ORGANIZATORI

ARTS
Arta de a trăi în siguranță
Asociație de utilitate publică

ANERSFR

SPONSOR OFICIAL

ENVIO
Let us protect your business!

PARTENER SILVER

SIEL INVEST
SECURITY EXPRESS CENTER

ASOCIAŢII PARTENERE

ARISI
ASOCIAȚIA ROMÂNĂ A INGINERILOR DE SECURITATE LA INCENDIU

ASI
Asociația pentru Securitate la Incendiu

FEDERAȚIA SERVICIILOR DE SECURITATE

DE 10 ANI ÎMPREUNĂ

PARTENERI MEDIA

Profesioniștii între ei
Conferințele Media Makers

rfi ROMÂNIA
FRANCE MÉDIAS MONDE

ibuild.info

proidea

Evaluarea riscului de securitate parte a planificării sistemelor

Riscurile de securitate induse de evoluția tehnologica

Outstanding Security Performance Awards WINNER 2018

SECANT security

Dimensionarea mecanismului de securitate

- Analiza riscurilor – nivelul amenințării, consecințele, modul de operare, elemente de vulnerabilitate, măsuri de control necesare
- Evaluarea modului de îndeplinire a cerințelor minimale din HG 301/2012

- Analiza amplasament
- Elaborare soluție tehnică – (sub)sisteme, (tele)comunicații, alimentare cu energie, specificare software
- Elaborare deviz, caiete sarcini etc.
- Elaborare manuale de utilizare
- Elaborare plan de calitate

- Dimensionarea unui mecanism de securitate – tehnic+servicii pază și intervenție+organizatoric - inclusiv estimarea costurilor pentru implementare
- Specifica Gradul de securitate

Planificarea - etapa a lucrarii

- identificarea legilor, reglementărilor şi standardelor relevante;
- termeni şi cerinţe în legătură cu contractul;
- diagrame (de exemplu, în forma unei diagrame funcţionale/diagrame bloc);
- rezultatul evaluării de risc;
- interfeţe cu alte servicii.

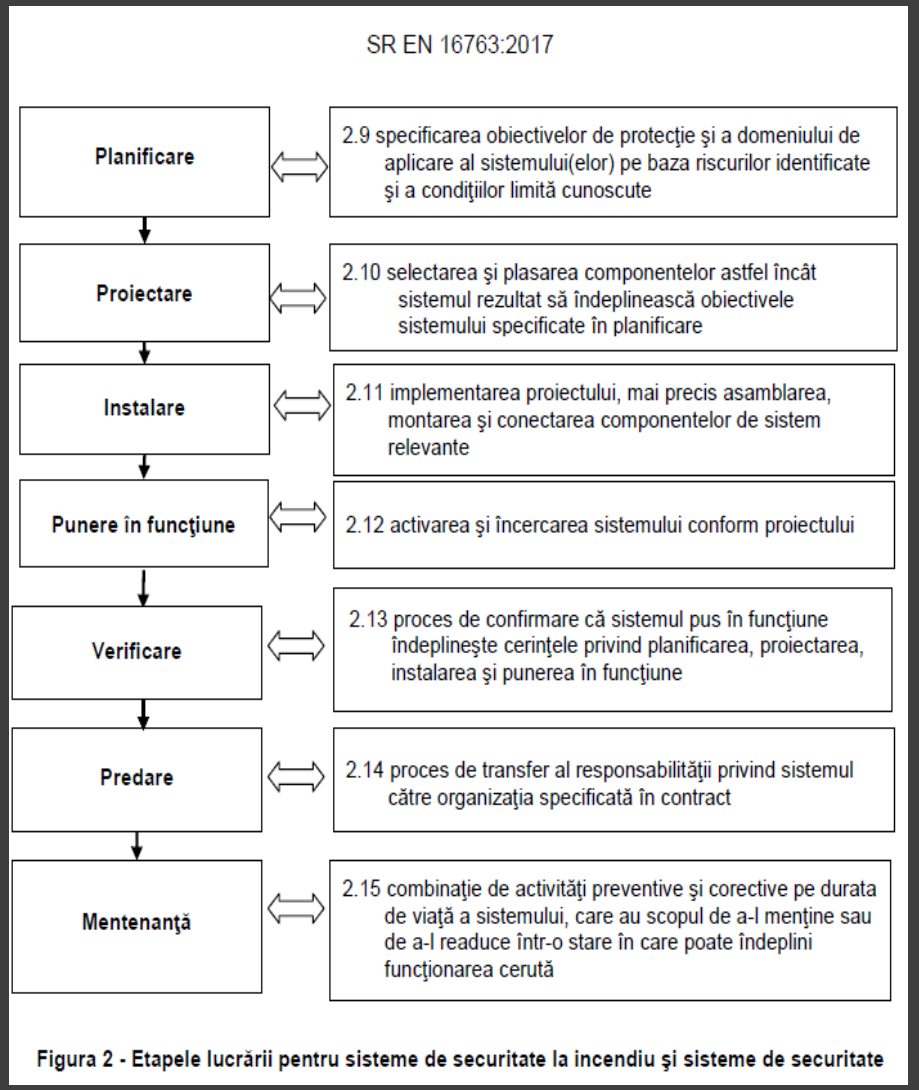


Figura 2 - Etapele lucrării pentru sisteme de securitate la incendiu şi sisteme de securitate

Planificarea – relatia cu analiza de risc

SR CLC/TS 50131-7 Sisteme de alarmă la efracţie şi jaf armat. Partea 7: Linii directoare pentru aplicaţii

SR EN IEC 60839-11-2 Sisteme electronice de control al accesului – Linii directoare pentru aplicații

SR EN 62676-1-1 Sisteme de supraveghere video utilizate în aplicaţii de securitate. Cerinţe de sistem

CEN/TR 16705 Perimeter protection – Performance classification methodology

- Analiza de risc – stabilire Grad de securitate – implicit nivel de supraveghere
- Analiza amplasament – conținuturi, clădire, factori de influență din interior și din exterior
- Evaluarea riscurilor înainte de implementarea sistemului de control al accesului
- Gradele de securitate iau in considerare nivelul de risc care depinde de probabilitatea apariţiei unui incident şi daunele potenţiale cauzate de acesta
- Prima variabilă în evaluarea performanței unei protecții perimetrale este legată de riscuri, amenințări și vulnerabilități

Evaluator de risc sau proiectant?

- ✓ Competențe de management al riscului
- ✓ Competențe tehnice de securitate
- ✓ Capabilitatea de a întelege rapoartele de evaluare și tratare a riscului, respectiv proiectele tehnice de securitate
- ✓ Capacitate de comunicare cu beneficiarul
- ✓ Schimb de informații și perfecționare continuă

Our dependence of technology is growing faster than our ability to secure it – Scott Erven PwC

- Sisteme mult mai complexe – dispozitive care sunt in fapt computere (potențiale ținte)
- Rețele eterogene complexe
- Produse realizate pentru utilitate temporara – oamenii nu solicită securitate
- Sistemele au interacțiune cu lumea fizică și pot conduce la impact real.

- Mașini care imită funcții cognitive ale creaturilor vii – învățarea, soluționarea problemelor
- Factori favorizatori:
  - Volume mari de date din care sistemele pot învăța – identifică pattern-uri, generalizează
  - Pot atinge acuratețea recunoșterii umane, pot rezista interferențelor, pot clasifica și recunoaște mii de caracteristici

Video reprezintă 60% din Big data
Volumul datelor video crește cu 20% anual

Controlul riscului – contextul tehnic actual

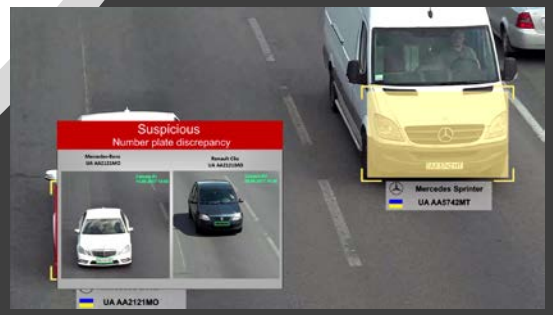
- Detectare, recunoaștere, identificare, intervenție (descurajare, întîrziere etc.)
  - efracție – perimetru, ușă, fereastră, zid
  - furt – desprindere, inlăturare
  - tâlhărie, hărțuire, vandalism
  - suspiciune – loitering
  - dezordine, violență
  - amenințare

- Detectoare in infraroșu pasiv
- Detectoare cu microunde
- Detectoare cu ultrasunete
- Contacte magnetice
- Detectoare de geam spart
- Detectoare de vibrații
- Butoane/pedale de panică
- Detectoare bazate pe tehnologii radar
- Magnasphere
- Detectoare bazate pe MEMS

Controlul riscului – contextul tehnic actual

- Recunoaștere automată a numerelor de înmatriculare + detectare tip autovehicul + autovehicul oprit, pe sens interzis .....
- Identificare față
- Discriminare om/vehicul/vehicul greu etc.
- Detectare sunet de armă
- Detectare comportament suspicios
- Clasificare obiecte
- Detectare/anihilare dronă
- Utilizare dispozitive smart (BYOD)
- Managementul identității

- Alertă la persoane, vehicule urmărite
- Alertă acces prea frecvent
- Detectare activitate neobișnuită
- Detectare furt, vandalism
- Detectare aglomerații, conflicte incipiente, ridicarea vocii, sunet de armă
- Detectare recunoaștere ostilă - terorism



Tendințe în managementul riscului de securitate

- Creșterea ponderii măsurilor tehnice în mecanismul de securitate
- Creșterea eficenței măsurilor tehnice de securitate
- Creșterea volumului de informații culese și a aportului activității de intelligence la profilarea amenințărilor
- Aportul tehnologiei de securitate în procesele de business
- Diversificarea echipamentelor tehnice de securitate, protecție la sabotaj, adaptabilitate crescută

- Creșterea vulnerabilității la atacuri cibernetice
- Creșterea complexității – competențe și calificări noi
- Atingere libertăți și drepturi personale

- Diversificare amenințări, modificări majore în context
- Abordare integrată a securității – fizică și cibernetică
- Diversificarea mijloacelor de control al riscului
- Schimbare profil profesional in serviciile de pază și intervenție
- Profilarea amenințărilor, valorificarea activități de intelligence

DISCUȚII

Evaluarea riscului de securitate parte a planificării sistemelor

Riscurile de securitate induse de evoluția tehnologica

Stelian Arion

stelian.arion@arts.org.ro

stelian.arion@secant.ro