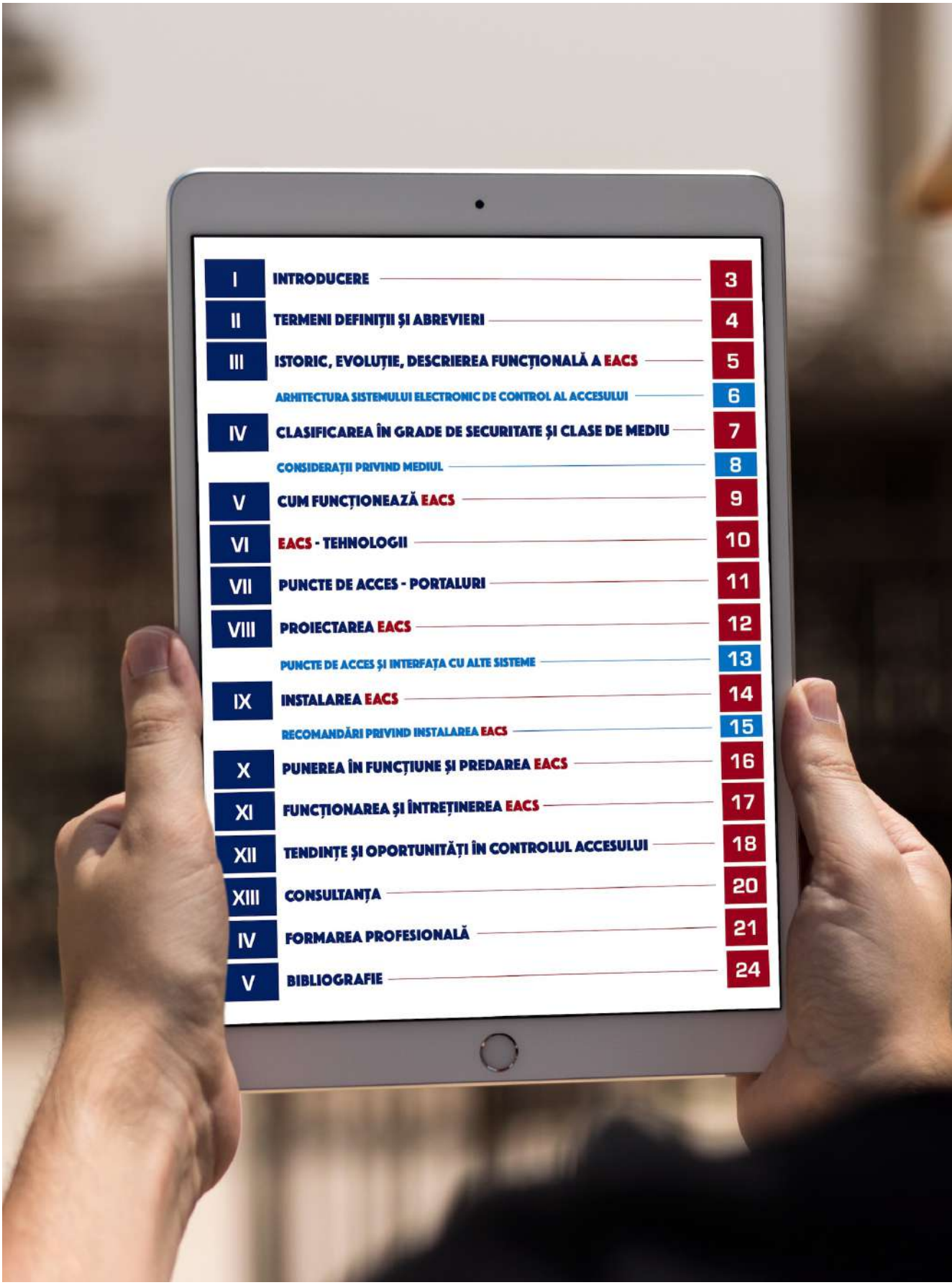
SISTEME ELECTRONICE DE CONTROL AL ACCESULUI

GHID ILUSTRAT

pentru societățile specializate în domeniul sistemelor de alarmare împotriva efracției și a celor din domeniul pazei și protecției

Ion Iordache
Adrian Marian Fleacă

CUPRINS:



I. INTRODUCERE

Pe măsură ce tehnologia se dezvoltă și securitatea fizică se schimbă utilizând tot ceea ce noul val tehnologic pune la dispoziție, controlul accesului într-o clădire, de exemplu, privit multă vreme doar prin prisma asigurării unor încuietori sau agenți de securitate care să împiedice accesul, joacă un rol tot mai mare în procesele de asigurare a securității fizice.

Toate aceste schimbări tehnologice au creat o schimbare importantă în modul de abordare a proceselor de proiectare, instalare și întreținere. Un ajutor important pentru această nouă abordare vine de la seria de standarde "IEC 60839 Sisteme electronice de control al accesului" care include două părți: Partea 11-1: Sisteme electronice de control al accesului – Cerinţe pentru sistem şi componente și Partea 11-2: Sisteme electronice de control al accesului – Linii directoare pentru aplicaţii".

Controlul accesului se clasifică în control de tip logic care include software, protocoale de identificare, autentificare, autorizare și responsabilitate (audit), pentru a permite accesul la un sistem informatic și/sau la o resursă de rețea și de tip fizic (o unitate centrală) care "gestionează punctele de control, unităţile de comandă, cititoarele, încuietorile sau dispozitivele electromagnetice de acţionare a uşilor, şi are rolul de restricţionare a accesului neautorizat în spaţiile protejate" așa cum se specifică în legislația incidentă domeniului sistemelor de securitate private aflată în vigoare în România.

În acest ghid ne vom referi la mecanismele de control al accesului fizic cu o abordare a planificării, instalării, operării, întreţinerii şi documentării sistemelor electronice de control al accesului tratate în "SR EN 60839-11-2+AC:2016 Partea 11-2: Sisteme electronice de control al accesului. Linii directoare pentru aplicaţii" și vom face referiri la tendințele, oportunitățile și provocările actuale în controlul accesului.

Scopul nostru este acela de a demonstra că, controlul accesului cuprinde mai mult decât "o unitate centrală" și unul sau mai multe cititoare; acest subsistem fiind de fapt, un segment fundamental al unui sistem de securitate integrat care se extinde dincolo de clădire, porți sau garduri pentru a proteja instalațiile, bunurile, proprietatea intelectuală și oamenii iar eficiența unui sistem de control al accesului depinde de ușurința în utilizare, comunicarea și instruirea utilizatorilor și mai ales de integrarea cu alte sisteme de securitate.

II. TERMENI, DEFINIȚII ȘI ABREVIERI

Subsistemul de control al accesului cuprinde unitatea centrală, care gestionează punctele de control, unităţile de comandă, cititoarele, încuietorile sau dispozitivele electromagnetice de acţionare a uşilor, şi are rolul de restricţionare a accesului neautorizat în spaţiile protejate.
(HG. 301/2012)

EACS - Sistem electronic de control al accesului (Electronic Access Control System), sistem conceput să permită persoanelor sau entităţilor autorizate intrarea într-o/ieşirea dintr-o zonă de securitate controlată şi să refuze o astfel de intrare şi/sau ieşire indivizilor sau entităţilor neautorizate
(SR EN 60839-11-1:2014)

Zonă a perimetrului, parte a perimetrului protejat care are propriul set de niveluri de acces.

Perimetru protejat (perimetru controlat), perimetru definit de o graniţă fizică, prin care trecerea este controlată prin intermediul unuia sau mai multor puncte/portaluri de acces.

NOTĂ: *Poate conţine mai multe zone ale perimetrului separate cu grade de securitatea identice sau diferite.*
(SR EN 60839-11-2+AC:2016)

Punct de acces (portal), intrare/ieşire fizică la care accesul poate fi controlat printr-o uşă, un turnichet sau altă barieră de securitate.
(SR EN 60839-11-1:2014)

ACU - Unitate de control al accesului (Access Control Unit), parte a unui sistem de control al accesului care are interfaţă cu cititoare, dispozitive de blocare şi dispozitive de sesizare, luând o decizie de a autoriza sau de a refuza accesul printr-un portal.
(SR EN 60839-11-1:2014)

CEM - Compatibilitate electromagnetică (Electromagnetic Compatibility)
(SR EN 60839-11-2+AC:2016)

REX - Dispozitiv de solicitare a ieşirii (Request to Exit)
(SR EN 60839-11-2+AC:2016)

Echipamente accesorii, orice componentă a unui sistem electronic de control al accesului alta decât unitatea de control al accesului.

Anti-passback, mod de funcţionare care solicită validarea utilizatorului la ieşirea dintr-o zonă de securitate controlată pentru a-i autoriza reintrarea şi invers.

Biometrie (biometric), orice caracteristică fiziologică unică, măsurabilă, sau trăsătură personală care este utilizată ca identificator pentru a recunoaşte şi verifica identitatea dinamicii unui individ (Ex. amprente digitale, geometrie a mâinii sau a feţei, retină/ochi, faţă, voce, dinamica semnăturii sau a tastării.

Controlul accesului tip sas, combinaţie de două sau mai multe portaluri care trebuie să fie utilizate secvenţial pentru a obţine acces într-o zonă de securitate controlată.
(SR EN 60839-11-1:2014)

Turnichet, portal conceput să limiteze fizic trecerea unei singure persoane o dată.

Consolă de monitorizare, componentă funcţională care constă din dispozitive folosite ca interfaţă de control, înregistrare şi indicare pentru operatorul sistemului electronic de control al accesului.

Dispozitiv de acţionare a punctului de acces, dispozitiv de acţionare a portalului, parte a unui sistem de control al accesului care are interfaţă cu o unitate de control al accesului care deblochează şi securizează un portal în conformitate cu un ansamblu de reguli prestabilite.

Interfaţă punct de acces, interfaţă portal, dispozitiv sau circuit care controlează deblocarea şi securizarea unui punct de acces.
(SR EN 60839-11-1:2014)

III. ISTORIC, EVOLUȚIE, DESCRIEREA FUNCȚIONALĂ A EACS

Controlul accesului nu este o noutate. De când s-au inventat ușile a fost întotdeauna cineva și/sau ceva care le-a protejat, vechiul mecanism de zăvorâre evoluând treptat de la yale mecanice cu chei la echipamente electronice sofisticate.

În a doua jumătate a anilor 1700 au fost create și puse în aplicare primele încuietori de ușă, în timp ce în 1778 a intrat pe piață încuietorul cu pârghie, butucul pentru chei așa cum îl știm și în zilele noastre.

Cu toate acestea, în România, există în biserica evanghelică fortificată din Biertan, județul Sibiu construită în secolul al XII-lea o ușă, ușa sacristiei, care pe vremuri era camera tezaurului, cu un sistem complicat de 19 încuietori realizată de meșterii locali în anul 1515 care a fost premiată la Expoziția Mondială din 1900 de la Paris.

Cele 19 încuietori se împart ingenios: 3 în stânga, 3 în dreapta, 3 sus și 7 pe încuietoare, acționate simultan de o singură cheie.

Mai precis, prin cheie sunt activate patru mecanisme iar prin manivelă alte cinsprezece iar încuietoarea blochează ușa în 13 puncte.

Ușa, în sine, constituie un exemplu reprezentativ de manufactură săsească medievală, datorită intarsiilor și a sistemului original de închidere, care funcționează și astăzi.

"La sfârșitul anilor 1800, odată cu inventarea becului și extinderea energiei electrice, acum era posibil ca angajați să lucreze chiar și în cele mai întunecate nopți. Având în vedere că ideea de a lucra pe tot parcursul zilei și nopții devenind din ce în ce mai comună, sa concentrat și mai mult pe menținerea în siguranță a clădirilor și pe acordarea accesului numai personalului de lucru corespunzător. Aici utilizarea ceasurilor de timp, înregistrările detaliate și securitatea a început să devină o necesitate corporativă. Și aici este locul în care securitatea, managementul forței de muncă și controlul mediului dvs. au început să evolueze în ceea ce este astăzi.

Există numeroase dovezi de securitate prin controlul accesului de-alungul întregii istorii a umanității.

Acestea includ încuietori mecanice din lemn descoperite în Asiria (Irakul de astăzi) încă din 4000 î.Hr. iar romanii, inspirați de sistemele de închidere din lemn ale grecilor antici, au creat primele chei metalice unice, unele suficient de mici pentru a fi folosite ca bijuterii iar idea aceasta a condus la crearea lacătului roman care a fost apoi îmbunătățit de chinezi pentru a fi folosit pe rutele comerciale și a inspirat lacătele grele din fier forjat care au fost folosite în Anglia în jurul anilor 870 – 890 d.Hr.

Toate aceste elemente istorice s-au combinat și au evoluat pentru a deveni controlul nostru de acces de zi cu zi. Controlul general al accesului și toate caracteristicile sale sunt înrădăcinate în istorie și arată cât de fiabil este controlul accesului pentru siguranța noastră."

(Sursa: The History of Access Control)

ARHITECTURA SISTEMULUI ELECTRONIC DE CONTROL AL ACCESULUI

Sistemul electronic de control al accesului trebuie să cuprindă, după cum este adecvat configuraţiei specifice a sistemului de control al accesului, următoarele funcţii de bază:

A - Procesare: compararea modificărilor apărute în cadrul sistemului cu un ansamblu de reguli prestabilite pentru a produce acţiuni predefinite.

B - Comunicare: transmiterea semnalelor între componentele sistemului de control al accesului pentru a asigura aplicarea regulilor prestabilite.

C - Configurare (programare): stabilirea regulilor de procesare.

D - Interfaţa punctului de acces.

E - Recunoaştere: recunoaşterea utilizatorilor autorizaţi care solicită acces.

F - Anunţare: funcţiile de alertă, afişare şi/sau înregistrare.

G - Semnalizarea constrângerii: avertizare silenţioasă, emisă de către utilizatorii sistemului, privind condiţii de solicitare coercitivă a accesului în desfăşurare.

H - Interfaţă cu alte sisteme: utilizarea în comun a funcţiilor şi/sau a modificărilor care se produc în sisteme.

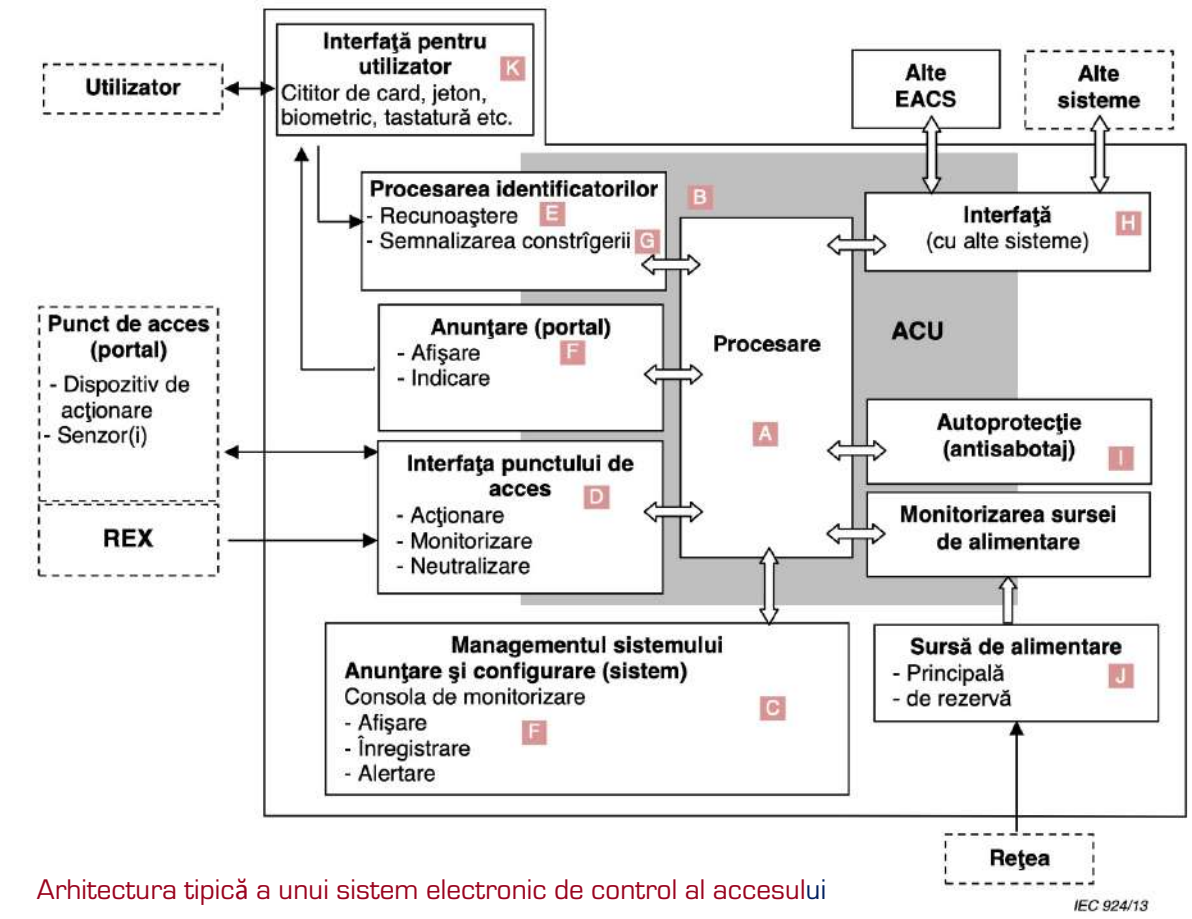
I - Autoprotecţia sistemului: prevenirea, detectarea şi/sau raportarea unui sabotaj sau a unei interferări intenţionate şi/sau accidentale cu funcţionarea sistemului.

J - Sursă de alimentare: modul care furnizează energie electrică sistemului de control al accesului.

K - Interfaţă pentru utilizator: mijloc prin care utilizatorul solicită acces (de exemplu, tastatură sau cititor de jeton) şi primeşte indicaţii despre starea accesului.

Funcţiile pot fi distribuite şi pot fi localizate în mai mult de o incintă sau integrate într-un singur cabinet.

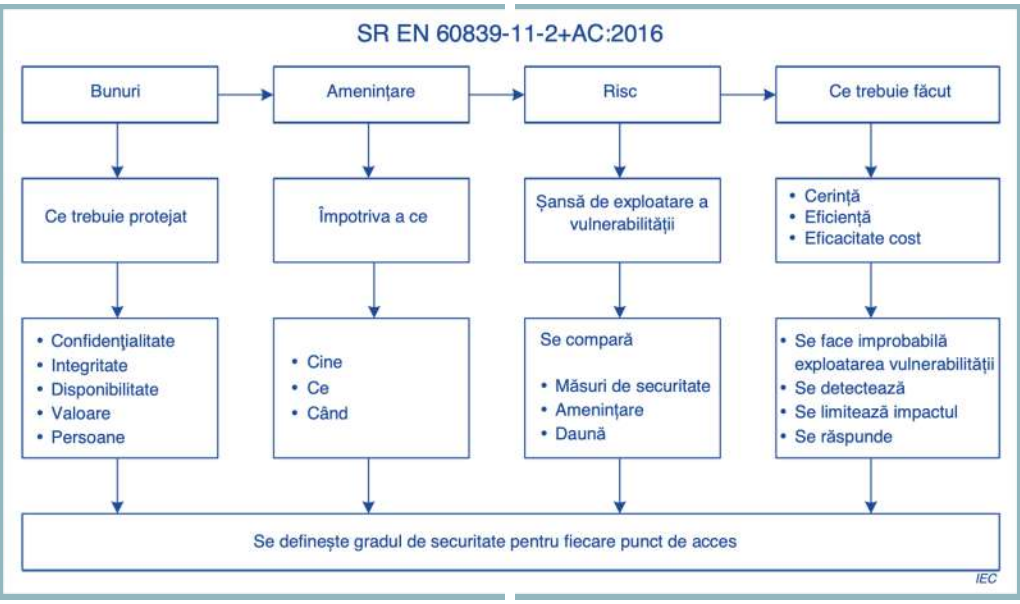
SR EN 60839-11-1:2014



Arhitectura tipică a unui sistem electronic de control al accesului

IV. CLASIFICAREA ÎN GRADE DE SECURITATE ȘI CLASE DE MEDIU

Este esenţial ca evaluarea riscurilor să fie efectuată înainte de implementarea sistemului de control al accesului. Diagrama de evaluare a riscurilor din figură identifică considerentele cheie.



Gradele de securitate sunt definite în funcţie de valoarea bunurilor care necesită protecţie şi determinarea (cunoştinţe/abilităţi) şi metodele de atac ale persoanelor care intenţionează să eludeze sistemul (adversarii). Tabelul prezintă exemple de aplicaţii tipice pentru fiecare grad.

Grad	1	2	3	4
Nivel de risc	**Scăzut**	**Scăzut spre mediu**	**Mediu spre ridicat**	**Ridicat**
Aplicaţie	Aspecte organizaţionale, protecţia bunurilor cu valoare scăzută	Aspecte organizaţionale, protecţia bunurilor cu valoare scăzută până la medie	Mai puţine aspecte organizaţionale, protecţia bunurilor comerciale de valoare medie până la valoare înaltă	Protejarea în principal a infrastructurii comerciale sau critice de foarte mare valoare
Abilităţi/cunoştinţe ale adversarilor/atacatorilor	Abilităţi scăzute, cunoştinţe scăzute despre EACS, lipsa cunoştinţelor despre identificatori şi tehnologii IT. Mijloace financiare scăzute pentru atacuri	Abilităţi şi cunoştinţe despre EACS medii, cunoştinţe scăzute despre identificatori şi tehnologii IT. Mijloace financiare scăzute până la medii pentru atacuri	Abilităţi şi cunoştinţe despre EACS înalte, cunoştinţe medii despre identificatori şi tehnologii IT. Mijloace financiare medii pentru atacuri	Abilităţi şi cunoştinţe despre EACS foarte înalte, cunoştinţe înalte despre identificatori şi tehnologii IT. Mijloace financiare mari pentru atacuri
Exemple tipice	Hoteluri	Birouri comerciale, întreprinderi mici	Industriale, administraţie, financiare	Zone foarte sensibile (instalaţii militare, guvern, cercetare şi dezvoltare, zone critice de producţie)

CONSIDERAȚII PRIVIND MEDIUL

Este de aşteptat ca fiecare componentă a unui sistem electronic de control al accesului să funcţioneze corect în mediul său de utilizare şi să continue să o facă pentru o perioadă rezonabilă de timp. Însă, echipamentele unui sistem de control al accesului sunt instalate în numeroase medii foarte diferite şi ar fi lipsit de sens practic să se supună încercării fiecare aspect al celor mai extreme condiţii de mediu imaginabile şi de imunitate la efecte electromagnetice.

Componentele trebuie să fie adecvate pentru una dintre următoarele clase de mediu:

Clasa de mediu I – Echipament amplasat în interior, restricţionat la mediul rezidenţial sau de birouri. Clasa de mediu I cuprinde influenţe de mediu resimţite în mod normal în interior atunci când temperatura este menţinută bine (de exemplu, într-o proprietate rezidenţială sau comercială).

NOTĂ - Este de aşteptat ca temperaturile să varieze între +5 °C şi +40 °C.

Clasa de mediu II – Echipament amplasat în interior în general. Clasa de mediu II cuprinde influenţe de mediu resimţite în mod normal în interior atunci când temperatura nu este bine menţinută (de exemplu, pe coridoare, în hale sau pe casa scărilor şi unde poate avea loc condensare pe ferestre şi în zonele de depozitare neîncălzite sau în depozitele unde încălzirea este intermitentă).

NOTĂ - Este de aşteptat ca temperaturile să varieze între –10 °C şi +55 °C.

Clasa de mediu III – Echipament amplasat în exterior – adăpostit sau în interior în condiţii extreme. Clasa de mediu III cuprinde influenţe de mediu care apar în mod obişnuit în exterior, atunci când componentele EACS nu sunt pe deplin expuse vremii sau în interior, unde condiţiile de mediu sunt extreme.

NOTĂ - Este de aşteptat ca temperaturile să varieze între –25 °C şi +55 °C.

Clasa de mediu IV – Echipament amplasat în exterior – Generalităţi. Clasa de mediu IV cuprinde influenţe de mediu care se întâlnesc în mod obişnuit în exterior atunci când componentele EACS sunt pe deplin expuse vremii.

NOTĂ - Este de aşteptat ca temperaturile să varieze între –25 °C şi +70 °C în funcţie de regiune. Intervalul de temperaturi poate fi extins în plus şi/sau în minus pentru diferite zone geografice sau climatice.

V. CUM FUNCȚIONEAZĂ EACS

Concepte de sisteme de control al accesului

Controlul accesului este prezent peste tot în viața noastră, de la încuietoarea ușii casei sau a autoturismului personal până la numărul de identificare personală pentru cardul bancar.

Scopul este același, EACS-urile sunt concepute pentru a ne asigura că numai persoanelor autorizate li se permite să intre într-un spațiu exclusiv.

Acreditări: EACS se bazează pe utilizatori autentificați iar acreditările pot fi, de exemplu, amprenta.

Cititoare de acreditări: EACS combină acreditările cu un cititor de acreditări (cititor de carduri, tastatură sau cititor biometric) pentru a trimite un cod către computer unde este comparat cu o bază de date de coduri. Dacă se găsește o potrivire, computerul ordonă portalului să descuie ușa și să vă permită intrarea (sau ieșirea).

Cine, Unde și Când: Fiecare utilizator autorizat (Cine) este valabil pentru anumite portaluri (Unde) și pentru un anumit program autorizat (Când) — cui i se permite să intre, unde pot intra și când au voie să intre sau să iasă.

Autorizare cu doi factori: În acest caz, accesul la o zonă critică, cum ar fi o cameră de server sau un seif, necesită prezentarea a două acreditări într-o perioadă scurtă de timp, de obicei una de la un angajat și una de la un manager.

Controlul accesului angajaților și vizitatorilor: cardurile de acces sunt, de obicei, eliberate angajaților și sunt purtate pe haine prin intermediul unei agrafe sau al șnurului. Sistemele de control al accesului din facilitățile care primesc vizitatori pot fi configurate cu un card special pentru vizitatori pentru a permite contractorilor, vânzătorilor și vizitatorilor să aibă acces la anumite zone desemnate.

Integrarea sistemului video: Ca răspuns la o alarmă sau o încercare de acces neautorizat (și la multe alte tipuri de evenimente), sistemul de alarmă/control acces poate face ca sistemul video de securitate să afișeze una sau mai multe camere video care sunt legate de eveniment.

Elementele de control al accesului includ:

- Utilizatori.
- Portaluri de acces.
- Acreditări și cititoare de acreditări.
- Procesul de autorizare a acreditărilor.
- Încuietori, alarme și dispozitive de ieșire.
- Zone de acces și orare.
- Baza de date a sistemului de control al accesului.
- Infrastructura de comunicații.
- Politici și proceduri de control al accesului.

Controlul accesului, într-un sistem de securitate, este o problemă cel puțin la fel de importantă ca și detectarea intruziunilor și presupune rezolvarea a două probleme: admiterea accesului pentru persoanele autorizate, adică identificarea persoanei respective într-o bază de date, respectiv controlul persoanei în sensul interdicției accesului în situația detectării unor materiale sau obiecte interzise.

Identificarea este o problemă dificilă și multidisciplinară cu conotații nu numai tehnice, ci și legale, având în vedere conformarea cu cerințele Regulamentului European (GDPR) .

În prezent există preocupări, în special pentru:

- identificare personală;
- culegerea informațiilor despre persoane;
- detectarea sau limitarea deplasărilor, acțiunilor și comportamentului persoanelor;
- forme de identificare care, mai degrabă, arată apartenența la un grup social decât identitatea personală;
- identificarea produselor și ambalajelor;
- identificarea vehiculelor;
- identificarea animalelor.

Măsurile electronice de control al accesului fac mai mult decât deschiderea unor uși. Ele permit sau interzic accesul persoanelor în funcție de nevoile organizației. Programele software din centrul acestor sisteme permit administratorilor de securitate posibilitatea de a determina cine obține acces, la ce oră și în ce zile/date specifice.

Personalul de securitate sau alt personal utilizează software protejat prin parolă pentru alarme sonore de intruziune și elaborează rapoarte pentru activitatea de control al accesului în unitate.

VI. EACS - TEHNOLOGII

Cartelele cu cod de bare au apărut și s-au dezvoltat ca urmare a necesității unui sistem pentru identificarea mărfurilor în transporturi, depozite, magazine etc. Legătura dintre informația asupra produsului și stocarea acesteia în baza de date este locul unde intervin codurile de bare.

Dispozitive cu banda magnetică - identificarea cu ajutorul cartelelor personale de identitate a început să fie dezvoltată de marile societăți bancare pentru mijloacele de plată fără numerar, ATM, (de unde și numele – credit card), cu mai bine de 25 ani în urmă. Credit card-urile au impus și dimensiunile, standardizate astăzi: 2"-3.5" (aproximativ 54-85 mm).

Cartele de proximitate - sistemul de recunoaștere cu cartele de proximitate este cel mai performant din seria de sisteme credit card, în sensul că este singurul echipament care este capabil să detecteze și să identifice cartela, fără să fie necesar ca aceasta să fie introdusă într-un cititor special. Astfel, persoana poate fi identificată chiar dacă cartela de proximitate este păstrată în portmoneu sau poșetă.

Smart card - alături de cartelele de proximitate, cartelele inteligente sunt cele mai sigure dispozitive de personalizare a cartelelor. Cartelele inteligente au avantajul că, spre deosebire de cartelele de proximitate, fiind realizate cu o memorie care poate fi ștearsă și scrisă electric de mii de ori

Sisteme biometrice - termenul „biometrie" se referă la toate tehnicile de identificare bazate pe o serie de caracteristici fizice sau fiziologice, dificil sau imposibil de modificat sau imitat.

Fotografia și fizionomia - fotografia, o reprezentare grafică a unei fizionomii, sau trăsături specifice, realizată la un moment anume în timp și realizată în condiții de iluminare specifice, este, încă, printre cele mai utilizate metode biometrice.

Holograma - o metodă de identificare mai dificil de falsificat dar, în aceeași măsură, greu de implementat, presupune folosirea unei holograme. Aceasta este, principial, tot o fotografie dar are marele avantaj că nu memorează numai intensitatea luminoasă (în tonuri de gri pentru o fotografie alb-negru sau tonuri ale culorilor fundamentale RGB pentru o fotografie color) ci și faza semnalului.

Antropometria - presupune măsurarea unor părți ale corpului uman. Dispozitivele electronice se folosesc pentru măsurarea parametrilor antropologici ai mâinii sau pentru explorarea tridimensională a indexului

Amprentele papilare - după fotografie, aceasta este cea mai veche metodă biometrică. Identificarea prin amprentele papilare cunoaște două abordări: una folosește compararea între buclele, liniile și traseele dactiloscopice memorate în baza de date și amprenta persoanei de identificat; cealaltă presupune o verificare minuțioasă, a zonelor de început și de bifurcare a crestelor și adâncițurilor papilare.

Imaginea retiniată - constă în determinarea aspectului și mărimii vaselor de sânge existente în retină. Este o metodă de identificare extrem de sigură însă este puțin folosită datorită caracterului invaziv. Persoana trebuie să-și scoată ochelarii sau lentilele de contact și să-și focalizeze privirea pe un punct, astfel încât sistemul optic al cristalinului să nu modifice focalizarea sistemului optic de citire.

VII. PUNCTE DE ACCES PORTALURI

Intrare cu card/ieșire liberă

Atunci când o persoană se confruntă cu un portal cu acces controlat, trebuie să arate autorizație pentru a trece.

Cea mai comună formă de proiectare a portalului este cea concepută pentru a permite intrarea numai utilizatorilor autorizați, dar și pentru a permite oricui din zona de acces să iasă liber.

Acest lucru este în mod normal găzduit prin utilizarea unui cititor de carduri, tastatură sau cititor biometric (sau o combinație a acestora) pentru a autoriza utilizatorul să intre. Ieșirea este posibilă fără a fi un utilizator autorizat; adică orice vizitator sau persoană neautorizată care a fost escortată înăuntru de către un utilizator autorizat este liber să iasă în orice moment și fără niciun impediment.

Un portal tipic are un sistem de blocare care trebuie deblocat pentru a ieși.

Pot fi utilizați diferiți senzori de cerere de ieșire, inclusiv un buton de ieșire, bara tactilă de ieșire în panică sau un detector de mișcare deasupra ușii.

Intrare cu card/ieșire cu card

O altă configurație comună a portalului folosește un cititor de acreditări pe ambele părți ale ușii.

Această variație ajută la asigurarea faptului că persoanele sunt luate în considerare atunci când intră și ies dintr-o zonă.

Este obișnuit să vedeți acest tip de portal în zonele în care instrumentele financiare sau informațiile deținute sunt controlate, cum ar fi într-o cameră de contorizare a numerarului sau o cameră de arhivă.

Atunci când utilizați acest tip de portal, este imperativ să vă asigurați că ușa poate fi deschisă în caz de urgență fără a necesita o acreditare, care ar putea să nu fie disponibilă imediat.

Este uzual să se integreze mecanismul de blocare de pe portalurile de intrare/ieșire cu sistemul de alarmă de incendiu și, de asemenea, să se monteze un dispozitiv de deschidere de urgență a ușii lângă cititorul de ieșire, astfel încât ocupanții să poată ieși în caz de incendiu sau alt tip de urgență.

VIII. PROIECTAREA EACS

Clasificarea de securitate trebuie definită pentru fiecare punct de acces, luând în considerare nevoile de control ale intrării şi ieşirii. Pentru punctele de acces din acelaşi sistem pot fi utilizate diferite grade de securitate iar pentru componentele comune ale sistemului, care protejează puncte de acces cu grade diferite de securitate, trebuie să se asigure îndeplinirea cerinţelor punctului de acces cu cel mai înalt grad de securitate pe care îl operează împreună.

În cazul în care nu este practic să existe grade diferite pentru punctele de acces gestionate de un singur sistem de control al accesului, este permis să existe mai multe sisteme de control al accesului separate. Un punct de acces nu trebuie să fie controlat de mai mult de un sistem separat de control al accesului.

Următoarele linii directoare prezentate în SR EN 60839-11-2+AC:2016 sunt utile pentru punctele de discuţie cu clientul pentru ca acesta să înţeleagă şi să răspundă nevoilor instalării finale; acestea nu sunt exhaustive şi nu sunt prezentate în niciun fel de ordine sau prioritate.

Se recomandă luarea în considerare a următoarelor elemente:

- recomandările producătorului;
- ameninţarea (ameninţările);
- bunurile specifice care necesită protecţie;
- activităţile desfăşurate la amplasament/clădire;
- filozofia măsurii controlului accesului;
- gradul de securitate pentru fiecare punct de acces;
- fluxul de utilizatori (numărul de persoane într-o perioadă de timp);
- funcţionarea sistemului de control al accesului în condiţii de defecţiune (de exemplu, necesitatea unei a doua surse de alimentare, infrastructura cablurilor echipamentelor, pierderea comunicaţiei etc.);
- controlul accesului pentru utilizatorii cu dizabilităţi;
- cerinţele de securitate (de exemplu, ieşirile de urgenţă, protecţia împotriva incendiilor etc.);
- condiţiile de mediu şi CEM ale amplasamentului;
- redundanţa, planurile de recuperare în caz de dezastru pentru consola de monitorizare;
- amplasarea echipamentului (unitatea de control, interfaţa utilizatorului, consola de monitorizare);
- cooperarea utilizatorilor (motivare, instruire etc.);
- formarea operatorilor;
- traseele de cablu, tipul de cablu, lungimea maximă a cablului;
- metoda de raportare a alarmei/alertei.

Elementele proiectării unui sistem de securitate includ:

Desene - acestea sunt "inima" proiectului pentru că ilustrează conceptele proiectantului despre modul în care sistemul ar trebui să se raporteze la clădire și relația dintre dispozitive și mediul lor fizic (planuri, elevații și detalii fizice).
Specificații - dacă desenele sunt "inima" proiectului, specificațiile sunt "capul" acestuia și ar trebui să includă o descriere a ceea ce presupune proiectul; descrieri ale întregului sistem integrat și ale fiecărui subsistem, o descriere a serviciilor pe care contractorul le va furniza, etc.
Coordonare interdisciplinară - determină dacă un proiect funcționează conform intenției sau nu și dacă integratorul realizează un profit sau o pierdere.
Selectarea produsului - aici proiectantul are libertatea dar mai ales datoria de a face ceea ce este în interesul clientului său. Dacă acesta este pus sub presiune pentru a alege un producător sau altul, proprietarul va avea de suferit.
Managementul de proiect - aici, managementul proiectului se referă la livrarea unui proiect care să răspundă nevoilor clientului, integratorului și managerului de proiect al clientului. De regulă, proiectantul trebuie să facă toate acestea în timp ce lucrează la alte proiecte; trebuie să furnizeze livrabilele proiectului la timp și să mulțumească toate părțile.
Managementul clientilor - este procesul de gestionare a relației dintre firma pe care o reprezentați și reprezentantul clientului. Cel mai important aspect al unui bun management al clienților este menținerea proiectului la sfera sa de aplicare, la program și la buget.

PUNCTE DE ACCES ȘI INTERFAȚA CU ALTE SISTEME

Pentru instalarea şi operarea adecvată a punctelor de acces, se recomandă ca în procesul de proiectare să fie luate în considerare următoarele elemente:

- cerinţele pentru indicare;
- funcţionarea în condiţii de defecţiune;
- alţi factori relevanţi (de exemplu, riscul de vandalism etc.);
- rezistenţa fizică;
- structura clădirii înconjurătoare;
- selectarea dispozitivelor de acţionare a punctului de acces adecvate, adică a încuietorilor, a uşilor (nivelul de securitate, aspectul, mediul de funcţionare, timpii de răspuns operaţional, cerinţele pentru a se potrivi structurii existente);
- cerinţele de securitate (de exemplu, ieşirile de urgenţă, protecţia împotriva incendiilor etc.);
- monitorizarea punctului de acces;
- detectarea/prevenirea încercării a două sau mai multe persoane să intre simultan (adică singularizarea);
- metoda de revenire a punctului de acces la starea închis (de exemplu, echipament automat de închidere a uşii);
- configuraţia de funcţionare în caz de întrerupere a alimentării cu energie electrică (cu deschidere intrinsecă, cu blocare intrinsecă ...);
- măsurile pentru persoanele cu dizabilităţi;
- măsurile specifice pentru manipularea livrărilor;
- clasificarea de securitate pentru punctele de acces care conduc la acelaşi perimetru controlat din punct de vedere al securității;
- măsurile suplimentare de recunoaştere/detectare (greutatea, detecţia metalelor, comparaţia imaginilor, inspecţia vizuală etc.);
- anti-passback-ul (logic, temporizat, controlat);
- neutralizarea;
- alarma de constrângere;
- condiţia de acces doi utilizator;
- verificarea prezenţei.

Interfața cu alte sisteme

Atunci când este necesar să se interconecteze sistemul EACS cu alte sisteme, cum ar fi sistemele de alarmă la efracţie, sistemele de supraveghere video, sistemele de administrare, interfonul, controlul ascensorului etc., se recomandă să fie luate în considerare următoarele aspecte:

- tipul de legături de comunicaţii, disponibilitatea dorită, fiabilitatea şi securitatea datelor transmise asociate acestor legături
- cerințele privind infrastructura de rețea
- comenzile specifice de funcționare, de exemplu, apelul pentru ascensor, selectarea etajului şi a destinaţiei
- comenzile de raportare asociate controlului liftului

IX. INSTALAREA EACS

Înainte de începerea lucrului, se recomandă să fie luate în considerare toate cerinţele de securitate relevante.

Metodele de instalare electrică trebuie să respecte reglementările naţionale şi locale în vigoare.

Se recomandă instalarea componentele sistemului EACS în locaţii care să asigure o securitate adecvată a funcţionării şi să permită accesul facil pentru întreţinere şi service.

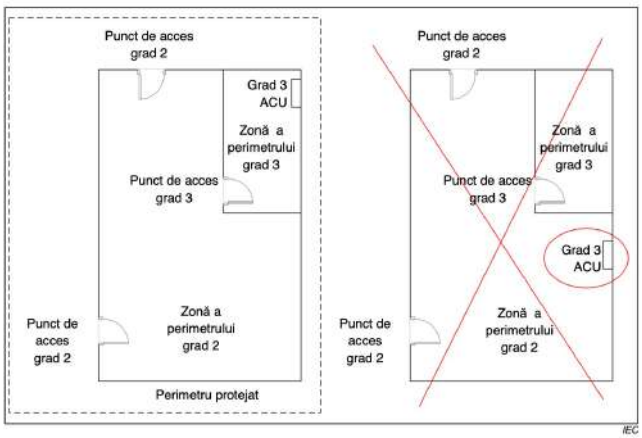
Se recomandă ca toate componentele sistemului să fie adecvate condiţiilor de mediu în care urmează să funcţioneze.

În timpul selecţiei componentelor se recomandă să se asigure compatibilitatea tuturor componentelor sistemului. În caz de incertitudine, se recomandă să aibă loc o consultare adecvată, de exemplu, cu producătorul componentelor, furnizorul, laboratorul de încercare sau altă terţă parte relevantă.

Rezultatele evaluării riscurilor trebuie să determine gradele de securitate ale zonelor din perimetrul protejat. Punctele de acces la zonele respective trebuie să fie de acelaşi grad sau mai mare. Pentru fiecare zonă de perimetru pot fi definite niveluri de acces separate.

Cu excepţia interfeţei cu utilizatorul, echipamentele critice pentru integritatea de securitate a sistemului de control al accesului nu trebuie să fie amplasate într-o zonă desemnată ca având un grad de securitate inferior celui mai înalt grad al perimetrului protejat pe care îl controlează.

SR EN 60839-11-2+AC:2016



Instalatorul trebuie să aducă la cunoştinţă proprietarului sistemului orice funcţionalitate particulară care trebuie pusă în aplicare pentru a îndeplini măsurile organizatorice şi constructive care sunt necesare pentru buna funcţionare a EACS. De exemplu, se recomandă detectarea/prevenirea încercării a două sau mai multe persoane să intre simultan (singularizare) pentru punerea în aplicare a măsurilor împotriva trecerii multiple.

Se recomandă să se ia în considerare ca pozarea cablurilor să se facă numai în perimetrul protejat

Echipamentul trebuie să fie instalat în conformitate cu instrucţiunile producătorului de personal instruit corespunzător. Dacă nu este posibilă instalarea unei componente în conformitate cu recomandările producătorului, se recomandă să se solicite sfatul producătorului şi acest lucru să fie înregistrat în documentaţia conformă cu execuţia.

Atunci când EACS utilizează infrastructura de comunicaţie (reţea) existentă la locaţia clientului, se recomandă să se acorde atenţie asigurării unor capacităţi, performanţe şi măsuri de protecţie suficiente care să permită buna funcţionare a EACS pentru gradul de securitate selectat.

Se recomandă ca sursele cu conexiune la reţeaua de alimentare să utilizeze un circuit electric dedicat, protejat separat.

Trebuie să se acorde atenţie cerinţelor de alimentare de rezervă ale EACS instalat şi componentelor reţelei sale de comunicaţii asociate.

RECOMANDĂRI PRIVIND INSTALAREA EACS

Cablare

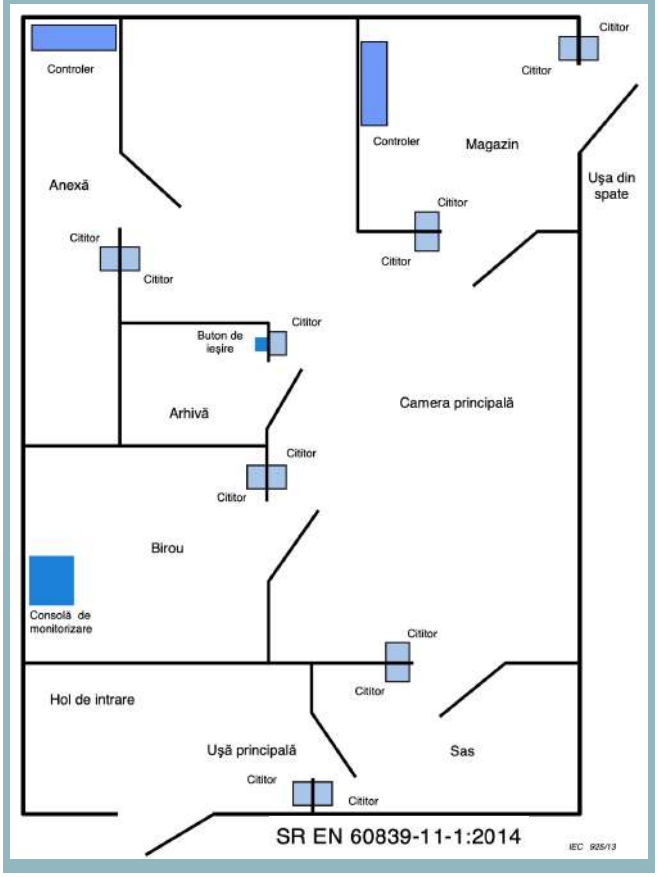
Traseele de cabluri trebuie să fie selectate pentru a asigura cea mai scurtă distanţă practică între poziţiile echipamentului. Acolo unde cablurile sunt pozate prin structura construcţiei, trebuie să se asigure menţinerea clasificării la incendiu a clădirii.

Se recomandă să se ia în considerare posibilitatea unei viitoare extinderi a sistemului şi a oricărei modificări probabile a clădirii/sitului.

Tipurile de cabluri trebuie să fie selectate pentru a minimiza căderea tensiunii şi pierderile de semnal şi pentru a respecta specificaţiile de mediu, siguranţă şi securitate. Se recomandă să nu fie depăşite valorile curenţilor admisibili şi, ori de câte ori este posibil, să fie prevăzute marje de siguranţă adecvate.

Se recomandă instalarea cablurilor în zone controlate din punct de vedere al securităţii şi, ori de câte ori este posibil, se recomandă să fie ascunse sau să nu să fie uşor accesibile.

Alimentarea cu energie electrică a fiecărei componente a unui sistem EACS instalat în afara perimetrului pe care îl controlează trebuie să fie protejată împotriva condiţiilor de scurtcircuit.



Considerații privind instalarea echipamentelor EACS

Instalatorul trebuie să cunoască modul în care echipamentele interacționează cu mediul lor, cum ar fi montarea cititoarelor de carduri pe o clădire de oțel într-un mod care să nu le provoace supraîncălzirea, de exemplu. Iată și alte exemple:

- Asigurați-vă că utilizați încuietoarea corectă pentru tipul de ușă. Acest lucru este deosebit de important dacă ușa este rezistentă la foc sau este o ușă de ieșire împotriva incendiilor.
- Asigurați-vă că utilizați rezistoare de capăt de linie adecvate pe toate dispozitivele de alarmă.
- ATENȚIE! Atunci când utilizați funcția de comutator de poziție a ușii integrată a unei încuietori magnetice, aceasta nu vă spune că ușa este închisă, ci doar că este încuiată.
- După instalarea și cablarea dispozitivelor începe testarea sistemului. Primul pas este testarea conectivității. Fiecare dispozitiv apare pe computer sau pe panoul de monitorizare la care este conectat? Toate dispozitivele de detectare a alarmei afișează toate cele patru stări de alarmă? Funcționează toate încuietorile? Toate dispozitivele "Request-to-Exit" deblochează ușile? Toate cititoarele de carduri funcționează cu un card de probă?

Verificați și/sau reglați:

- alimentarea și împământarea corespunzătoare a tuturor dispozitivelor;
- integritatea tuturor izolațiilor, a terminațiilor de ecranare și a conexiunilor;
- integritatea conexiunilor lipite;
- dacă toate cablurile sunt protejate corespunzător;
- continuitatea și funcționarea tuturor circuitelor;
- integritatea mecanică și estetica tuturor dispozitivelor montate;
- dacă toate dispozitivele care trebuie pornite sau oprite într-o anumită secvență sunt configurate pentru a face acest lucru;
- toate dispozitivele pentru o funcționare optimă și documentați ajustările.

X. PUNEREA ÎN FUNCȚIUNE ȘI PREDAREA EACS

Punerea în funcțiune a EACS

Instalatorul trebuie să cunoască modul în care echipamentele interacționează cu mediul lor, cum ar fi montarea cititoarelor de carduri pe o clădire de oțel într-un mod care să nu le provoace supraîncălzirea, de exemplu. Iată și alte exemple:

- Asigurați-vă că utilizați încuietoarea corectă pentru tipul de ușă. Acest lucru este deosebit de important dacă ușa este rezistentă la foc sau este o ușă de ieșire împotriva incendiilor.
- Asigurați-vă că utilizați rezistoare de capăt de linie adecvate pe toate dispozitivele de alarmă.
- ATENȚIE! Atunci când utilizați funcția de comutator de poziție a ușii integrată a unei încuietori magnetice, aceasta nu vă spune că ușa este închisă, ci doar că este încuiată.
- După instalarea și cablarea dispozitivelor începe testarea sistemului. Primul pas este testarea conectivității. Fiecare dispozitiv apare pe computer sau pe panoul de monitorizare la care este conectat? Toate dispozitivele de detectare a alarmei afișează toate cele patru stări de alarmă? Funcționează toate încuietorile? Toate dispozitivele "Request-to-Exit" deblochează ușile? Toate cititoarele de carduri funcționează cu un card de probă?

Scopul procesului de punere în funcţiune este de a confirma că sistemul instalat corespunde cerinţelor proiectului sistemului.

Se recomandă ca procedura de punere în funcţiune să fie convenită în scris între proprietarul sistemului şi alte părţi interesate.

Se recomandă să fie efectuată o inspecţie vizuală amănunţită pentru a se asigura că instalaţia, metodele, materialele şi componentele utilizate respectă instrucţiunile de proiectare a sistemului şi că documentaţia conformă cu execuţia (inclusiv desenele înregistrate, instrucţiunile de exploatare şi excepţiile convenite) corespund cu instalaţia reală.

Verificați și/sau reglați:

- alimentarea și împământarea corespunzătoare a tuturor dispozitivelor;
- integritatea tuturor izolațiilor, a terminațiilor de ecranare și a conexiunilor;
- integritatea conexiunilor lipite;
- dacă toate cablurile sunt protejate corespunzător;
- continuitatea și funcționarea tuturor circuitelor;
- integritatea mecanică și estetica tuturor dispozitivelor montate;
- dacă toate dispozitivele care trebuie pornite sau oprite într-o anumită secvență sunt configurate pentru a face acest lucru;
- toate dispozitivele pentru o funcționare optimă și documentați ajustările.

Predarea sistemului

Predarea sistemului reprezintă transferul oficial al responsabilităţii de la societăţile de proiectare şi instalare către proprietarul sistemului. Se recomandă definirea clară a condiţiilor de predare ale sistemului între aceste părţi.

Se recomandă să se furnizeze o demonstraţie completă a EACS şi să se ţină seama de următoarele aspecte:

a) documentaţia;
b) instruire în managementul şi funcţionarea sistemului.

După finalizarea predării sistemului, se recomandă ca EACS să fie supus încercării pentru o perioadă de timp care va fi convenită cu proprietarul sistemului.

În această perioadă, se recomandă ca EACS să fie utilizat normal.

De asemenea, este posibil ca perioada de încercare să fie efectuată ca parte a procesului de punere în funcţiune şi verificare înainte de predare.

XI. FUNCȚIONAREA ȘI ÎNTREȚINEREA EACS

Funcţionarea sistemului

Se recomandă să revină proprietarului sistemului responsabilitatea de a se asigura că:

a) utilizatorii şi operatorii sunt instruiţi;

b) sunt furnizate instrucţiuni pentru utilizatori şi operatori;

c) utilizatorii sunt instruiţi şi motivaţi în legătură cu securitatea amplasamentului;

d) sunt respectate procedurile de administrare a sistemului şi de back-up al datelor;

e) datele de sistem sunt actualizate;

f) oricărei alerte îi este furnizat răspunsul corect;

g) sunt îndeplinite cerinţele naţionale de reglementare aplicabile;

h) este organizată întreţinerea regulată a sistemului;

i) există măsuri organizatorice în caz de defectare a EACS.

Se recomandă ca societatea de instalare/întreţinere să informeze proprietarul sistemului cu privire la responsabilităţile sale de gestionare.

Întreţinerea sistemului

Pentru a se asigura funcţionarea corectă a EACS, se recomandă ca acesta să fie inspectat şi deservit la intervale convenite, de exemplu, de două ori pe an sau dacă este disponibilă diagnosticarea la distanţă, intervalul de inspecţie şi de deservire poate fi redus la o dată pe an.

Se recomandă ca acordurile de întreţinere să fie făcute înainte ca EACS să fie pus în funcţiune.

Se recomandă să fie încheiat un acord privind nivelul serviciului de întreţinere cu o organizaţie competentă pentru inspecţie şi deservire. Se recomandă ca întreţinerea să fie efectuată numai de persoane instruite corespunzător şi competente în activităţile necesare pentru inspecţia şi deservirea sistemului.

Pot fi utilizate diferite tipuri de aranjamente de întreţinere, de exemplu:

- procedura (procedurile) de inspecţie - acţiunea limitată la o verificare de diagnosticare a sistemului;
- procedura (procedurile) de deservire - inspecţie urmată de repararea sau înlocuirea părţilor defecte ale sistemului;

Se recomandă ca procedurile de inspecţie şi deservire să fie furnizate şi documentate de producătorul componentei sau de către instalator.

Se recomandă ca inspecţia şi deservirea să fie efectuate de către organizaţia competentă în conformitate cu aceste proceduri şi să includă inspecţia funcţionării punctelor de acces.

În cazul în care există indicii privind funcţionarea defectuoasă (sau posibile defecţiuni viitoare) a sistemului sau deteriorarea oricărei părţi a sistemului, se recomandă informarea imediată a organizaţiei competentă pentru inspecţie şi deservire.

Se recomandă să se furnizeze un registru al sistemului pentru a se înregistra toate defecţiunile sistemului, acţiunile de întreţinere şi detaliile privind orice modificări sau adăugiri la EACS.

XII. TENDINȚE ȘI OPORTUNITĂȚI ÎN CONTROLUL ACCESULUI

Așa cum am am spus în prezentarea acestui ghid, ritmul schimbărilor tehnologice din ultimul deceniu este impresionant iar unii specialiști din domeniul securității nu se feresc să afirm că este chiar înfricoșător.

TEHNOLOGIA MOBILĂ ESTE UTILIZATĂ FRECVENT PENTRU CONTROLUL ACCESULUI.

Atât pentru managementul angajaților, cât și al vizitatorilor, acreditările pentru sistemele de control al accesului au folosit în mod tradițional carduri sau tag-uri de acces. În timp ce acestea nu sunt deloc o relicvă a unei epoci apuse, utilizarea smartphone-urilor și a dispozitivelor portabile devine o metodă din ce în ce mai populară de identificare și acces. Mai mulți producători și distribuitori de echipamente de control acces au subliniat că această tendință s-a accelerat în timpul pandemiei, deoarece managerii de securitate au căutat alternative de control al accesului fără atingere.

În mod esențial, tehnologia mobilă oferă o modalitate flexibilă de a emite și de a revoca acreditările, cu soluții unificate de gestionare a accesului la software care lucrează adesea mână în mână cu tehnologia.

BIOMETRIE PENTRU ACCES FĂRĂ CONTACT

Nu este surprinzător faptul că a existat o cerere din ce în ce mai mare pentru tehnologia de control al accesului, care permite utilizatorilor să intre și să se deplaseze într-o clădire fără a fi nevoie să atingă fizic vreunul dintre sisteme. Pe măsură ce guvernele din întreaga lume s-au concentrat pe reducerea contactului fizic între oameni pentru a reduce răspândirea coronavirusului; cu ușile și punctele de intrare acționând ca puncte de contact, managerii clădirilor au căutat tehnologii alternative.

Opțiunile fără atingere au fost o caracteristică a dezvoltării produselor și a marketingului producătorilor în 2020 și 2021. Deși o mare parte a tehnologiei exista deja, producătorii au acționat rapid pentru a evidenția beneficiile „covid-secure" ale implementării tehnologiei lor.

Recunoașterea facială, cititoarele de amprente, identificarea irisului și chiar amprentele audio sunt toate opțiuni viabile pentru a se integra acum cu un sistem de acces.

ROLUL ACCESULUI ÎN „CLADIRILE CONECTATE"

Evaluând răspunsurile producătorilor de control al accesului, supraveghere video și alarmă de intruziune, există puține îndoieli în rândul industriei că influența și cererea pentru „cladiri conectate" va crește.

Ce înțelegem mai exact prin „cladirea conectată"? În acest caz, ne referim la clădiri și spații (un campus universitar cu mai multe locații, de exemplu) care integrează mai multe funcții diferite ale clădirii, adesea operate dintr-un sistem unificat de management al clădirii. Termenul „clădiri inteligente" poate fi, de asemenea, utilizat, deși există încă dezbateri cu privire la utilizarea „inteligenței" în industria securității, unde vulnerabilitățile cibernetice ale dispozitivelor IoT interconectate continuă să ridice îngrijorări.

ACCESUL - PRIMUL PAS CĂTRE CLĂDIRILE CONECTATE

Producătorii s-au grăbit să identifice exact cât de important este controlul accesului în acest domeniu.

Sistemele integrate de securitate fizică, în general, sunt privite ca primul pas în proces.

Din motive de securitate, „identificarea persoanelor" este crucială, iar integrarea controlului accesului și a supravegherii video permite personalului să se asigure că acreditările utilizate corespund cu cele ale persoanei care le deține.

TENDINȚE, OPORTUNITĂȚI ȘI PROVOCĂRI ÎN CONTROLUL ACCESULUI

CLOUD-UL ȘI CONTROLUL ACCESULUI

Sistemele bazate pe "cloud", care funcționează în general pe un model de abonament recurent, oferă mai multe beneficii conform furnizorilor; deși educarea utilizatorilor finali și a integratorilor acestora rămâne o provocare.

BENEFICIILE ARHITECTURII BAZATE PE "CLOUD"

Un factor cheie în creștere, susțin mai mulți producători, este că organizațiile sunt acum destul de familiare cu un model bazat pe abonament, pe care se bazează în general un serviciu bazat pe "cloud". Costurile lunare permit departamentului de securitate să reducă și să distribuie cheltuielile pe o perioadă mai lungă de timp pentru o mai bună predictibilitate a bugetului.

DE CE NU TOATĂ LUMEA A TRECUT LA MANAGEMENTUL CONTROLULUI ACCESULUI BAZAT PE "CLOUD"?

Educația, se pare, are o contribuție semnificativă la obținerea unei mai mari acceptări a modului în care soluțiile "cloud" pot sprijini operațiunile de afaceri.

Aproape toți participanții la sondajul IFSEC Global au evidențiat că majoritatea clienților de astăzi nu înțeleg prea bine beneficiile accesului controlat și se tem de "cloud din cauza securității datelor.

Ei au remarcat că mulți nu își dau seama de rentabilitatea afacerii care le-ar putea aduce un management centralizat al facilităților și al sistemului de acces, cum ar fi o mai bună conștientizare a zonelor aglomerate și un control mai mare asupra fluxului de ocupanți pe parcursul zilei.

Prejudiciul reputației cauzat de o încălcare a datelor ar putea fi catastrofal pentru astfel de furnizori de servicii în "cloud", având drept rezultat protecția perimetrului, protocoalele stricte de securitate și echipele dedicate de apărare cibernetică.

OPORTUNITĂȚILE VIITORULUI ÎN CONTROLUL ACCESULUI

CUM SE VOR SCHIMBA CERINȚELE CLIENȚILOR?

Producătorii prevăd o schimbare continuă către clădiri mai integrate și inteligente, în care controlul accesului poate fi privit ca „declanșator", sau cel puțin în a juca un rol central în automatizarea proceselor de management al clădirilor.

Rolul „integratorului de securitate" se va transforma, pentru că acest loc de muncă presupune integrarea și instalarea sistemelor de securitate fizică dar va include și pe cea a altor platforme BMS, cum ar fi HVAC, dispozitive de iluminat și de alertă la incendiu.

Mai mulți producători au remarcat, de asemenea, probabilitatea unei implicări mai mari din partea diferitelor părți interesate în achizițiile și specificarea controlului accesului. În special dacă sistemele sunt conectate la rețea sau legate de un furnizor extern bazat pe "cloud", profesioniștii IT vor continua să aibă influență asupra deciziilor de cumpărare a sistemelor de securitate – lucru pe care furnizorii, integratorii și consultanții vor trebui să-l ia în considerare în soluțiile propuse.

O MUTARE CĂTRE SOLUȚII DE ACCES "VERTICAL-SPECIFIC"?

Câțiva furnizori au evidențiat o creștere deosebită a cererii pentru soluții de acces mai avansate pe piața rezidențială (în special în Statele Unite).

Se spune că proprietarii de proprietăți imobiliare multirezidențiale caută tehnologii de construcții și sisteme de interfonie mai inteligente, cu o abordare „centrată pe aplicații", pentru a impresiona potențialii rezidenți, în timp ce există și o creștere a achizițiilor de încuietori inteligente electronice.

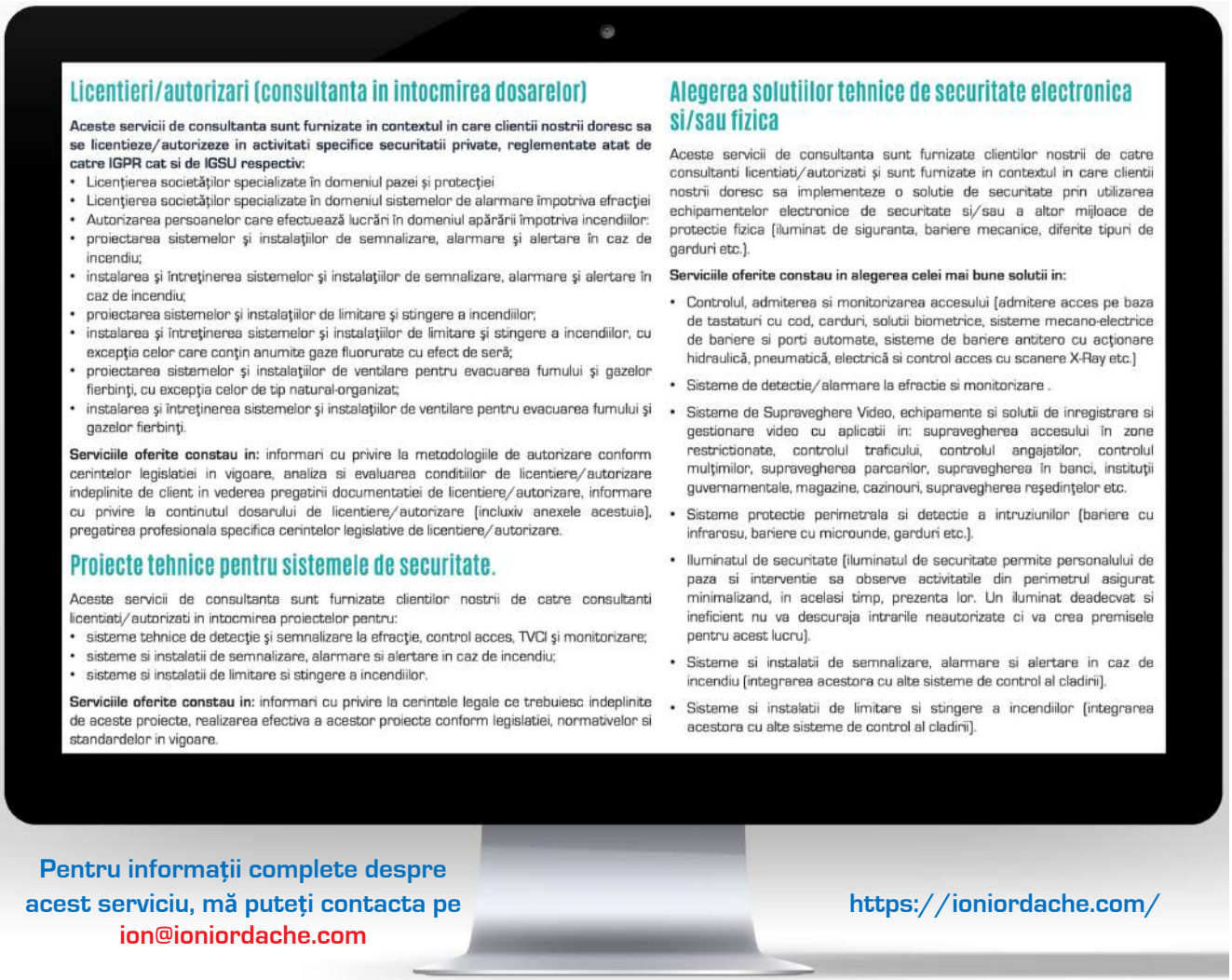
Pentru multe clădiri mici și mijlocii, încuietorile electronice de sine stătătoare care se conectează la aplicații software și nu necesită conectivitate hardware pentru a funcționa, vor rămâne o alegere populară.

Transportul, de asemenea, pare a fi o verticală în creștere. Principalele gări, auto-gări și aeroporturile formează o verigă cheie în lanțul „orașului inteligent" care necesită o tehnologie de securitate mai sofisticată pentru controlul accesului fizic care poate oferi puncte suplimentare de captare a datelor.

Materialul acestui capitol a fost preluat din lucrarea "**Trends, opportunities and challenges in Physical Access Control**" elaborată de IFSEC Global în 2021.

XIII. CONSULTANȚA

Metodologia de consultanță de securitate "Security Management Solutions" (SMS) propusa de **iQuality Services** este o alternativa la modelul traditional de management al securitatii ce ofera o serie de soluții la problemele companiilor de securitate.



Licentieri/autorizari (consultanta in intocmirea dosarelor)

Aceste servicii de consultanta sunt furnizate in contextul in care clientii nostrii doresc sa se licentieze/autorizeze in activitati specifice securitatii private, reglementate atat de catre IGPR cat si de IGSU respectiv:

- Licențierea societăților specializate în domeniul pazei și protecției
- Licențierea societăților specializate în domeniul sistemelor de alarmare împotriva efracției
- Autorizarea persoanelor care efectuează lucrări în domeniul apărării împotriva incendiilor:
- proiectarea sistemelor și instalațiilor de semnalizare, alarmare și alertare în caz de incendiu;
- instalarea și întreținerea sistemelor și instalațiilor de semnalizare, alarmare și alertare în caz de incendiu;
- proiectarea sistemelor și instalațiilor de limitare și stingere a incendiilor;
- instalarea și întreținerea sistemelor și instalațiilor de limitare și stingere a incendiilor, cu excepția celor care conțin anumite gaze fluorurate cu efect de seră;
- proiectarea sistemelor și instalațiilor de ventilare pentru evacuarea fumului și gazelor fierbinți, cu excepția celor de tip natural-organizat;
- instalarea și întreținerea sistemelor și instalațiilor de ventilare pentru evacuarea fumului și gazelor fierbinți.

Serviciile oferite constau in: informari cu privire la metodologiile de autorizare conform cerintelor legislatiei in vigoare, analiza si evaluarea conditiilor de licentiere/autorizare indeplinite de client in vederea pregatirii documentatiei de licentiere/autorizare, informare cu privire la continutul dosarului de licentiere/autorizare (incluxiv anexele acestuia), pregatirea profesionala specifica cerintelor legislative de licentiere/autorizare.

Proiecte tehnice pentru sistemele de securitate.

Aceste servicii de consultanta sunt furnizate clientilor nostrii de catre consultanti licentiati/autorizati in intocmirea proiectelor pentru:

- sisteme tehnice de detecție și semnalizare la efracție, control acces, TVCI și monitorizare;
- sisteme si instalatii de semnalizare, alarmare si alertare in caz de incendiu;
- sisteme si instalatii de limitare si stingere a incendiilor.

Serviciile oferite constau in: informari cu privire la cerintele legale ce trebuiesc indeplinite de aceste proiecte, realizarea efectiva a acestor proiecte conform legislatiei, normativelor si standardelor in vigoare.

Alegerea solutiilor tehnice de securitate electronica si/sau fizica

Aceste servicii de consultanta sunt furnizate clientilor nostrii de catre consultanti licentiati/autorizati și sunt furnizate in contextul in care clientii nostrii doresc sa implementeze o solutie de securitate prin utilizarea echipamentelor electronice de securitate si/sau a altor mijloace de protectie fizica (iluminat de siguranta, bariere mecanice, diferite tipuri de garduri etc.).

Serviciile oferite constau in alegerea celei mai bune solutii in:

- Controlul, admiterea si monitorizarea accesului (admitere acces pe baza de tastaturi cu cod, carduri, solutii biometrice, sisteme mecano-electrice de bariere si porti automate, sisteme de bariere antitero cu acționare hidraulică, pneumatică, electrică si control acces cu scanere X-Ray etc.)
- Sisteme de detectie/alarmare la efractie si monitorizare .
- Sisteme de Supraveghere Video, echipamente si solutii de inregistrare si gestionare video cu aplicatii in: supravegherea accesului în zone restrictionate, controlul traficului, controlul angajatilor, controlul mulțimilor, supravegherea parcarilor, supravegherea în banci, instituții guvernamentale, magazine, cazinouri, supravegherea reședințelor etc.
- Sisteme protectie perimetrala si detectie a intruziunilor (bariere cu infrarosu, bariere cu microunde, garduri etc.).
- Iluminatul de securitate (iluminatul de securitate permite personalului de paza si interventie sa observe activitatile din perimetrul asigurat minimalizand, in acelasi timp, prezenta lor. Un iluminat deadecvat si ineficient nu va descuraja intrarile neautorizate ci va crea premisele pentru acest lucru).
- Sisteme si instalatii de semnalizare, alarmare si alertare in caz de incendiu (integrarea acestora cu alte sisteme de control al cladirii).
- Sisteme si instalatii de limitare si stingere a incendiilor (integrarea acestora cu alte sisteme de control al cladirii).

Pentru informații complete despre acest serviciu, mă puteți contacta pe ion@ioniordache.com

https://ioniordache.com/

Managementul proiectelor de securitate fizică

Aceste servicii de consultanta sunt furnizate in contextul in care clientii nostrii accepta si inteleg importanta managementului de securitate fizică pe care le desfasoara si doresc sa faca acest lucru utilizand o metodologie moderna de management al proiectelor.

Serviciile oferite constau in consultanta si sprijin direct in urmatoarele grupe de procese:

1. initiere;
2. planificare;
3. executie;
4. monitorizare si control;
5. incheierea.

XIV. FORMAREA PROFESIONALĂ

RQM CERT, furnizor de formare profesională organizează în România atât cursuri acreditate de **Autoritatea Națională pentru Calificări (ANC)** în baza Standardelor Ocupaționale și a Programelor Cadru cât și cursuri ca provider pentru **PECB** („PECB Group Inc.") care este un organism internațional de educație și certificare în conformitate cu ISO/IEC 17024 pentru programele de certificare a personalului.

https://rqmcert.com

Responsabil cu protecția datelor cu caracter personal

(Cod COR: 242231)

Certificat de absolvire eliberat de Ministerul Muncii și Protecției Sociale și Ministerul Educației.

https://rqmcert.com

GDPR - Foundation

Certificat de absolvire eliberat de **PECB**.

Curs de formare introductiv care vă permite să înțelegeți conceptele de bază și cerințele GDPR.

- Înțelegeți conceptele de bază și componentele protecției datelor.
- Înțelegeți principiile, provocările, problemele de protecție a datelor și importanța unui responsabil cu protecția datelor, a unui operator și a unui procesator.
- Înțelegeți conceptele, abordările, metodele și tehnicile pentru protecția eficientă a datelor.

https://rqmcert.com

PECB | Data Protection Officer

GDPR - Certified Data Protection Officer

Certificat de absolvire eliberat de **PECB**.

Cursul de formare vă permite să dobândiți cunoștințele și abilitățile necesare și să dezvoltați competența de a îndeplini rolul Responsabilului cu Protecția Datelor într-o implementare a programului de conformitate cu GDPR.

După ce ați trecut cu succes examenul, puteți solicita acreditarea ca

PECB Certified Data Protection Officer.

FORMAREA PROFESIONALĂ – SECURITATEA PRIVATĂ

În România, ocupațiile din domeniile sistemelor de securitate private și apărării împotriva incendiilor se află pe ˝Lista profesiilor și ocupațiilor pentru care există cerințe speciale la organizarea pregătirii profesionale˝ iar cursurile de formare profesională sunt organizate de către **RQM CERT**, furnizor de formare profesionala acredita de **Autoritatea Națională pentru Calificări (ANC)** în baza Standardelor Ocupaționale și a Programelor Cadru avizate de către **Inspectoratul General al Poliției Române (I.G.P.R.)** și/sau **Inspectoratul General pentru Situații de Urgență (I.G.S.U.)**

Certificatele de competențe profesionale, eliberate de către Ministerul Muncii și Protecției Sociale și Ministerul Educației prin furnizorii de formare profesională acreditați de Autoritatea Națională pentru Calificări (ANC) fac parte din categoria actelor oficiale și sunt recunoscute la nivel național iar dacă sunt apostilate în cadrul instituției prefectului și traduse sunt recunoscute și la nivel internațional.

https://rqmcert.com

Manager de securitate
(Cod COR: 121306)

Certificat de absolvire eliberat de Ministerul Muncii și Protecției Sociale și Ministerul Educației.

Activitatea managerului de securitate cuprinde: Securitatea Fizică * Securitatea personalului * Securitatea documentelor clasificate * Securitatea Industrială * Securitatea Sistemelor Informatice și de Comunicații (INFOSEC) și Instruirea și educația preventivă a personalului.

https://rqmcert.com

Evaluator de risc la securitatea fizică
(Cod COR: 242115)

Certificat de absolvire eliberat de Ministerul Muncii și Protecției Sociale și Ministerul Educației.

Analiza de risc la securitatea fizică constituie fundamentul adoptării măsurilor de securitate a obiectivelor, bunurilor şi valorilor prevăzute de lege, transpuse în planul de pază şi proiectul sistemului de alarmare. Obținerea certificatului de absolvire vă va permite să solicitați înscrierea în Registrul Național al Evaluatorilor de Risc la Securitate Fizică (RNERSF)

FORMAREA PROFESIONALĂ – SECURITATEA PRIVATĂ

RQM CERT
Your Knowledge Provider

Furnizor de formare profesionala acredit de Autoritatea Națională pentru Calificări (ANC)

https://rqmcert.com

Proiectant sisteme de securitate
(Cod COR: 215119)

Certificat de absolvire eliberat de Ministerul Muncii și Protecției Sociale și Ministerul Educației.

Modului I - Proiectarea sistemelor tehnice de detecție și semnalizare la afracție și control acces, TVCI și monitorizare

Modului II - Proiectarea sistemelor tehnice de detecție și alarmare la incendiu/Proiectarea instalațiilor pentru stingere automată a incendiului/Proiectarea sistemului de control și evacuare a fumului și gazelor fierbinți din construcții și de limitare a propagării fumului în caz de incendiu.

https://rqmcert.com

Tehnician Sisteme de Detecție, Supraveghere Video, Control Acces
(Cod COR: 352130)

Certificat de absolvire eliberat de Ministerul Muncii și Protecției Sociale și Ministerul Educației.

Obținerea certificatului de absolvire este obligatorie dacă intenționați să vă licențiați/autorizați propria companie la I.G.P.R./I.G.S.U. sau să lucrați în cadrul unor companii licențiate de I.G.P.R. pentru ˝instalarea, modificarea, monitorizarea, întreținerea și utilizarea sistemelor de alarmare împotriva efracției˝ sau autorizate de I.G.S.U. pentru ˝instalarea și întreținerea sistemelor și instalațiilor de semnalizare, alarmare și alertare în caz de incendiu˝.

https://rqmcert.com

Tehnician sisteme și instalații de limitare și stingere a incendiilor
(Cod COR: 742106)

Certificat de absolvire eliberat de Ministerul Muncii și Protecției Sociale și Ministerul Educației.

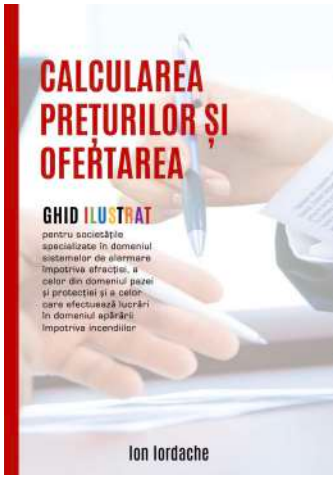
Obținerea certificatului de absolvire este obligatoriu dacă intenționați să vă autorizați propria companie la I.G.S.U. sau să lucrați în cadrul unor companii autorizate de I.G.S.U. pentru ˝instalarea si intretinere a sistemelor si instalatiilor de limitare si stingere a incendiilor, cu exceptia celor care contin anumite gaze fluorurate cu efect de sera.˝

XV. BIBLIOGRAFIE

- SR EN 60839-11-2+AC:2016 - Sisteme de alarmă şi de securitate electronică. Partea 11-2: Sisteme electronice de control al accesului. Linii directoare pentru aplicaţii
- SR EN 60839-11-1:2014 - Sisteme de alarmă şi de securitate electronică. Partea 11-1: Sisteme electronice de control al accesului. Cerinţe pentru sistem şi componente
- LEGEA nr. 333 din 8 iulie 2003 privind paza obiectivelor, bunurilor, valorilor şi protecţia persoanelor (republicată și actualizată)
- HOTĂRÂREA nr. 301 din 11 aprilie 2012 pentru aprobarea Normelor metodologice de aplicare a Legii nr. 333/2003 privind paza obiectivelor, bunurilor, valorilor şi protecţia persoanelor (actualizată)
- Electronic Access Control, 2nd Edition, by Thomas L. Norman
- Integrated Security Systems Design: A Complete Reference for Building Enterprise-Wide Digital Security Systems, 2nd Edition, by Thomas L. Norman
- Security Design Consulting: The Business of Security System Design 1st Edition, by Brian Gouin
- The Complete Guide to Physical Security 1st Edition, by Paul R. Baker & Daniel J. Benny
- Trends, opportunities and challenges in Physical Access Control (2021), by IFSEC Global
- Suport de curs "Tehnician pentru Sisteme de Detectie, Supraveghere Video, Control Acces" Cod COR: 352130, V.1. 2022, by RQM Certification

GHIDURI ILUSTRATE

DOWNLOAD GRATUIT!



https://ioniordache.com

Autori:

Ion Iordache, BEc

Consultant de Securitate,
Data Protection Officer (DPO) și Training & Development Manager la RQM Cert,
CEO și fondator la
Iordache Quality Services (iQS),
companii care oferă servicii de consultanță și cursuri de formare în managementul securității, GDPR și sisteme de management bazate pe standardele internaționale ISO.

www.ioniordache.com

ion@ioniordache.com

Adrian Marian Fleacă, Ing

Inginer electronist cu specializări și experiență profesională în domeniului sistemelor de securitate private (evaluarea riscurilor la securitatea fizică, proiectarea, instalarea și întreținerea sistemelor electronice de securitate).

ady_sibiu77@yahoo.com

DATA ȘI VERSIUNEA 01.05.2022, V.00

Copii ale celei mai recente versiuni ale acestui ghid pot fi descărcate de pe https://ioniordache.com.

Dacă aveți nevoie de informații suplimentare, asistență sau recomandări cu privire la conținutul acestui document, vă rog să mă contactați la ion@ioniordache.com.

RQM Certification

RQM Certification cu sediul în Timișoara este un furnizor de formare profesională cu o echipă excepțională de specialiști cu mare experiență în formare profesională, servicii de evaluare și audit. Compania are expertiză în domeniul sistemelor de management al calității, al mediului, al sănătății și securității la locul de muncă, al automobilelor, al securității fizice, al informațiilor și al serviciilor IT. Programele de formare sunt concepute pentru a sprijini învățarea activă în conformitate cu standardele internaționale și cerințele specifice fiecărei industrii.

www.rqmcert.com

office@rqmcert.com

+40 356 173 020