active necesita inlocuirea bateriei periodic dar pot fi citite de la o distanta mai mare. Sunt folosite in special pentru aplicatiile de identificare auto.

Din punctul de vedere al frecventei de lucru sistemele de proximitate sunt clasificate in :

- joasa frecventa : 100-500 kHz, dar uzual 125 kHz. Aceste sisteme sunt cele mai raspandite in acest moment, asigurand o viteza de citire mare si o raza de citire intre 5 cm si 2 m (folosind tag-uri active), in functie de tipul de cititor
- medie frecventa : 10-15MHz dar uzual 13.56MHz. Sistemele care folosesc aceasta gama de frecventa sunt cele pentru smart-card fara contact, avand o viteza mare de citire dar o raza de citire mai mica decat cea pe 125kHz.
- inalta frecventa : 2.4-5GHz. Asigura o distanta mare de citire impreuna cu tag-urile active si au o viteza de citire foarte mare.

Tehnologia de 125kHz, numita si de proximitate, nu se bazeaza pe un standard international ci pe unul de-facto, numit Wiegand. dupa numele lui John Wiegand, cel care a inventat tehnologia. Tehnologia contactless de medie frecventa 13.56Mhz este una folosita din ce in ce mai des in conjunctie cu smart-card-urile tip contactless.

Smart Card

Daca pentru tehnologia de 125kHz, nu exista standarde intrenationale impuse producatorilor, acestia producand sisteme proprietare ce nu sunt compatibile unele cu altele pentru smart card-uri exista standarde ISO care impun producatorilor caracteristici ce le fac cea mai buna alegere pentru o tehnologie contactless.
Smart card-ul este un tip de card « inteligent » ce poate fi folosit intr-o arie foarte larga de aplicatii, nu doar control acces electronic.
Exista două tipuri mari de smart card-uri : cele cu contact fizic intre cartela si cititor si cel fara contact. Cele cu contact nu sunt o optiune pentru control acces electronic din cauza timpului mare de procesare. Pentru control acces se folosesc smart-card-urile bazate pe tehnologia RF 13.56 MHz.

Din punct de vedere constructiv smart card-urile se impart in :

- carduri cu memorie (memory card)
- carduri cu logica cablata (wired logic)
- carduri inteligente bazate pe un microcontoller (MCU)

Cardurile cu memorie au in componenta lor un circuit in care sunt stocate informatiile de autentificare prin care se face accesul la zona de memorie protejata in care se afla un unic numar de identificare. Unele dintre ele folosesc diverse metode de criptare a informatiei.
Cardurile cu logica cablata folosesc un circuit electronic special pentru autentificarea dintre card si cititor. Acestea nu pot fi rescrise/reprogramate dupa producere.
Cardurile MCU sunt cele mai « inteligente« avand posibilitatea de a folosi diverse metode sofisticate de autentificare si criptare chiar pe card insusi si au o interactiune inteligenta cu cititorul. Ele au o capacitae de memorie destul de mare si ruleaza asa numte sisteme de operare de card tip MULTOS sau JavaCard.
Acest tip de card permite utilzarea zonelor de memorie pentru mai multe aplicatii, accesul la fiecare zona de memorie facandu-se prin intremediul unei chei de acces (publica sau privata). In plus, intre card si cititor are loc un proces de autentificare mutuala. Comunicatia dintre card si cititor se face criptat folosind alogoritmi avansati gen DES/3DES/RSA etc. Capacitatea de scriere/citire acestor carduri permite stocarea de informatii gen template biometric sau cod PIN si elimina necesitatea interogarii unei baze de date comune. Deasemenea aceste carduri constituie suport pentru tehnologii hibride : contact smart card, proximitate, biometrie, banda magnetica, printare logo, holograme etc.
Fiecare astfel de card are un umar unic de identificare numit CSN- Card Serial Number- alocat la momentul producerii. Folosirea acestuia in scopul de a controla accesul nu este recomandata deoarece acesta nu este criptat si poate fi citit cu orice cititor compatibil.

Avantajele tehnologilor fara contact sunt :
- este foarte usor de folosit, nu necesita o orientare anume a cardului si nici introducerea lui in vre-un cititor.
- viteza mare de transfer a datelor si de acces
- asigura o protectie mare a datelor codate in card
- durabilitate a cardurilor si cititoarelor
- nu pot fi falsificate usor
- se pot integra cu diferite alte tehnologii
- mentenata usoara pentru cititoare impreuna cu protectie anti-vandalism

Sisteme de identificare personala.Tehnologii de identificare biometrice

Tehnologiile biometrice, sau de verificare a caracteristicilor biologice, desi relativ mai scumpe, sunt utilizate atunci cand exista nevoia de a asigura cel mai inalt nivel de securitate. Ele au fost create pentru a depasi problemele cauzate de pierderea, furtul card-urilor/tag-urilor sau aflarea codului PIN de catre persoane neautorizate. Aceste sisteme permit inrolarea caractersticilor biometrice sub forma unor fisiere de date (template-uri) care apoi sunt folosite in procesul de autentificare. Aceaste tehnologii se bazeaza pe unicitatea caracteristicilor biologice ale fiecarui individ. Avantajul major este ca nu mai sunt necesare alte tipuri de verificari pentru autentificarea persoanei. Dezavantajul consta in costurile relativ mari si timpul de verifcare mai mare decat al altor tipuri de tehnologii. Sunt cateva procese particulare acestor tehnnologii :
Inrolarea – este procesul de preluare/citire a caracteristicii biologice si transformarea ei, prin algoritmi matematici, intr-un asa numit template – date binare care pot fi prelucrate si folosite de sistemele de calcul.

Verificarea - consta in compararea caracteristicilor citite la momentul cererii de acces cu cele citite la momentul inrolarii.
In acest loc se tine cont de doua criterii numite : False accept si False reject. False reject se refera la posibilitatea de rejectare/refuzare a accesului pentru o persoana autorizata, acesta ar trebuii sa fie cat mai mic. False accept - se refera la posibilitatea de acceptare a cererii de acces pentru o persoana neautorizata.

Cele mai utilizate tehnici de identificare biometrica sunt :
- fingerprint recognition/ recunoastrea amprentei
- hand geometry recognition/ geometria mainii
- iris recognition/ rcunoastrea irsiului
- face recognition/ recuoastrea fetei
- voice recognition/ recunoastere vocal

Cel mai adesea aceste tehnici de identificare sunt folosite in combinatie cu alte tehnici :
cod PIN, card de proxmitate, smart card. Aceste informatii suplimentare (cod PIN, numar de card) sunt folosite pentru gasirea template-ului in baza de date a unitatii/cititorului si actioneaza ca un index. In momentul in care locatia a fost gasita (de exemplu : codul PIN este valid) atunci se citeste din acea locatie valoarea template-ului si se compara cu cea citita in momentul verificarii. O alta abordare consta in citirea caracteristicii biometrice si cautarea liniara in baza de date dupa un template identic. Acest procedeu dureaza insa mai mult. Aceste doua tehnici se bazeaza pe existenta unei baze de date comune in care sunt stocate template-urile. O alta metoda utilizata este de a avea template-urile distribuite pe smart-card-ul utilizatorului. Comparatia se face intre template-ul citit de la cititor (in timpul procesului de autentificare) cu cel obtinut in urma citirii template-ului de pe smart card.
Trebuie mentionat ca aceste sisteme se pot folosii in situatii in care se cere o mare securitate a zonei si un control ridicat, dar in acelasi timp, procesul este destul de lent comparativ cu celelalte tehnologii.

Formatul cardurilor si protocoale de comunicatie

Formatul unui sistem (card, controller) este un element foarte important intr-un sistem de control acces. Formatul specifica modul de interpretare a datelor transmise de la cartela la cititor si de la cititor la controller. Formatul specifica din cati biti este format stream-ul de date si ce semnificatie au acestia. Formatul nu este numarul insusi !. Fiecare producator de sisteme de control acces isi poate creea propriul tip de format astfel incat sa asigure o cat mai mare securitate a datelor. Numarul de biti nu indica formatul -cu exceptia formatului de 26 de biti- de exemplu sunt peste 100 de formate de 34 de biti.

Formatul unui card este independent de tehnologia folosita (125kHz sau 13.56MHz).
Formatul unui card exprima urmatoarele caracteristici :

- numarul total de biti codati in cardul respectiv

- numarul de biti pentru Site Code sau Facility Code (Site Code-ul este un numar specific unui singur client/sistem, numar ce este comun tuturor cardurilor dintr-o locatie) precum si locatia acestora. Acest camp este testat intotdeauna primul de sistemul de control acces. Este acest card emis pentru locatia respectiva ? Daca da se trece mai departe la verificarea card number-ului, iar daca nu acel card este rejectat. Nu toate formatele folosesc conceptul de Site Cod. Acest camp adauga o masura de securitate in plus pentru sistem, deoarece este posibil ca numarul cardului sa fie aflat (de multe ori acesta este printat chiar pe card), dar Site Code-ul este stiut doar de instalator sau administratorul sistemului.

- numarul de biti pe care este reprezentat card number-ul, numarul unic de identificare al cartelei, si locatia acestora. Acest numar este folosit pentru verificarea drepturilor de acces in unitatea de control acces.

- biti de paritate si locatia lor, biti care sunt folositi pentru verificare corectitudinii transmisiei de la card la cititor si de la cititor la unitatea de control acces.

Pe langa aceste campuri, orice producator de sisteme de control acces poate sa-si defineasca alte campuri dupa care sa faca verificarile necesare, format ce trebuie respectat de toate cardurile din sistem.
Formatul Standard 26 de biti Wiegand

Este standardul de–facto al industriei de control acces, ce isi area originea in tehnologia cardurilor Wiegand. Toate unitatile de control acces permit utilizarea acestui tip de format. Descrierea acestui format este urmatoarea :

- Numar de biti – 26
- Biti de paritate -2, Even Parity –bitul 1 calculat pe primi 13 biti si Odd Parity-bitul 26, calculat pe ultimii 13 biti
- Site Code – lungime 8 biti, incep la bitul 2 si se termina la bitul 9
- Card Number- lungime 16 biti, incepe la bitul 10 si se termina la bitul 25

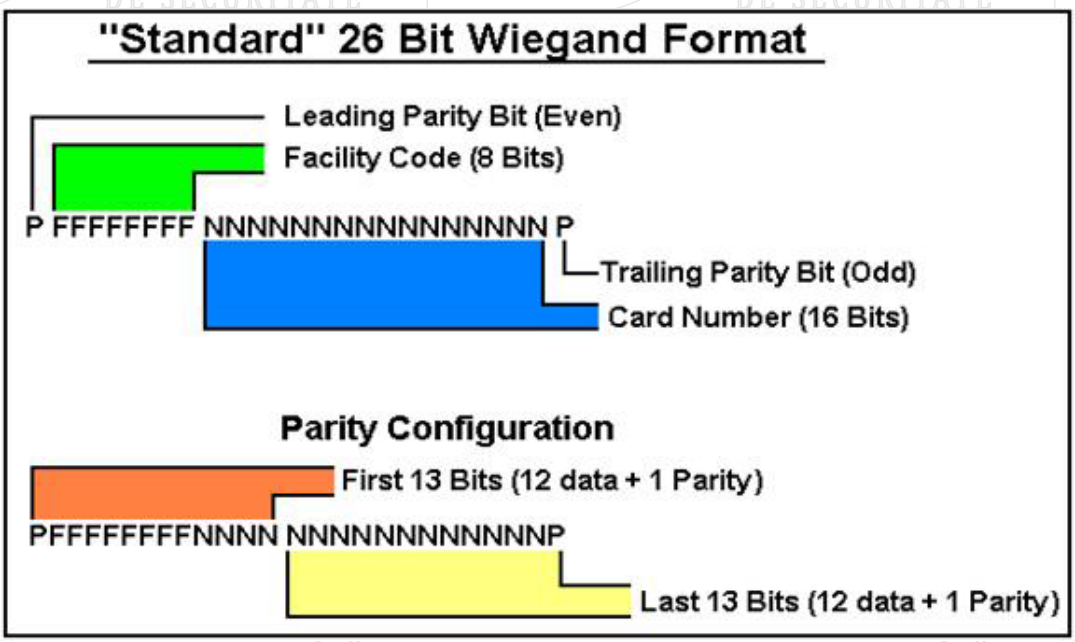


Figura. Descrierea formatului de 26 de biti Wiegand

Conform cu descrierea facuta un card ce are acest format poate sa aiba :
Facility Code (Site Code) : 1-255 si Card Number : 1-65535
Celelate formate au, conceptual, aceleasi fundamente ca formatul de 26 de biti. De exemplu se poate alege pentru un format de 34 de biti in care interpretarea bitilor sa fie urmatoarea :

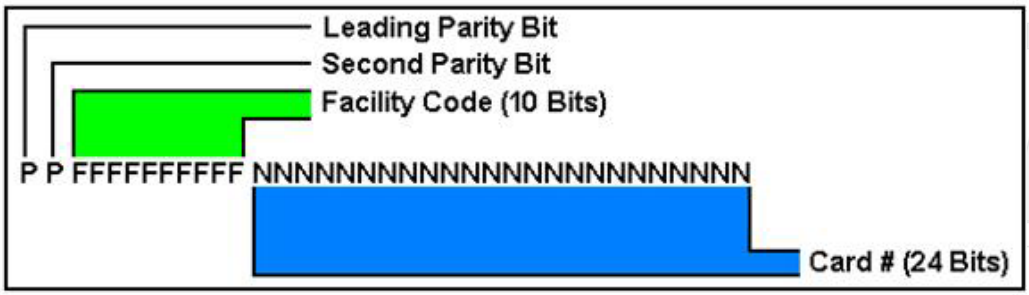


Figura. Format de 34 de biti

Interfete de comunicatie cititor-controller

O interfata de comunicatie specifica modul de comunicare intre doua echipamente, in cazul acest cititor si unitatea de control acces.
Cel mai raspandite interfete de comunicatie sunt :

- Wiegand
- Clock-and-Data
- RS-232, RS-485, RS-422
- 20mA bucla de curent
- TCP/IP

Cea mai utilizat interfata in sistemele de control acces este cea Wiegand. Este o interfata de comunicatie uni-directionala, de la cititor la unitatea de control acces. Interfata electrica consta in trei semnale numite DATA 0 (Verde), DATA 1 (Alb) si GND sau DATA RETURN (Negru) folositi pentru transmiterea valorilor binare 1 si respectiv 0. In mod normal DATA 0 si DATA 1 stau in valoarea high (+5V) iar cand se transmite o valoare de 1 sau de 0 linia respectiva “cade” pe 0V (GND sau DATA RETURN). In felul acesta se transmit secventele de date de la cititor la unitate. Majoritatea unitatilor de control acces si a cititoarelor au acest tip de interfata. Un avantaj major al acestui tip de interfata este distanta mare de transmisie, aproximativ 150 m.

O alta interfata des folosita este cea numita Clock-and-Data. Aceasta a fost utilizata de cititoarele magnetice care citeau Track-ul 2 al benzi magnetice, mai este denumita si MagneticStripe Track/2 sau ABA format. Aceasta interfata consista din 3 semnale numite: Card Present, Clock si Data. Semnalul “Card Present” ramane la valorea High (+5V) atat timp cat nu se transmite nimic, cand se incepe transmisia datelor “Card Present” « cade« in 0V si ramane acolo pana la incheierea transmisiei cand revine la +5V. Semnalul “Clock” sincronizeaza cititorul cu unitatea pentru a asigura un transfer sigur iar semnalul “Data” transmite datele (valoarea 0V inseamna bitul 1 iar valoarea +5V insemna bitul 0).

Protocoalele seriale sunt, deasmenea, folositoare pentru transmisia bidirectionala si sunt, in general folosite cu cititoare biometrice sau cititoare de smart card-uri, unde se impune un transfer bi-directional de date. Totusi exista unele aplicatii in care cititorul trebuie sa furnizeze card number-ul altor tipuri de echipamente decat unitatile de acces si atunci se impune folosirea unui cititor cu iesire seriala. Acest tip de protocol mai este folosit si in cazul cititoarelor care se conecteaza direct pe bus-ul sistemului, nu la o unitate de acces, cititoarele actionand ca unitati de tip slave, in care masterul este o unitate de acces sau un calculator.

Interfata TCP/IP este cel mai nou mod de interfatare al cititoarelor care, in acest caz, incorporeaza functii specifice unitatii de control acces.

Cititoare de control acces

Pe parcursul precedentelor paragrafe s-a vorbit despre diversitatea tehnicilor de identificare si a diverselor caracteristici implicate in transferul informatiei de la utilizator/card la sistemul de acces. Gama de cititoare este exterm de vasta, acestea se diferentiaza in functie de :

- tipul de tehnologie : simpla tehnologie, dubla tehnologie, tripla tehnologie. Cititoarele multi tehnologie sunt folosite de multe ori pentru a asigura o tranzitie de la un tip la altul de tehnologie. De exemplu, exista cititoare care citesc carduri de proximitate dar si smart card-uri, in plus pot avea si tastaura sau senzor de fingerprint.
- raza de citire
- caracteristici de comunicatie : simplu protocol, dual protocol,
- caracteristici de procesare : doar functie de cititor sau functii multiple
- mediu de instalare : interior, exterior

CAPITOLUL 4

UNITATI DE CONTROL ACCES. SISTEME DE CONTROL ACCES

In practica exista o varietate foarte mare de unitati de control acces si sisteme. Practic unitatea de control acces are cateva functii bine defintie :

- La unitatea de control acces/controller se conecteaza toate echipamentele unui sistem de control acces: contactul magnetic, incuietoarea electromagnetica, cititoarele, calculatorul de control, intrari/iesiri de alarma etc.
- Are rolul de a monitoriza aceste echipamente si a memora schimbarile de stare
- Primeste de la cititoare informatiile de identificare si decide daca acorda permisiunea de acces sau nu, bazandu-se pe baza de date stocata in memoria locala sau in cea de la nivel superior
- Comunica informatiile la nivelul superior cand este interogata sau cand trebuie sa raporteze diferite evenimente

Unitatile de control acces sunt echipamente electronice dedicate, care au in dotare diverse interfete pentru comunicatia cu echipamentele periferice si cu cele de nivel superior. Practic acestea sunt unitati sunt doatate cu circuite integrate ce cuprind:

- unitate de procesare: microprocesor de tip industrial sau unitate de comanda
- interfete de comunicatie seriale (RS-232, RS-485, 20mA,) sau de retea TCP/IP
- interfete de cititoare : Wiegand, ClockData, 20mA, RS-485
- interfete pentru intrari/iesiri (open colector sau pe releu)
- memorie locala tip flash, RAM, EPROM
- circuite specializate de protectie
- sursa de alimentare etc.

Evident numarul si combinatiile de tipuri de echipamente intalnite difera de la producator la producator. Fiecare producator avand un anumit specific. Din caracteristicile acestor unitati mentionam:

1. Numarul de porturi de cititoare/numarul de usi ce pot fi controlate de acea unitate,
2. Tipul de cititoare ce pot fi conectate, tehnologiile ce pot fi folosite (wiegand, proximitate, smart-card, biometrie, cititoare seriale etc)
3. Capacitate de memorare exprimata prin : numarul de cardholderi (utilizatori de cartele), numarul de evenimente stocate in regim off-line (cand nu transmite evenimentele unui software de gestiune)

4. Numarul de intrari/iesiri auxiliare
5. Numarul si tipul porturilor de comunicatie : seriale sau TCP/IP
6. Capacitatea de control a altor echipamente
7. Modalitatea de diagnosticare a functionarii normale si/sau de defect
8. Modalitatea de alimentare

Sistemele de control acces pot fi clasificate in:
Sisteme stand-alone ce cuprind:

- tastaturi de acces
- cititoare/controllere stand-alone

Sisteme in retea sau sisteme distribuite ce cuprind:

- sisteme single-site: sisteme mici, medii, mari
- sisteme multi-site: sisteme mici/medii distribuite pe arii largi
- sisteme integrate: sistem single-site complexe – integrate cu efractie, CCTV, incendiu, SMS sau BMS

Pentru fiecare dintre aceste tipuri exista o varietate de modele ce realizeaza functii dintre cele mai diverse.

Sistemele stand-alone sunt sisteme relativ simple ce au in vedere securizarea accesului pentru un numar mic de usi. Caracteristica esentiala a acestor sisteme este ca functioneaza independent de un sistem software, fara monitorizare din partea unui operator. Programarea acestor sisteme se face dintr-o tastatura existenta din care se seteaza functiile de baza gen: introducere/stergere carduri, modificare timp de deschidere usa, activare releu de alarma etc. Acest tip de echipament este unul care nu poate comunica cu alte tipuri de echipamente similare, nu pot face parte dintr-o retea de astfel de echipamente. Interfetele acestui tip de echipament permit conectarea elementelor de la o singura usa:

- 1, 2 cititoare, daca nu sunt deja incorporate
- o intrare pentru un buton de iesire
- o iesire pe releu pentru o yala electromagnetica
- un contact magnetic
- o intrare de alarma si 1 iesire pe releu de alarma/sirena

Principalele caracteristici ale acestui tip de sisteme includ : numarul de useri (purtatori de cartela) si capacitatea de stocare (numarul de evenimente stocate).

Sistemele in retea sau distribuite sunt sisteme in care unitatile de acces componente au functii mai complexe fata de cele tip stand-alone. Acestea comunica intre ele printr-o magistrala de comunicatie si sunt de cele mai multe ori conectate la un calculator central pe care ruleaza un software de gestiune. Unitatile componente ale unui sistem distribuit au functii diverse, ce depinde de complexitatea sistemului dorit.
Intr-un sistem distribuit exista intotdeauna un MASTER iar restul echipamentelor sunt SLAVE (unitati locale). Master-ul are rolul de a initia comunicatia cu unitatile slave si de a le interoga iar unitatile slave raspund. Pentru anumite sisteme MASTER este chiar PC-ul pe care ruleaza software-ul de gestiune, pentru alte sisteme MASTER este o unitate dedicata, la aceasta unitate nu se conecteaza cititoare sau alte tipuri de intrari/iesiri

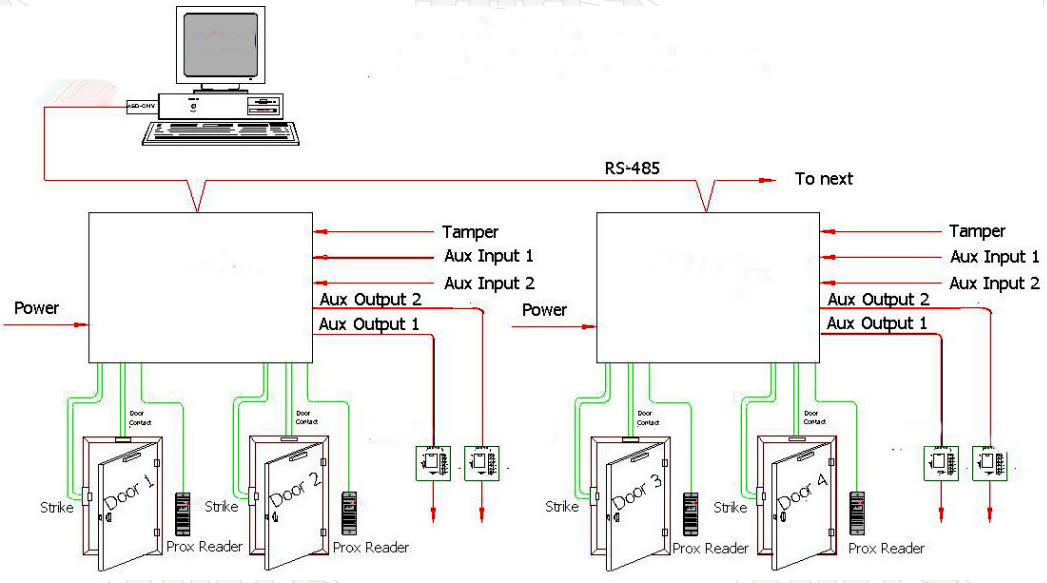


Figura. Arhitectura distribuita cu PC-Master

Tipuri de unitati de control acces :

- unitate de control acces tip Master : acest tip de unitate nu permite conectarea unor cititoare sau a altor tipuri de echipamente de intrari/iesire. Functiile acestui tip de unitate include : comunicatia cu software-ul de management si cu unitatile slave (interfetele de cititoare). Acest tip de unitate pastreaza toata baza de date cu utilizatori si drepturile de acces. Deciziile de acordare a accesului se iau la acest nivel.
- Interfete de cititoare : acest tip de unitate are rolul de a conecta echipamentele de camp si de a trimite cererile de acces la unitatea master. Exista si unitati care pot sa ia decizia local, deoarece au o copie a bazei de date in memoria proprie. In cazul in care conexiunea cu unitatea master este intrerupta aceste interfete de cititoare pot lua decizia de acordare a accesului pe baza Site Code-ului card-ului.
- Unitate de control acces slave (unitati locale) : este cel mai uzual tip de unitate de control acces, folosita in sisteme unde toate unitatile sunt controlate de software-ul de management. Aceasta unitate permite conectarea cititoarelor pentru un numar de 1,2 sau 4 usi simple sau duble (o usa dubla este cea cu un cititor pe intrare si unul pe iesire), intrari auxiliare si iesiri auxilizare. In plus fiecare unitate slave contine o copie a bazei de date care-i permite sa ia toate deciziile de acces. Uneori la aceasta unitate se pot conecta alte interfete de cititoare pentru care unitatea Slave devine unitate Master, astfel incat se extinde numarul de cititoare controlate.
- Interfete de intrari/iesiri : sunt unitati speciale care permit conectarea unui numar de intrari/ iesiri ce sunt folosite pentru diverse functii (interfatare sisteme de alarma, sisteme integrate, BMS, CCTV, incendiu).
- Unitati de control acces lifturi : acest unitati sunt destinate controlului lifturilor. Sunt unitati cu un numar mare de intrari/iesiri si cu 1, 2 sau 4 porturi de cititoare, care sunt montate in interiorul cabinei. Exista doua tipuri de unitati : standard sau de inalta securitate. Cele standard permit doar activarea butoanelor de acces pentru etajele din nivelul de acces al utilizatorului dar nu si monitorizarea butonului care a fost activat, astfel incat nu se stie la ce etaj s-a oprit liftul. Aceasta functie este posibila la unitatile de inalta securitate care monitorizeaza si starea butonului.
- Terminale de pontaj si acces: sunt unitati dedicate pentru functia de pontaj dar pot executa si functii specifice unui sistem de control acces. Uzual terminalele de control acces au o interfata utilizator formata din: tastatura, cititor de carduri, display LCD, butoane functionale ce pot fi programate pentru diverse evenimente de pontaj si/sau prezenta. Acest tip de echipament are o memorie suficient de mare pentru pastrarea evenimentelor de acces si pontaj si pot functiona atat off-line cat si on-line.

Metode de comunicatie

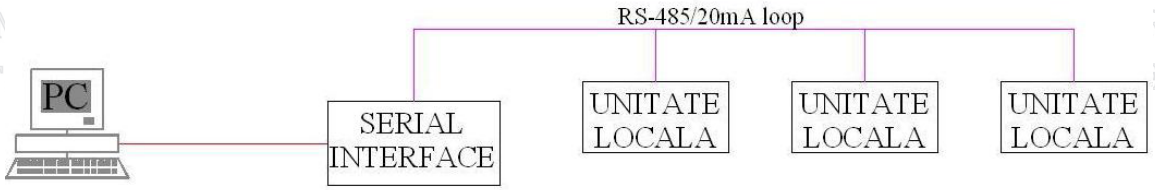
Intr-un sistem de control acces exista mai multe metode de a transfera datele intre diversele echipamente. Intre cititoare si controllere am detaliat mai sus. Pentru comunicatia dintre unitatile de control acces se folosesc metode de comunicatie seriala pentru distante mari. Cele mai des folosite protocoale de comunicatie sunt : RS-485 sau RS-422. Acest protocoale sunt protocoale de nivel electric, diferentiale, mulit-punct, transmisia facandu-se pe perechi torsadate. Distantele de transmisie tipice ajung la 1200m. Totusi aceaste distante pot fi marite folosind echipamente de tip repetor/amplificator. In ultimul timp multi producatori asigura conevertoare de fibra optica astfel incat distantele se pot marii pana la cativa kilometri.

Pentru comunicatia dintre calculatorul de gestiune al sistemului si sistemul de control acces se foloseste uzual protocolul RS-232. Acesta este un protocol serial de distanta mica, ce permite comunicatia doar intre doua echipamente conectate la mediul de transmisie (punct la punct). Dezavantajul acesteia este viteza mica de transmisie si distanta mica dintre echipamente si calculatorul de gestiune. Pentru depasirea acestor dezavantaje se folosesc convertoare seriale RS-232/RS-485 care permit marirea pana la 1200 m a distantei dintre calculator si controller.

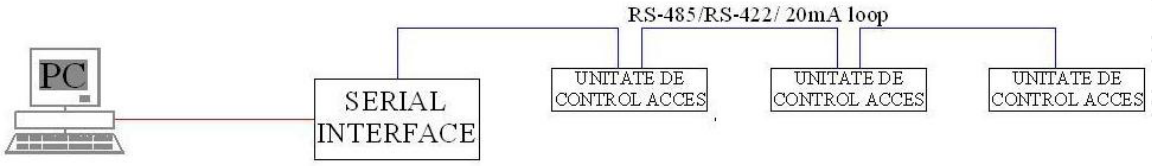
Comunicatie in retea folosind protocolul TCP/IP este din ce in ce mai folosita pentru o gama de aplicatii de tip multi-site sau pentru sisteme single-site mai complexe. Unitatea de control acces este dotata cu o interfata de retea (de obicei un serial server) care permite conectarea oriunde in retea si conectarea la unitate din orice punct al retelei. Avantajele acestei metode de trasnmisie constau in : viteza mare de transmisie, usurinta de conectare, distante mari de acoperit folosind protocoale de nivel retea, conectarea de la distanta pentru monitorizare si programare, posibilitatea de interconectare a sistemelor distribuite pe arii mari folosind retele tip LAN sau WAN, dar care logic apartin aceluiasi sistem. In ultimul timp tendinta de trecere la protocoale de comunicatie TCP/IP s-a facut simtita nu doar la nivelul unitatilor de control acces ci si la nivelul cititoarelor si al unitatilor de intrari/iesiri. Exista sisteme in care toata comuicatia dintre elementele componente este realizata prin protocolul TCP/IP. Toate elementele din sistem: cititoare, unitati de intrare/iesire (pentru contacte magnetice, butoane de iesire, comenzi etc) au o placa de retea. Topologia unui astfel de sistem este cea a unei retele LAN, in care toate elementele sistemului sunt egale din punct de vedere al comunicatiei.

Cele mai raspandite topologii de comunicatie sunt :

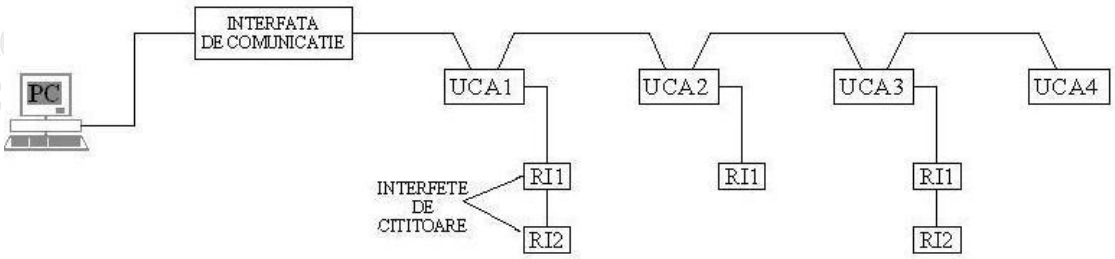
- topologia bus de tip daisy-chain



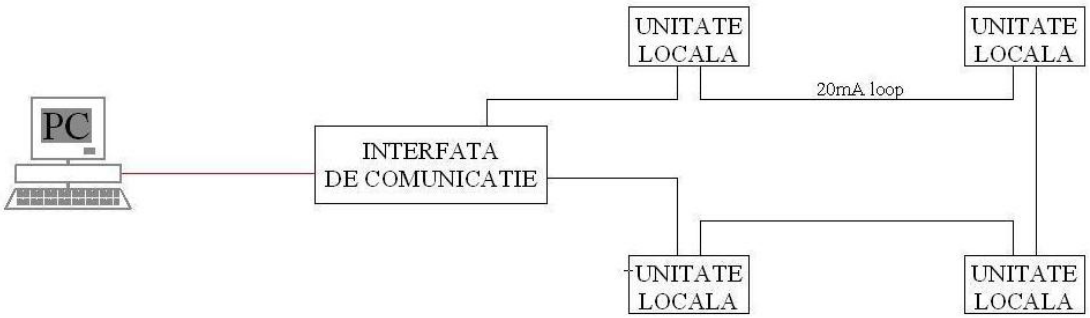
- topologia bus de tip multi-drop



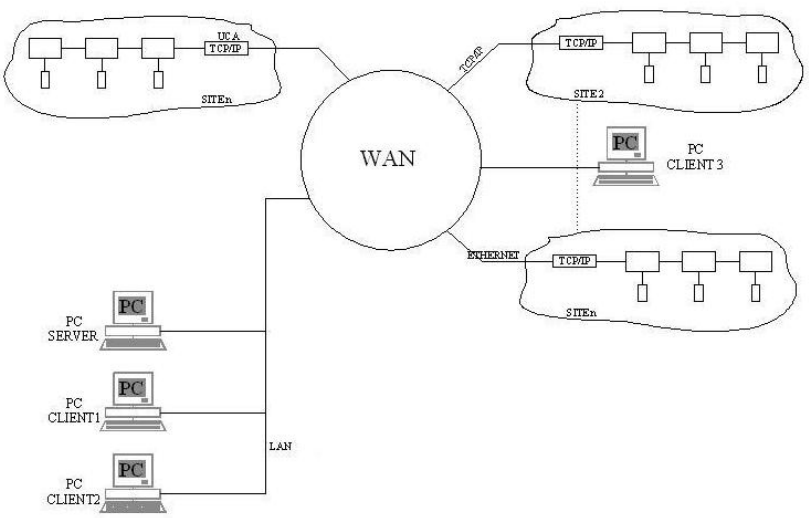
- topologie mixta



- topologia bucla



- topologie de retea tip multi-site



CAPITOLUL 5

SOFTWARE DE CONTROL ACCES

Pentru gestionarea intregului ansamblu de echipamente mecanice, electrice si electronice (hardware si firmware) ce compun un sistem de control acces se utilizeaza un software de control acces. Prin intermediul acestui software se realizeaza cateva functii de baza:

- Se realizeaza programarea intregului sistem
- Se administreaza sistemul
- Se monitorizeaza evenimentele de control acces produse in sistem
- Se executa rapoartele de administrare si se exporta in diferite formate
- Se interfateaza cu baze de date pentru import/export de date din/spre alte sisteme

Orice software de control acces utilizeaza pentru stocarea informatiilor de setare a sistemului si istoricul de evenimente intr-o baza de date. Dintre bazele de date cele mai utilizate mentionam : MS-SQL Server, MSDE, Interbase, FireFox, Microsoft Access, Oracle, baze de date proprietare. Din punctul de vedere al operabilitatii software-ul de control acces poate fi de tip single user – folosit doar de un singur operator la un moment dat sau poate fi de tip client–server, in care pot exista mai multi operatori simultan fiecare executand un set de functii specifice pe un software client conectat prin retea la software-ul server. De exemplu pentru operatorii din dispeceratul de securitate se asigura functiile de monitorizare evenimente, administratorul sistemului executa functii de configurare iar managerii de departamente executa rapoartele de prezenta pentru departamentele respective. Intr-un astfel de sistem functiile sunt executate distribuit, fiecare operator avand un set de permisuni.

Caracteristici de baza :

Functii de programare. Aceste functii sunt specifice instalatorului si sunt de obicei executate doar la momentul punerii in functiune a sistemului. Aceste functii includ : definirea si setarea parametrilor de comunicatie dintre unitatile de acces si calculatorul de gestiune, setari specifice fiecarui tip de echipament din sistem, incluzand unitatea de acces, tipul de cititor si portul unde se conecteaza in unitate, setari privind formatul cardului si a caracteristicilor cardului etc.

Functii de administrare. Aceste functii sunt cele realizate de administratorul sistemului si includ : crearea de time-zone-uri (perioade de timp), crearea/modificarea nivelelor de acces si a utilizatorilor de carduri, executia de rapoarte si gestiunea operatorilor si a permisiunilor acordate acestora. Notiuni si termeni folositi in sistemele de acces :

Cardholder - utilizatorul unui sistem de control acces, ce are un card si/sau cod PIN

Time zone - reprezinta o perioada de timp in care utilizator poate sa aiba acces intr-o anumita zona.

Reader group –grup de cititoare, folosit pentru crearea nivelelor de acces

Access Level, Clearence Code, Drept de Acces – acest concept sta la baza oricarui sistem de control al acces-ului, acesta raspunde la intrebarile unde ? si cand ? se poate intra. Un nivel de acces este compus din una sau mai multe perechile <Grup de Cititoare, Time zone>. Pentru a rspunde la intrebarea cine ? se aloca nivelul de acces unui utilizator (cardholder).

Anti-passback : acest termen defineste capacitatea sistemului de a interzice accesul unui card cand acesta este prezentat de doua ori pe acelasi sens fara ca el sa fi fost prezentat pe sensul invers. Regula care trebuie respectata este sa se prezinte cardul atat la intrare cat si la iesire, succesiv. Exista doua

tipuri de antipasaback ; hardware si software. Cel hardware interzice accesul cardului in zona de antipassback iar cel software nu interzice accesul dar acest eveniment este semnalizat in software ca eveniment de alarma.

Un concept invecinat este cel de arie sau zona de antipassback. O arie de antipassback se defineste logic prin setarea cititoarelor de intrare si iesire din acea arie. Un utilizator figureaza in interiorul ariei de antipassback indiferent pe la ce cititor a intrat si poate sa iasa din arie pe la oricare alt cititor de iesire trecand intr-o alta arie de antipassback. Tinand cont de acest concept exista cateva tipuri de antipassback: local, zonal sau temporar.

- local antipassback ; acest tip de antipassback se aplica doar pentru doua cititoare conectate la o singura usa de acces (interior, exterior), uzual conectate la aceeasi unitate de control acces
- zonal antipassback : se foloseste de conceptul de arie de antipassback si se aplica pentru mai mult de doua cititoare conectate la unitati diferite, cititoare care fac parte dintr-o arie de antipassback
- timed antipassback (temporar): este o forma de antipassback care interzice accesul pe acelasi cititot pentru un timp prestabilit, daca timpul dintre cele doua accesari este mai mic decat acel timp prestabilit, astfel se produce, de fapt, o intarziere a utilizatorului in cazul in care acesta incalca regula de antipassback. Dupa trecerea acelui timp starea de antipassback dispare.

  Implementarea ariei de antipassback permite cunoasterea stricta a numarului de persoane aflate intr-un anumit spatiu si, implicit, luarea unor decizii pe baza prezentei/absentei utilizatorilor in acea arie (de exemplu se poate produce auto-armare sau activarea/dezactivarea unor intrari sau actionarea unor iesiri).

Drepturi/permisiuni. Fiecare operator al unui software de control acces poate sa aiba drepturi diferite, alocate de admistratorulu sistemului. Acesta poate creea grupuri de permisiuni sau profile de utilizator in care sunt setate functiile alocate pentru acel nivel de permisiune.

Functii de monitorizare si raportare. Toate evenimentele din sistem sunt afisate in timp real si stocate in baza de date pentru raportare ulterioara dupa criterii multiple.

Functii de mentenanta . In aceasta grupa de functii se gasesc instrumente de monitorizare si diagmoza pentru echipamentele din sistem si pentru baza de date, incluzand back-up/restore si arhivare. Sunt utile pentru verificarea functionarii componetelor din sistem si detectarea starilor de defect.

Caracteristici optionale ale aplicatiilor de control acces.

Pe langa functiile de baza majoritatea aplicatiilor de control acces integreaza si functii suplimentare cum ar fi :

- visitor management: gestioneaza vizitatori care folosesc cardurile de acces temporare (care au atributul de vizitator escort)
- badge design: permite realizarea machetelor de carduri si printarea acestor prin intermediul imprimantelor de carduri specializate
- control lifturi: integreaza controlul lifturilor
- time&attendance: aplicatie de prezenta si pontaj
- trimitere de mesaje email & SMS: permite trmiterea de mesaje email sau SMS in cazul anumitor tipuri de alarme
- Guard tour: turul garzi sau patrol tour, permite folosirea cardurilor de acces pentru realizarea unui tur de paza, cardul trebuie prezentat la un anumit numar de cititoare fara ca usa sa fie deschisa, in vederea verificari prezentei in punctele determinate in turul de paza
- Muster report: permite realizarea manuala sau automata a unui raport care se executa in anumite situatii de urgenta pentru verificarea prezentei unor persoane in anumite spatii ce trebuie eliberate in caz de urgenta. Pentru ca acest lucru sa fie functional trebuie definite punctele de prezenta la intrarea si iesirea din zona monitorizata.

Întocmit
Ing. Viorel TULEŞ