ROLUL SECURITĂȚII ELECTRONICE IN PROTECȚIA INFRASTRUCTURILOR CRITICE

PROTECTIA INFRASTRUCTURILOR CRITICE

HELINICK

Securitatea unei națiuni, în conformitate cu „Strategia Europeana de Securitate", este definită de urmatoarele cinci dimensiuni: politică, militară, economică, diplomatică și de protecție a mediului.

În conformitate cu directivele UE gestionarea securității constituie „un proces deliberat prin care se vizează evaluarea riscului și punerea în operă a acțiunilor destinate să-l aducă la un nivel determinat și acceptabil, cu un cost acceptabil".

Prin gestionarea securității se vizează:

- identificarea riscului asociat vulnerabilităților de sistem și de proces al infrastructurilor critice, pericolelor și amenințărilor la adresa acestora;
- analiza și evaluarea riscului;
- controlul dinamicii acestuia;
- menținerea lui în limitele stabilite.

IC constituie „un bun material care este vital pentru funcționarea economiei și societății", iar prin PIC putem admite „totalitatea măsurilor stabilite pentru reducerea riscurilor de blocare a funcționării sau de distrugere a unei infrastructuri critice".

Protecția Infrastructurilor Critice (PIC) presupune, pentru realizarea unor standarde de performanță actionala, un parteneriat clar definit între proprietarii IC, personalul de exploatare sau administrare și autoritățile competente.

PROTECTIA INFRASTRUCTURILOR CRITICE

HELINICK

Etapele prin care se realizează Protecția Infrastructurilor

Critice sunt urmatoarele:

a. Descurajarea;

b. Detectarea sau identificarea: definită ca probabilitatea de determinare a unei acțiuni neautorizate aparute, sau în curs de apariție și include sesizarea, comunicarea alarmei la centrul de control și evaluarea alarmării;

c.Întîrzierea: definită ca intervalul de timp, măsurat în minute, în care componentă a sistemului de protecție fizică, desemnată să împiedice penetrarea în interior sau ieșirea din spațiu, devine activă în zona protejată;

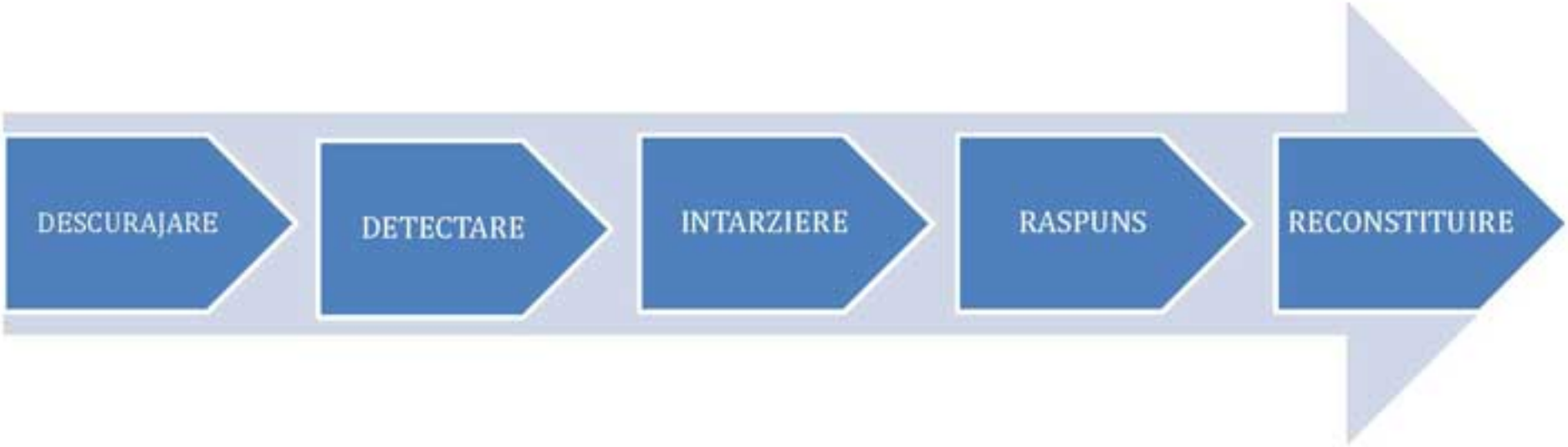
d. Răspunsul: intervalul de timp (în minute), în care se raspunde la Amenințare;

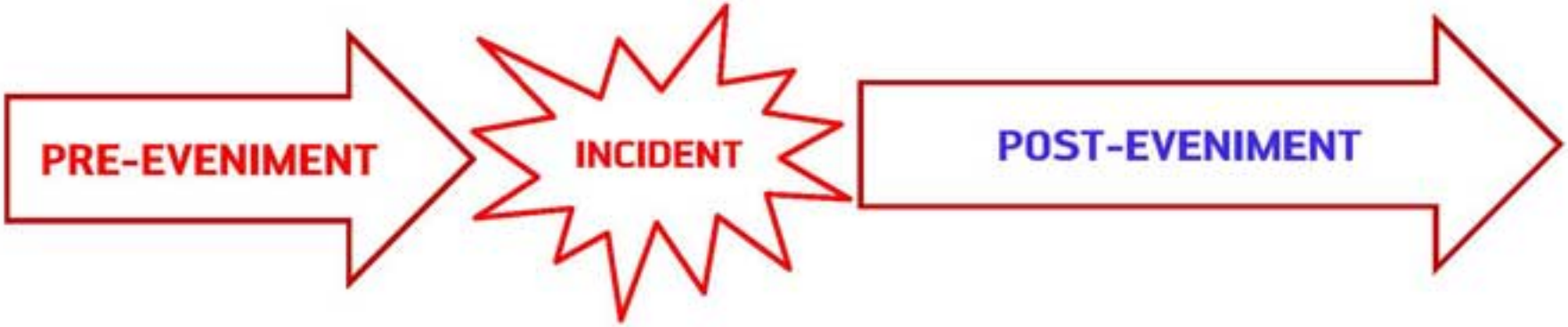
e. Reconstituire (intervine dupa eveniment): este ultima fază a ciclului PIC și implică acțiunile necesare pentru repornirea utilității deteriorate în urma acțiunii de distrugere.

PROTECȚIA INFRASTRUCTURILOR CRITICE

HELINICK

„Protecția infrastructurilor critice – cooperarea dintre sectorul guvernamental, mediul de afaceri și societatea civilă"





PROTECTIA INFRASTRUCTURILOR CRITICE

HELINICK

Dupa cum se constata, cele mai importante etape în realizarea PIC sunt Descurajarea și Detectarea unor acțiuni neautorizate și comunicarea alarmei la centrul de control și evaluare a alarmării.

HELINICK oferă o gamă completă de servicii de securitate care vă ajută să realizați barierele fizice și protecția electronică a infrastructurilor critice.

Realizăm proiectarea elementelor de securitate pornind de la analiza de risc și procedurile de lucru, în condiții normale sau în condiții de risc crescut de producere a unui eveniment, ale personalului care operează și administrează infrastructura critică.

Soluția HELINICK pentru Protecția Infrastructurilor Critice.

VidSys

PROTECTIA INFRASTRUCTURILOR CRITICE

HELINICK

Datorita riscurilor mari, se impune alegerea unor sisteme de securitate cu grad mare fiabiliate, toleranță la defecte și bazate pe tehnologii sigure.

HELINICK vă propune o soluție realizată special pentru protecția infrastructurilor critice, produsă de VidSys, denumită PSIM - PHYSICAL SECURITY INFORMATION MANAGEMENT.

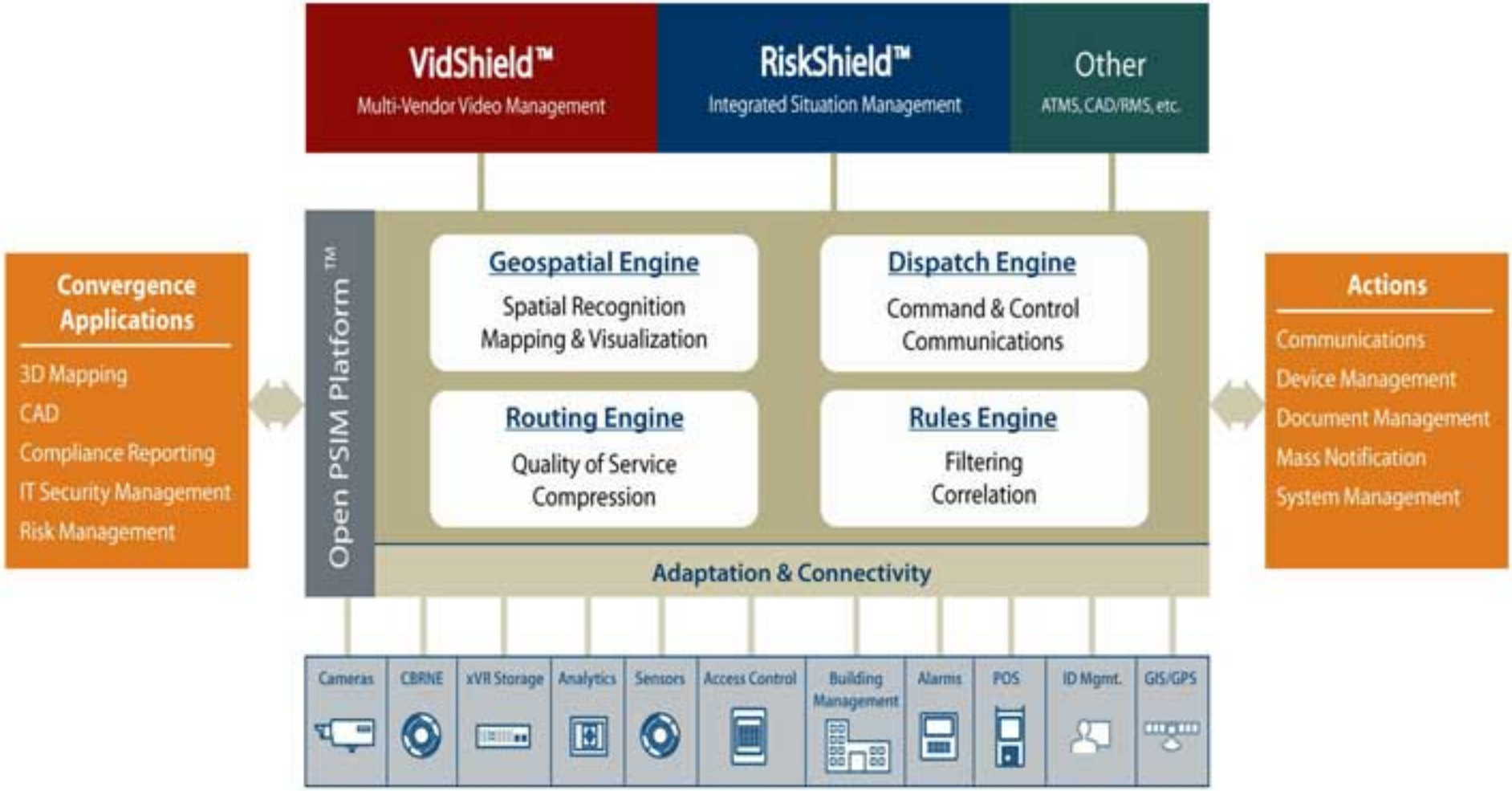
PROTECTIA INFRASTRUCTURILOR CRITICE

HELINICK

Un sistem bazat pe software-ul PSIM are cinci capabilități cheie:

1. Colectarea: software-ul de management colectează date de la un număr nelimitat de dispozitive sau sisteme de securitate disparate.
2. Analiza: Sistemul analizează și corelează date, evenimente, și alarme, pentru a identifica situațiile reale și prioritatea lor.
3. Verificare: Software-ul PSIM prezintă informațiile relevante într-un format ușor de interpretat.
4. Rezoluție: Sistemul furnizează procedurile standard de operare (POS), urmarind pas-cu-pas politicile organizației pentru a rezolva situația.
5. Raportarea: Software-ul PSIM urmărește toate informațiile colectate, pentru realizarea unui raport și eventual, pentru o analiză aprofundată a situației.

„Protecția infrastructurilor critice – cooperarea dintre sectorul guvernamental, mediul de afaceri și societatea civilă"



PROTECTIA INFRASTRUCTURILOR CRITICE

HELINICK

Componentele unei soluții PSIM scalabile sunt urmatoarele:

- **Platforma deschisa:** oferă o integrare ușoara cu diferite sisteme și dispozitive, în scopul de a realiza comunicația bidirecțională a sistemelor.

- **Motorul de corelare:** oferă posibilitatea de a integra evenimente și alarme multiple de la sisteme diferite împreună cu informații referitoare la timp și poziție, pentru identificarea automată a situațiilor periculoase și actualizarea lor dinamică în timpul desfășurării lor.

- **Localizarea geospațială:** sistemul poate localiza dinamic dispozitivele, oamenii, activele și creează conexiunile între ele.

Ex: poate identifica automat cea mai apropiată cameră de locul în care este sesizată o problemă, sau în cazul unei urgențe medicale, localizează cel mai apropiat responsabil de securitate capabil să intervină.

- **Cartografierea dinamica:** reprezintă capacitatea sistemului de a afișa locația unei situații de alarmă, a unui dispozitiv mobil sau fix, oameni sau alarme, și arată ce se întamplă într-o anumită situație, sau la nivel global în orice situație.

- **Interfața WEB browser:** permite accesul ușor și colaborarea facilă între organizație și personalul responsabil, facilitand suportul echipelor de intervenție mobile din centrul de comandă.

- **Prezentarea SOP** (proceduri de operare standard): sistemul prezintă operatorului, pe langă informații referitoare la incident, instrumente și date de contact necesare rezolvării rapide a incidentului, toate prin intermediul unei interfețe utilizator unice, bazate pe un set de instrumente vizuale sunt importate automat din sistem pentru a genera politici și proceduri pentru identificarea și rezolvarea incidentelor.

- **Raportarea granulară:** centralizează toate informațiile recepționate (video, alarme, audio), acțiunile intreprinse, într-un singur fișier care va fi utilizat în cazul analizei incidentului sau pentru a determina acțiunile post-eveniment necesare.

- **Platforma modulară:** PSIM este o soluție care permite adaptarea dinamică la modificările de configurație, situații, politici și raportări, în timp ce sistemul este complet funcțional.

Fiecare subsistem are principii și metode specifice de funcționare/operare dar aceste aspecte sunt uniformizate și tratate unitar de către software-ul de management integrat.

Intotdeauna se vor utiliza tehnologii complementare: mecanice, electronice, hardware și software care să realizeze o protecție efectivă a intregii infrastructuri.

„Protecția infrastructurilor critice – cooperarea dintre sectorul guvernamental, mediul de afaceri și societatea civilă"

✓ Pentru protecția perimetrală utlizăm sisteme de protecție bazate pe tehnologii diverse: IR, microunde, cablu sensitiv, taut-wire, etc.

✓ Supravegherea video se Realizează zi și noapte, indiferent de condițiile de mediu prin intermediul camerelor video fixe sau mobile PTZ sau SpeedDome Day/Nigth, radar , cu termoviziune, etc.

PROTECTIA INFRASTRUCTURILOR CRITICE

HELINICK

„Protecția infrastructurilor critice – cooperarea dintre sectorul guvernamental, mediul de afaceri și societatea civilă"

- ✓ Controlul accesului este bazat pe o centrală de acces și efracție cu interfață de rețea Ethernet.
- ✓ Protecția auto și pietonală se realizează prin bariere, turnicheți full-high, sisteme de acces individual.
- ✓ Blocarea, restricționarea, identificarea și autentificarea se face folosind tehnologii diverse: electromecanice, electronice, software și de comunicații.
- ✓ Acces individual bazat pe factori multiplii de autentificare (PIN, card, biometrie).
- ✓ Funcții avansate de urmărire și control (anti-passback, tracking, acces temporizat).
- ✓ Gestiune vizitatori

PROTECTIA INFRASTRUCTURILOR CRITICE

HELINICK

„Protecția infrastructurilor critice – cooperarea dintre sectorul guvernamental, mediul de afaceri și societatea civilă"

Protecția la incendiu este bazată pe un sistem analog adresabil ce permite identificarea și avertizarea automata a alarmelor de incendiu.

✓ Permite conectarea mai multor centrale în rețea pentru o monitorizare distribuită sau centralizată.

✓ Interconectarea cu sistemul integrat de securitate la nivel software si hardware.

PROTECTIA INFRASTRUCTURILOR CRITICE

✓ Sistem de detecție ultrarapidă a începuturilor de incendiu.

✓ Monitorizarea centralei de stingere incendiu in sistemul de detectie.

HELINICK

PROTECTIA INFRASTRUCTURILOR CRITICE

HELINICK

Siguranță prin tehnologie

Vă mulțumesc!