

FUNCȚII SPECIALE ALE SISTEMELOR DE CONTROL AL ACCESULUI ȘI APLICAȚII PRACTICE ALE ACESTORA

Ing. Laurentiu POPESCU
SC SETALARM, București

Acest articol este dedicat atât dezvoltatorilor de aplicații de control al accesului cât și potențialilor beneficiari, pentru a înțelege mai bine performanțele și diferențele dintre diferite sisteme de control al accesului.

O aplicație simplă de control al accesului presupune următoarele elemente fizice și funcțiuni:

- un punct de acces controlat electromecanic
- un element de identificare (cititor de tag-uri, identificator biometric, etc). – pentru a permite accesul unidirecțional (intrare)
- un buton de deschidere pentru ieșire
- un controler în care sunt memorate elementele de identificare.

O astfel de aplicație simplă permite controlul unidirecțional al accesului, restricționând accesul persoanelor neautorizate, dar singura informație oferită este cine a intrat sau a permis accesul în zona restricționată și când (în condițiile în care controlerul este conectat la o stație de lucru pe care rulează un program dedicat). În analizele post-eveniment aceste informații sunt insuficiente, iar în cazul obiectivelor cu grad ridicat de risc total inadecvate.

Din acest motiv, toate sistemele dedicate de control al accesului, permit (sau ar trebui să permită) următoarele funcțiuni, pornind de la controlul bidirecțional al accesului.

1. Definirea zonelor de acces și introducerea funcției de anti-passback (APB). O zonă de acces este o arie delimitată, cu una sau mai multe căi de intrare/ieșire, toate controlate. Funcția APB restricționează accesul multiplu unidirecțional al unui utilizator, ceea ce se traduce prin faptul că dacă un utilizator a intrat în zona APB, el trebuie să iasă din zonă înainte de a i se permite accesul din nou. Această funcție previne utilizarea incorectă (sau frauduloasă) a sistemului de control al accesului și permite generarea de rapoarte utile atât pentru managementul securității obiectivului cât și pentru managementul de personal.

2. Numărarea de persoane în zona APB. Introducerea acestui counter permite dezvoltarea unor funcțiuni de securitate speciale, atât pe partea de control al accesului cât și pe partea de sistem antifracție. Sistemul de control al accesului poate limita numărul de persoane din zona APB sau poate fi utilizat pentru implementarea unor funcții de automatizări în funcție de gradul de ocupare a zonei. Ca exemplu deosebit de util pentru beneficiari, în cazul în care gradul de ocupare a spațiului este zero, anumite instalații electrice (ventilație, iluminat) pot fi oprite iar sistemul antifracție poate fi activat (utilizând o zonă de "switch"). Pentru sisteme de înaltă securitate se pot dezvolta aplicații speciale cum ar fi "dead man trapp" – capcana mortului - care lucrează astfel: în cazul în care zona APB nu este ocupată, dacă sistemul antifracție detectează mișcare atunci alarma este declanșată instantaneu. În cazul în care gradul de ocupare este diferit de zero și sistemul antifracție NU detectează mișcare pentru un interval de timp pre-definit (să spunem 10 minute) atunci este

declanșată alarma. O astfel de funcțiune este utilă spre exemplu pentru camere de pază /dispecerizare, în cazul unui atac în care dispecerul a fost imobilizat din exterior: el este înregistrat în zona APB dar va genera prin inactivitate fizică o alarmă după scurgerea intervalului de timp prestabilit.

3. Restricționarea accesului pe intervale de timp. Aceste funcțiuni sunt deosebit de importante pentru buna desfășurare a fluxului de persoane. Restricționarea se poate face la nivel de element de acces (ușă controlată) sau pe grupuri de utilizatori.

4. "Reason code". Un alt mod de restricționare, derivat din accesul dual, elemente de identificare + PIN (cod personal numeric), presupune introducerea unui cod de 2 cifre, de exemplu pentru motivul pentru care este utilizată calea de acces. Această funcție poate fi corelată cu restricționarea accesului pe intervale de timp. Să luăm ca exemplu cazul unei întreprinderi la care accesul personalului este restricționat bidirecțional. În intervalul de timp în care personalul trebuie să sosească la serviciu, intrarea poate fi efectuată doar pe baza de cartelă de identificare. După începerea programului, accesul poate fi restricționat la cartelă + "reason code", adică un cod predefinit pentru motivul pentru care persoana a sosit după începerea programului: să zicem 01 pentru întârziere, 02 învoit cu permisiunea conducerii, 03 pentru că persoana a vizitat în prealabil un client, 04 pentru aprovizionare, etc. Aceste coduri permit obținerea de rapoarte extrem de utile pentru managementul personalului.

5. Definirea de trasee obligatorii.

6. Managementul lifturilor și multe alte aplicații.

Rapoarte

Cel mai obișnuit raport se referă la tranzacțiile din sistem (prin tranzacție se înțelege atât accesul cât și respingerea accesului unui utilizator). El poate fi generat pe zi, locație, utilizator, etc.

Localizarea unei persoane - în funcție de structura sistemului și de restricționări, un utilizator poate fi localizat pe baza ultimei tranzacții efectuate.

Rapoarte de managementul personalului - rapoarte de prezență sau absenteism, număr de ore lucrate în zone APB, etc.

O altă categorie de rapoarte se referă la utilizatorii sistemului (cei care au acces la programarea cardurilor de acces, a dispecerilor, etc.). Diferiți utilizatori ai sistemului pot avea drepturi diferite: de ex. dispecerii pot emite doar carduri de vizitatori, programarea utilizatorilor obișnuiți fiind efectuată doar de managerul de securitate. Sistemele trebuie să permită generarea de rapoarte de audit, din care să rezulte cine și când a programat sau a modificat accesul unui utilizator sau vizitator.

Utilizând baze de date relaționale și comunicația prin Internet, sistemele pot fi extinse la un număr impresionant de puncte de acces, site-uri, cu management local dar cu bază de date centralizată, făcând din sistemul de control al accesului un instrument modern, nu numai de asigurare a securității cât și de management de zi cu zi al personalului.