

Sistemes i Subsistemes de Seguretat Electrònica

Sant Jordi Club i Palau Sant Jordi Projecte Bàsic

Videovigilància (CCTV)

- Monitoratge i gravació d'espais amb càmeres IP. Inclou analítica de vídeo: reconeixement, detecció de moviments, lectura de matrícules, merodeig, etc.
- Instal·lació de càmeres sense fil si fos necessari en zones molt complexes d'arribar amb cable.
- Cobertura Exhaustiva: Essencial per assolir màxims nivells de seguretat. Ha d'incloure:
 - Accessos principals i secundaris, sortides d'emergència, passadissos, àrees esportives, magatzems.
 - El perímetre exterior.
 - Accessos específics com el de personal BSM, proveïdors i descàrrega.
 - Àrees crítiques com a sales de racks, sales elèctriques, CPDs, Centre de Control de Seguretat (CCS).
 - Punts estratègics interiors, com ara túnel de proveïdors/treball o accés proveïdors específics.

Requisits tècnics clau: Cobertura i característiques de les càmeres

- El disseny s'ha d'alinejar amb una estratègia de protecció en profunditat, **definint anells de seguretat (Privativa, Protegida, Crítica)** i assegurant que el CCTV contribueixi a cobrir els accessos i el perímetre d'aquests anells.
- **Instal·lar càmeres IP d'alta resolució:** Fonamentals per a una identificació clara d'individus i activitats, oferint qualitat superior i funcionalitats avançades. Es recomana l'ús de càmeres IP antivandàliques a exteriors i zones d'alt risc.
- **Operació Contínua:** Les càmeres han de funcionar les 24 hores del dia, els 7 dies de la setmana, amb enregistrament continu.
- **Visió Nocturna:** És crucial garantir el rendiment en condicions de baixa il·luminació. Cal la instal·lació de càmeres amb tecnologia infraroja (IR) per assegurar una vigilància efectiva nocturna. Incrementar la il·luminació exterior també millora la visibilitat i efectivitat del CCTV.
- **Resistència i Durabilitat:** Les càmeres, especialment a exteriors i zones vulnerables, han de ser resistents al vandalisme (IK10) i a les condicions climàtiques (IP67).

Requisits tècnics clau: Cobertura i característiques de les càmeres

Ubicació	Cobertura	Tipus de càmera	Característiques
Entrades i Sortides	Monitoritzar l'accés i la sortida de persones	Càmera IP Domo Fixa Càmera IP Bala	Visió nocturna, possibilitat de LPR en accessos de vehicles
Àrea de Recepció	Supervisar interaccions amb visitants i control d'accés	Càmera IP Domo Fixa	Discreta, bona qualitat d'imatge per a identificació facial
Passadissos i Zones de Circulació	Rastrear moviments interns i detectar presències no autoritzades	Càmera IP Domo Fixa Càmera IP Bala	Ampli camp de visió
Àrees Esportives (Gimnàs, Pistes, Camps)	Garantir la seguretat durant les activitats i prevenir el vandalisme	Càmera IP Domo Fixa Càmera IP PTZ	Resistent a impactes, ampli camp de visió, possibilitat de PTZ per a cobertura extensa
Magatzems i àrees d'equips	Prevenir robatoris i accessos no permisos	Càmera IP Domo Fixa Càmera IP Bala	Bona qualitat d'imatge per a identificació
Àrees d'estacionament	Dissuadir el robatori i el vandalisme de vehicles	Càmera IP Bala amb IR Càmera IP amb LPR	Resistent a la intempèrie (IP rating), visió nocturna, possibilitat de LPR
Tanques i portes perimetrals	Detectar intents d'entrada no autoritzada	Càmera IP Bala amb IR (Exterior)	Resistent a la intempèrie (IP rating), ampli camp de visió
Àrees amb equips d'alt valor	Vigilància enfocada a actius sensibles	Càmera IP Domo Fixa d'alta resolució	Màxima qualitat d'imatge per identificar detalls
Punts d'accés vulnerables (secundaris)	Cobrir tots els possibles punts d'entrada	Càmera IP Domo Fixa Càmera IP Bala	Discreta si cal

Requisits tècnics clau: Gestió, emmagatzematge i integració

- **Sistema de Gestió de Vídeo (VMS):** La integració amb un VMS robust i escalable és necessària per a la gestió, emmagatzematge i recuperació eficient. Un VMS permet visualització en temps real, cerca d'esdeveniments i configuració. Les càmeres s'integraran amb:
 - **El VMS XProtect de *Milestone* instal·lat al CCS de Calabria 66**
 - **El VMS XProtect de *Milestone* instal·lat al Palau Sant Jordi.**
- **Emmagatzematge Segur i Redundant:** Essencial per a la disponibilitat de proves i per prevenir la pèrdua de dades crítiques. Cal establir polítiques de retenció adequades. La redundància del Centre de Control de Seguretat millora la resiliència del sistema de gestió.
- **Sincronització Temporal:** Els enregistraments han d'estar sincronitzats amb marques de temps i data precises per a la seva validesa com a evidència.
- **Connectivitat:** Avaluar l'ús de connectivitat sense fils per a flexibilitat, i tecnologia PoE per a simplificar la instal·lació.

Requisits tècnics clau. Gestió, emmagatzematge i integració

- **Integració de sistemes:** El disseny ha de contemplar la integració del CCTV amb altres sistemes de seguretat per a una gestió centralitzada i una resposta eficaç.
 - **Integració amb PSIM (Physical Security Information Management):** Centralitzar tots els incidents de seguretat (incloent-hi vídeo) per millorar la capacitat i rapidesa de resposta. Això permetrà la integració amb Sistemes de Detecció d'Intrusió que també estiguin integrats amb el PSIM, característica fonamental per a permetre el posicionament automàtic de càmeres al videowall o monitors davant la detecció d'esdeveniments de seguretat, facilitant la verificació i la resposta ràpida.
 - **Integració amb Sistemes de Control d'Accés:** Permet l'enregistrament automàtic quan tenen lloc esdeveniments d'accés i en facilita la gestió integrada.
 - **Interconnexió amb altres dispositius d'entrada/sortida (E/S)**
segons el cas d'ús



Videovigilància (CCTV)

Direcció Corporativa de Seguretat i Autoprotecció i

Aparcaments de Concessió Municipal

Funcionalitats avançades i optimització operativa

- **Analítiques de vídeo intel·ligents (IA):** Implementar analítiques per a la detecció proactiva d'activitats sospitoses. Això inclou ***detecció de moviment en àrees restringides, merodeig, anàlisi de comportament, comptatge de persones, identificació d'objectes abandonats***. Les analítiques impulsades per IA milloren la seguretat en automatitzar la detecció d'esdeveniments potencials.
- **Accés Remot:** Permetre l'accés remot segur per a personal autoritzat (seguretat, gestors) per facilitar la supervisió i la resposta des de qualsevol ubicació. Les aplicacions mòbils poden permetre la visualització de transmissions en viu. S'ha de garantir la seguretat a l'accés a través de xarxes públiques.
- **Màscares de privadesa:** Utilitzar funcions d'emascarament per excloure de l'enregistrament àrees que no són rellevants per a la seguretat o on la vigilància seria desproporcionada.
- **Disseny Ergonòmic del Centre de Control:** Considerar la disposició i les eines del Centre de Control de Seguretat (CCS) per optimitzar l'eficiència operativa del personal que monitoritza el sistema de videovigilància. Això inclou la disposició de monitors i l'automatització de la visualització davant d'esdeveniments,

Compliment normatiu i protecció de dades (RGPD/AEPD/LOPDGDD)

- El disseny del sistema ha de complir rigorosament les normatives de protecció de dades i privadesa, com el RGPD, les directrius específiques de l'AEPD i la LOPDGDD.
- **Protecció de Dades des del Disseny i per Defecte (Privacy by Design/by Default):** La protecció de dades ha de ser present a les primeres fases de concepció del projecte. Això es tradueix en mesures tècniques i organitzatives integrades en el disseny i especificacions del sistema.
- **Deure informació: Utilitzar un sistema d'informació de "doble capa".**
 - És una obligació fonamental. El distintiu informatiu (cartell) de la Instrucció 1/2006 és d'ús obligatori amb fins de seguretat i ha de situar-se en tots els accessos a les zones vigilades.
 - El cartell (primera capa) ha d'indicar l'existència del tractament, la identitat del responsable, la possibilitat d'exercir els drets (Art. 15 a 22 RGPD) i on obtenir més informació. Un QR pot enllaçar més detalls. La informació addicional (segona capa) es pot facilitar per altres mitjans, com ara una política de privadesa a la web o impresos disponibles.

Detecció d'amenaques físiques

- Inclou detectors d'armes blanques i escàners de persones, borses i/o equipatges mitjançant raigs X o ones mil·limètriques.
- APP de comunicació d'incidents de seguretat en espai en carga als serveis de seguretat.
- Complementant el control d'accessos, la detecció proactiva d'amenaques físiques és un pilar fonamental per garantir un entorn segur dins del recinte, especialment durant esdeveniments massius i a les àrees sensibles del recinte.
- Els principis claus són:
 - Detecció d'armes en accessos massius.
 - Control de la paqueteria i objectes que arriben al recinte.
 - Gestió d'alertes.
- Per a un accés àgil i segur als esdeveniments, s'implementaran detectors d'armes de barres amb tecnologia magnètica de banda ampla. Aquests sistemes discriminaran eficaçment objectes quotidians per focalitzar-se en amenaces reals, optimitzant el flux de persones i reduint les interrupcions per falses alarmes.
- En la recepció a les oficines del Palau Sant Jordi disposar d'un escàner de raigs X pel control de la paqueteria entrant.



Detecció d'amenaques físiques

Alertes

- Caldria disposar d'una APP de comunicació d'alertes als equips de seguretat amb integració al PSIM (Physical Security Information Management).
- Aquesta APP ha de permetre generar alertes en temps real, visualització de la ubicació de l'alerta, possibilitat de comunicar incidents, etc.

- L'objectiu principal dels controls d'accessos previstos és garantir la seguretat de les persones, la protecció dels béns i la salvaguarda de la informació, gestionant de manera eficient i segura el flux d'individus i vehicles a totes les àrees.
- **Els principis claus sobre els quals s'ha de dissenyar són:**
- **Seguretat per Capes:** Implementar diferents nivells de seguretat i tecnologies d'identificació adaptats a la criticitat de cada zona.
- **Flexibilitat i Escalabilitat:** Dissenyar un sistema modular que permeti adaptar-se a les necessitats canviants i possibles futures ampliacions del recinte o dels seus usos.
- **Traçabilitat:** Registrar de manera fiable i inalterable tots els accessos i intents d'accés per a propòsits d'auditoria i investigació forense.
- **Integració:** Connectivitat total amb el sistema PSIM (Physical Security Information Management) existent per a una gestió centralitzada i correlació d'esdeveniments amb altres sistemes de seguretat (CCTV, alarmes, etc.).
- **Resiliència:** Garantir l'operativitat del sistema davant de possibles fallades tècniques o talls de subministrament elèctric.
- Regular l'entrada i sortida de persones. Inclou targetes RFID, i torns motoritzats.
- A partir anàlisis específic, implantar panys i claus electròniques eliminant les claus mecàniques als edificis.
- Armaris electrònics de claus.
- Possibilitat operacions en remot d'obertura, tancament i comprovació per càmera.
- Connexió a CRA i redundant amb CCS Calabria i Centre Control Palau Sant Jordi.

Control d'accés

Accés amb vehicles automatitzat

- Lectura de matrícules (LPR/ANPR) per a vehicles autoritzats (proveïdors, personal clau, etc).
- Lectura de targetes/identificadors RFID de llarg abast per a personal acreditat amb vehicle.
- Integració amb bases de dades de vehicles autoritzats i llistes negres.
- Incorporar *road blockers* en accessos estratègics per tal de reforçar la seguretat perimetrals, de forma que permeti mitigar els possibles atacs terroristes amb vehicles. Han de ser dispositius amb capacitat de detenir vehicles pesants a gran velocitat, han de poder ser controlats des del CCS de Palau Sant Jordi, CCS de Calabria, CRA i de forma local des del punt de control en l'accés (si existeix). Han de disposar de il·luminació led per alertar de la seva presència i evitar xocs accidentals, han de disposar de certificacions conforme la seva robustesa davant d'impactes.

Polsadors de pànic amb interfonia

- Instal·lar polsadors de pànic en zones crítiques, tant d'accés del públic a esdeveniments com zones privades, amb sistemes d'interfonia integrats al PSIM.
- Aquests equips d'interfonia han de tenir una segona funcionalitat la de permetre generar alarmes de forma autònoma en cas de que detectin sorolls inesperats segons franges horàries.



Control d'accés

Zona d'oficines, sales tècniques i espais restringits (vestidors, backstage, etc..)

- Instal·lar controls d'accessos amb lectors de targetes (on sigui possible ubicar torns per accedir) tant a les entrades com a les sortides d'oficines i equipaments tècnics, tant pels treballadors propis del recinte com per les empreses subcontractades. Aquests lectors també hauran d'estar integrats al PSIM.
- Millorar la gestió de les claus de les portes per millorar la traçabilitat i minimitzar el risc d'extraviaments o usos indeguts, es proposa un sistema de amb doble opció d'apertura a cada porta que permeti millorar el control de qui accedeix a cada àmbit:
 - Pany electrònic amb apertura mitjançant targeta, smartphone o smartwatch.
 - Pany tradicional amb apertura mitjançant clau que estigui custodiada en armari intel·ligent de gestió de claus. Aquesta segona opció permetria resoldre possible incidències en casos excepcionals del primer sistema o per si a cert personal no se'l volgués donar accés al sistema.
 - Establiment de perfils d'usuari amb permisos definits per accedir a zones específiques durant franges horàries determinades (personal de manteniment, neteja, seguretat, personal d'oficines, organitzadors d'esdeveniments, etc.).
 - Les portes hauran de tenir possibilitat de tancament remot amb visualització per càmera des dels centres de control.
 - Reforçar les mesures de seguretat en sales amb actius d'alta criticitat (sales de servidors, el CCS, etc..) mitjançant càmeres que registrin les persones que hi accedeixen per tenir un control forense en cas de qualsevol incidència.
 - Els sistemes de d'accés als panys electrònic i armari intel·ligent hauran d'estar integrats al PSIM i caldrà que disposin de connexió amb el CCS de Calabria, CCS de Palau Sant Jordi i CRA.

Detecció d'intrusió

Requisits clau del disseny: Normativa i Grau de Seguretat

- El disseny i la instal·lació del sistema d'intrusió ha de complir estrictament la normativa espanyola aplicable en seguretat privada.
- Això inclou la Llei 5/2014 de Seguretat Privada, el Reglament de Seguretat Privada (RD 2364/1994), i les ordres ministerials corresponents (INT/316/2011 i INT/314/2011).
- La instal·lació només la poden fer empreses de seguretat degudament autoritzades d'acord amb l'Ordre INT/314/2011.
- És fonamental el compliment de les normes europees UNE-EN de la sèrie 50131, que estableixen requisits generals per a sistemes d'alarma contra intrusió i atracament, així com especificacions per als seus components (detectors, centrals, interconnexions, fonts d'alimentació). També aplica la norma UNE-EN 50136 per a la transmissió de senyals.
- La normativa UNE-EN 50131 defineix diferents graus de seguretat segons el risc.
- El sistema s'ha d'ajustar, com a mínim, al grau 2 (risc mitjà) segons UNE-EN 50131-1. Aquest grau és adequat per a entorns amb amenaces moderades.
- Considerant l'objectiu de màxima seguretat per a la remodelació del pavelló, es pot requerir un nivell de protecció superior, com ara el Grau 3 (Risc Mitjà/Alt), destinat a establiments amb risc significatiu o que requereixin mesures avançades.
- Tots els components del sistema han de complir els estàndards UNE-EN aplicables i tenir certificats d'homologació. El grau de seguretat general del sistema estarà limitat pel component de menor grau.
- Els sistemes connectats a una Central Receptora d'Alarmes (CRA), com serà el cas, han de tenir un grau de seguretat adequat al risc (Grau 2 ó 3).

- **Objectius principals del sistema de detecció d'intrusió**
 - Aconseguir una detecció precoç i precisa (mitjançant la zonificació) d'accessos no autoritzats.
 - Cobrir els punts d'accés perimetrals (portes, finestres, tanques) i el moviment intern.
 - Assegurar una resposta immediata mitjançant la integració amb una central d'alarmes.
 - Protegiu els actius crítics i les sales sensibles.
 - Garantir la fiabilitat operativa (protecció contra manipulacions, redundància, còpia de seguretat).
 - Facilitar la gestió eficient d'incidències a través d'una plataforma centralitzada.
 - Millorar la protecció general i eliminar les vulnerabilitats.
 - Complir amb la normativa espanyola pertinent.
- Sensors de moviment, contactes magnètics i barreres infraroges per detectar accessos no autoritzats. Anàlisis dels espais per definir tipologies.
- Connexió a CRA i redundant amb CCS Calabria i Centre Control Palau Sant Jordi.

Requisits clau del disseny: Arquitectura i Components

- **Central d'Alarma:** Serà el nucli del sistema. Ha de ser una central d'intrusió amb capacitat per gestionar alarmes per zones i comptar amb funcions d'autodiagnòstic, autoarmat, armat parcial/nocturn/temporitzat i registre d'esdeveniments. Haureu de permetre configuració, diagnòstic i manteniment remots. Idealment, la central ha de ser certificada per a Grau 3.
- **Detectors:** S'instal·laran per a la detecció primerenca d'accessos no autoritzats tant al perímetre com a l'interior.
 - Inclouran detectors volumètrics distribuïts estratègicament segons els nivells de seguretat i zones de valor.
 - Es preveuran detectors de doble tecnologia (infrarojos/microones) amb anti-emmascarament en punts crítics com accessos, passadissos i zones amb actius valuosos. Podran ser de llarg abast si cal. Els detectors volumètrics seran de tipus convencional.
 - Es poden contemplar altres tipus de detectors específics segons la vulnerabilitat (contactes magnètics, etc.).
- **Sirenes:** El sistema comptarà amb dispositius d'avís sonor i/o visual.
 - Sirenes interiors, certificades i amb protecció contra manipulació (tamper). Es recomanen de baix perfil.
 - Sirenes exteriors, òptic-acústiques i protegides contra manipulació.
- **Control i accés al Sistema:** S'instal·laran consoles amb pantalles LCD i teclat alfanumèric per a la control del sistema. El disseny ha d'assegurar que només l'usuari autoritzat pugui armar i desarmar.
- **Interconnexions:** Les connexions entre els components del sistema seran cablejades i dedicades (no compartides amb altres sistemes). El cablatge ha de ser inaccessible, ocult, ben subjecte, i complir les especificacions del fabricant i normatives de baixa tensió. Es faran servir elements de canalització lliures

Detecció d'intrusió

Requisits clau del disseny: Arquitectura i Components

- **Comunicació:** La central ha de transmetre els senyals a una CRA i al PSIM del CCS de Calabria 66 i al PSIM del CCS del Palau Sant Jordi.
 - La via principal serà un mòdul de comunicació bidireccional TCP/IP (Ethernet), que permet connexió a múltiples destinacions i avisos.
 - Es comptarà amb una via de suport mitjançant un mòdul de comunicació GPRS/3G per garantir la comunicació en cas de fallada de la xarxa IP.
- **Alimentació:** El sistema inclourà fonts d'alimentació supervisades i bateria de respatller per assegurar-ne el funcionament davant de talls de subministrament elèctric. La instal·lació elèctrica del sistema ha de complir el Reglament Electrotècnic de Baixa Tensió.
- Zonificació del sistema. Tot i que les fonts se centren en la zonificació per a sistemes de detecció d'incendis, el principi és aplicable a la detecció d'intrusió: **dividir la instal·lació en àrees o zones lògiques i físiques per localitzar amb precisió qualsevol esdeveniment d'alarma.**
- La zonificació permet optimitzar la resposta a l'incident, ja sigui per part del personal intern (com l'equip d'intervenció en emergències en un pla d'autoprotecció) o dels serveis externs.
- El disseny s'ha d'alinejar amb els estàndards locals, nacionals i internacionals, tot garantint el compliment dels requisits de risc i nivell de protecció. Tot i que el document esmenta un mínim de grau 2, l'avaluació de riscos i l'objectiu de "màxima seguretat" poden orientar cap a un grau 3 en funció de les àrees a protegir i els actius presents.
- La zonificació ha de tenir en compte les característiques específiques de les instal·lacions i els components.

Detecció d'intrusió

Requisits Clau del Disseny: Instal·lació i posada en marxa

- **Disseny i Planificació:** L'empresa instal·ladora ha de presentar una "Proposta de Disseny del Sistema" i un "Pla d'Instal·lació" (si escau), basats en la norma UNE-EN 50131-7 i un estudi tècnic detallat del lloc.
- **Instal·lació:** Els components han d'instal·lar-se segons les recomanacions del fabricant i ser adequats per a les condicions ambientals. Es prendran mesures per protegir els equips durant la instal·lació i assegurar-ne l'accessibilitat futura per a manteniment. La instal·lació elèctrica ha de complir la normativa vigent.
- **Qualitat de materials:** Tots els elements del sistema han d'estar aprovats o homologats d'acord amb les normes europees aplicables a cada tipus de component.
- **Proves i Inspecció:** Un cop completada la instal·lació, el personal tècnic realitzarà una inspecció per confirmar que s'ha executat segons la proposta de disseny i l'estudi tècnic. Es portaran a terme assaigs per verificar el funcionament correcte de cada detector, component i dispositiu d'avís.
- **Verificació d'alarmes:** La CRA haurà d'implementar procediments de verificació (seqüencial, vídeo, àudio, personal) per confirmar l'autenticitat dels senyals d'alarma abans de notificar-los a les Forces i els Cossos de Seguretat de l'Estat (FCS). La CRA ha de disposar de com a mínim dos operadors i transmetre immediatament les alarmes reals a la policia. El sistema ha de ser capaç de diferenciar clarament entre un senyal d'alarma i un senyal de sabotatge.

Zonificació: Identificació de zones potencials

- La divisió en zones permet adaptar les mesures de seguretat a les característiques i el nivell de risc de cada àrea.
- Algunes zones potencials a considerar inclouen:
 - **Àrees d'accés i recepció:** Punt principal d'entrada/sortida de l'edifici.
 - **Pista Poliesportiva:** L'àrea de joc principal. Depenent de la seva mida, podria subdividir-se.
 - **Graderies i passarel·les per a espectadors:** Zones d'alta ocupació durant esdeveniments, però buides i susceptibles a intrusió fora d'ells.
 - **Vestuaris i Lavabos:** Espais auxiliars associats a la pràctica esportiva.
 - **Magatzems:** Àrees que solen contenir equipament esportiu o altres actius valuosos. Aquestes zones poden presentar un risc més elevat.
 - **Oficines i àrees d'administració:** contenen informació i possiblement equips administratius [Mencionat com a àrea auxiliar en tipus de pavellons grans, similar al Pla d'autoprotecció que situa la central d'incendis en administració].
 - **Sales d'instal·lacions tècniques:** Incloent quadres elèctrics, calderes, sistemes d'acumulació, etc. Són àrees crítiques pel potencial de sabotatge.
 - **Cafeteria/Bar:** Zona de servei amb accés públic.
 - **Espais exteriors:** Pistes exteriors, àrees d'aparcament, perímetres.

Detecció d'intrusió

Zonificació: Criteris i components del Sistema

- La definició de les zones es basa en diversos criteris:
 - **Funció i ús:** Agrupar àrees amb propòsits semblants (ex. zones d'accés, zones esportives, zones tècniques).
 - **Nivell de risc:** Zones que contenen actius valuosos o instal·lacions crítiques (magatzems, sales tècniques, oficines) poden requerir zones separades i possiblement detectors més sensibles o redundància.
 - **Possibilitats d'armat/desarmat parcial:** Permetre l'activació del sistema en certes àrees mentre que altres estan en ús (ex. armar magatzems i oficines mentre la pista està oberta).
 - **Facilitat de localització:** Cada zona s'ha de correspondre amb una àrea fàcilment identificable en plànols o al terreny per a una resposta ràpida i eficient.
- **Delimitació física:** Les zones han de respectar les barreres arquitectòniques i la compartimentació de l'edifici. Dins de cada zona, cal instal·lar detectors apropiats per al tipus d'espai (detectors de moviment, contactes magnètics a portes i finestres, detectors de trencament de vidre, etc.) que compleixin els estàndards requerits per al grau de seguretat definit.
- Els senyals d'alarma han d'incloure informació clara sobre la ubicació del sensor activat (la zona) per facilitar-ne la verificació i la resposta immediata.
- La integració amb sistemes de videovigilància pot permetre la verificació en temps real de les intrusions a la zona afectada.

Detecció d'intrusió

Elements de detecció: Criteris de selecció i tipus

- Els detectors són dispositius clau que informen la central d'alarmes sobre variacions a les àrees protegides.
- Hi ha diversos tipus de detectors d'intrusió, classificats per la seva actitud (actius o passius), zona de vigilància (puntuals, lineals, planars, volumètrics) i ubicació (perimetrals, perifèrics, d'interior).
- **Criteris clau per a l'elecció del detector:**
 - **Tipus de material a protegir:** Materials tous (fusta, vidre, maó) vs. superfícies dures (formigó armat, acer estructural, caixes fortes).
 - **Naturalesa de l'atac potencial:** Atacs amb eines contundents o força bruta (cops, trencaments) vs. atacs més sofisticats (trepants diamantats, serres mecàniques, explosius, eines tèrmiques).
 - **Ubicació en el model de protecció multicapa:** Perímetre, perifèria, o interior.

Detecció d'intrusió

Elements de detecció: Criteris de selecció i tipus

- **Tipus de detectors rellevants:**

- **Detectors d'impacte/vibració/inercials:** Identifiquen atacs físics amb eines contundents sobre materials com fusta, vidre o maó. Estan regulats per la norma UNE-EN 50131-2-8. El seu ús es recomana en elements estructurals vulnerables com portes, finestres o envans interiors. Són detectors passius i planars o puntuals, utilitzats en àrees perimetrals/perifèriques/interiors.
- **Detectors sísmics:** Capten vibracions subtils, de baixa freqüència i llarga durada, generades per atacs sofisticats com forats, serres, explosius o eines tèrmiques. La seva aplicació està regulada per la norma alemanya VdS 2331. Són imprescindibles en superfícies dures exposades a sabotatges complexos, com caixers automàtics, cambres cuirassades, caixes fortes, o murs de formigó armat o acer estructural. Són detectors passius i superficials, recomanats per a àrees perimetrals.
- **Detectors de moviment (volumètrics):** Detecten canvis de temperatura (Passius Infrarojos - PIR) o emeten energia (Microones, Ultrasons) per detectar irregularitats mitjançant l'efecte Doppler (Actius). Els **detectors "Dual Tec" combinen tecnologies PIR i microones per reduir falses alarmes**. Estan dissenyats per captar el desplaçament de l'intrús a partir de les pertorbacions que origina aquest moviment en les condicions ambientals. Són detectors volumètrics, principalment interiors.

Detecció d'intrusió

Elements de detecció: Selecció de detectors per zones

Aplicant el model de protecció multicapa i els criteris de selecció:

- **Àrea Perimetral:** La primera capa externa, definida pel perímetre.
 - Per detectar intents d'intrusió a través de la superfície o línia del contorn (tanques, murs exteriors).
 - Considerar detectors inercials o de cable sensor per a detecció sobre tanques o murs.
 - Per a murs de formigó o acer, o àrees d'alt risc al perímetre, on s'esperin atacs sofisticats (perforació, tall), els detectors sísmics són imprescindibles.
 - En espais a l'aire lliure dins del perímetre, es poden fer servir detectors de moviment perimetrals actius (radars, sonars) Es recomana instal·lar dos o més anells de seguretat perimetral amb diferents principis de funcionament i àrees de detecció solapades per a instal·lacions d'alt risc.
 - La vigilància perimetral ofereix precocitat en la detecció.

Detecció d'intrusió

Elements de detecció: Selecció de detectors per zones

Aplicant el model de protecció multicapa i els criteris de selecció:

- **Àrea Perifèrica:** Superfícies properes als edificis (contorns de les edificacions).
 - Vulnerabilitats com portes, finestres, lluernes, murs i superfícies de vidre.
 - Per a portes i finestres vulnerables a atacs amb eines contundents, utilitzeu detectors d'impacte o vibració.
 - Complementar amb contactes magnètics a portes i finestres per detectar obertures.
 - Utilitzar detectors de trencament de vidre per a finestres.
 - Aquests detectors (impacte, magnètics, trencament de vidre) poden ser puntuals o superficials i s'utilitzen en àrees perimetrals/perifèriques/interiors.

Detecció d'intrusió

Elements de detecció: Selecció de detectors per zones

- **Àrea Interior:** Dissenyada per detectar intrusos que han penetrat capes externes.
 - Espais tancats com sales, oficines, vestuaris, passadissos.
 - Els detectors volumètrics, principalment detectors infrarojos passius (PIR) i detectors de microones (o combinats), són els més característics per detectar el desplaçament de persones.
 - En àrees d'alt risc interior, com sales tècniques o zones d'emmagatzematge d'equipament valuós, l'elecció dependrà del tipus d'atac esperat i materials a protegir, i també es poden requerir detectors d'impacte o sísmics si es protegeixen elements específics com caixes fortes.
 - Els sistemes de videovigilància (CCTV) són elements irrenunciables en la protecció interior per a suport, verificació, detecció i anàlisi.

Detecció d'intrusió

Elements de detecció: Selecció de detectors per zones

- **General:** La certificació Grau 3 o 4 implica requisits específics per als equips i la instal·lació. En instal·lacions d'alt risc (Grau 4), s'espera que els intrusos tinguin una gamma completa d'equips, incloent-hi mitjans de substitució de components vitals, cosa que exigeix mitjans per detectar retard, modificació o substitució de senyals. És crucial assegurar la fiabilitat dels sistemes, especialment a Grau 4, combinant detectors amb lògiques com 'Y' (And) per reduir falses alarmes.

Detecció d'intrusió

Elements de detecció: Selecció de detectors per zones

Tipus de detector	Àrea de col·locació recomanada	Consideracions específiques
Contacte magnètic	Portes i finestres exteriors i accessos interns restringits	Protecció contra manipulació
Detector de moviment PIR	Passadissos interns, àrees esportives principals, espais oberts	Ajustar sensibilitat per evitar falses alarmes
Detector de doble tecnologia (PIR i microones)	Àrees d'alt trànsit o ambients amb possibles falses alarmes	Major immunitat a falses alarmes
Detector de trencament de vidres	Grans superfícies de vidre	Sensibilitat adequada al tipus de vidre
Botó de pànic	Àrea de recepció, oficina del gerent, ubicacions estratègiques	Fàcilment accessible en cas d'emergència

Detecció d'intrusió

Integració amb altres sistemes: Avantatges clau

- **Validació visual d'alarmes:** La integració amb la videovigilància (CCTV) permet que la Central Receptora d'Alarmes (CRA) o el personal de seguretat visualitzin en temps real què passa quan s'activa una alarma d'intrusió. Això ajuda a verificar l'autenticitat del senyal i redueix les falses alarmes.
- **Resposta coordinada i efectiva:** La connexió del sistema d'intrusió amb altres dispositius de seguretat, com ara sensors de moviment, alarmes i sistemes de control d'accés, a través de la integració (per exemple, mitjançant IoT), facilita una resposta coordinada i efectiva davant de qualsevol incident.
- **Seguretat perimetral completa:** Es pot aconseguir un sistema de seguretat perimetral mitjançant l'ús de sistemes combinats que inclouen detecció d'intrusió, videovigilància i barreres físiques. La detecció primerenca d'un intent d'intrusió pot activar l'alarma i permetre l'acció dissuasòria.

Detecció d'intrusió

Integració amb altres sistemes: Avantatges clau

- **Millora de la gestió d'accessos:** Els sistemes de control d'accés regulen l'entrada i la sortida de persones autoritzades, cosa que complementa la seguretat del sistema d'intrusió en prevenir activament l'accés no autoritzat a àrees sensibles. La integració permet, per exemple, que una detecció d'intrusió a una zona d'accés activeu una verificació d'accés o restringeixi la sortida.
- **Informació integral per a la presa de decisions:** La combinació d'informació de diferents sistemes (intrusió, CCTV, control d'accessos) proporciona una visió més completa de la situació, millorant la capacitat de resposta i la gestió de la seguretat en general.
- **Potencial per a l'automatització:** la integració permet automatitzar respostes; per exemple, una alarma d'intrusió pot activar càmeres específiques per gravar o enfocar la zona afectada, o desencadenar accions al sistema de control d'accés.

Detecció d'intrusió

Integració amb altres sistemes: Requisits per al sistema d'intrusió

- **Connexió a Central Receptora d'Alarmes (CRA):** Per ser plenament operatiu i permetre una gestió professional dels senyals, el sistema d'intrusió ha d'estar connectat a una CRA degudament enregistrada i autoritzada. Això és fonamental per a la recepció, la verificació i la gestió d'alarmes les 24 hores. Les comprovacions de manteniment d'un sistema d'intrusió inclouen el test de connexió a la CRA.
- **Infraestructura de xarxa i cablejat adequats:** Un cablejat correcte i una infraestructura de xarxa apta són crucials per a l'exercici i la gestió dels sistemes de seguretat, inclòs el d'intrusió. Els problemes i errors en els equips sovint es deuen a infraestructures deficientes o de baixa qualitat. És vital utilitzar materials de qualitat i sota estàndards normatius per assegurar una major seguretat i evitar pèrdues o sorolls al senyal.
- **Suport per a comunicació bidireccional:** L'evolució dels sistemes d'intrusió inclou centrals bidireccionals avançades. La comunicació bidireccional és important perquè la CRA pugui monitoritzar l'estat del sistema, verificar senyals (incloent-hi videoverificació) i gestionar el sistema remotament.

Detecció d'intrusió

Integració amb altres sistemes: Requisits per al sistema d'intrusió

- **Capacitat d'integració amb altres sistemes:** el sistema d'intrusió ha de tenir la compatibilitat o les interfícies necessàries per integrar-se amb altres sistemes de seguretat com la videovigilància (VMS), la gestió d'informació de la seguretat física (PSIM) i les plataformes IoT. Això permet que els sistemes intercanviïn informació i actuïn de manera conjunta.
- **Fiabilitat dels elements de detecció i control:** l'eficàcia de la integració depèn de la fiabilitat dels elements individuals. Els sistemes moderns d'intrusió utilitzen detectors de doble tecnologia amb microprocessadors que confirmen el senyal abans d'emetre'l, millorant l'eficiència.
- **Manteniment regular del Sistema:** Un requisit fonamental per assegurar el funcionament correcte i la integració eficaç és el manteniment regular del sistema d'intrusió, així com dels sistemes de videovigilància i control d'accessos amb què s'integra.

Control d'aforament

- Sistema de control d'aforament en temps real i sectorització per zones o utilització segons usos de l'espai.
- Aplicació pel seu control a partir de dispositius mòbils i al Centre de Control de Palau Sant Jordi i al CCS Calàbria.
- La gestió eficient i segura de l'aforament és essencial, especialment en un recinte que acull esdeveniments massius. Un control precís de la densitat de persones a les diferents zones és crucial per garantir la seguretat, facilitar l'evacuació en cas d'emergència i optimitzar l'experiència del públic.
- Els principis clau seran:
 - Control en temps real i sectorització dinàmica.
 - Gestió intel·ligent de cues.
 - Generació automàtica d'alarmes.
 - Monitorització i visualització.
 - Capacitat de generació d'informes amb patrons de moviment i distribució del públic segons tipologia de l'esdeveniment.
- Sistema intel·ligent de control d'aforament en temps real amb sectorització dinàmica per zones (per exemple, graderies dividides per seccions en un partit o zona de pista segmentada per tipus d'entrada en un concert).
- Gestió intel·ligent de cues als accessos del Palau Sant Jordi i el Sant Jordi Club, amb capacitat per comptabilitzar persones i estimar temps d'espera.
- El sistema es basa en intel·ligència artificial (IA) aplicada a l'anàlisi de vídeo
- Control i monitorització accessibles des de dispositius mòbils i els Centres de Control del Palau Sant Jordi i el CCS Calàbria, amb integració al sistema de gestió de vídeo (VMS) existent.

Sistema de control d'aforament

Funcionament del sistema

- Generació automàtica d'alarmes en detectar excés d'aforament en sectors específics (àrees de graderies o sectors de la pista).
- Generació automàtica d'alarmes en detectar acumulacions inusuals de persones a les cues o sobrepassar una certa longitud.
- El sistema generarà mapes de calor en temps real per a una visualització intuïtiva i immediata de la densitat de l'aforament a tot el recinte.
- Haurà de proporcionar informes estadístics sobre patrons de moviment, densitat i distribució del públic durant cada esdeveniment. Aquests informes hauran d'alertar si durant els esdeveniments s'ha sobrepassat l'aforament en algun sector.

Sistema de control d'aforament

Informes

- Haurà de proporcionar mètriques clau sobre l'eficiència dels accessos, com el nombre mitjà de persones processades per cua per unitat de temps (per exemple, persones per minut per cua), per identificar possibles colls d'ampolla.
- El sistema generarà un dashboard amb l'anàlisi agregada del comportament de diversos esdeveniments similars (com concerts) per identificar patrons que optimitzin la seguretat, els recursos i l'experiència del públic en el futur.

Detecció i alarma d'incendis

- Detectar fum, calor o gas. Incloure alarmes acústiques i visuals, integrades amb sistemes d'evacuació.
- Elements talla focs i de confinament.
- Connexió a CRA i redundància al Centre de Control del Palau Sant Jordi i CCS Calabria. Integració a *scada* i a PSIM.

Detecció i alarma d'incendis

Context, objectiu i normativa aplicable

- **Objectiu:**

- Establir regles i procediments per complir les exigències bàsiques de seguretat en cas d'incendi.
- La correcta aplicació del conjunt del Document Bàsic SI (DB SI) satisfà el requisit bàsic "Seguretat en cas d'incendi".

- **Normativa aplicable:**

- Codi Tècnic de l'Edificació (CTE) - Document Bàsic SI (DB SI). La seva aplicació és obligatòria a l'àmbit establert per al CTE.
- Reglament d'Instal·lacions de Protecció contra Incendis (RIPCI) (Reial Decret 513/2017), que cobreix disseny, instal·lació, manteniment i inspecció.
- Normes UNE, UNE-EN, UNE-EN ISO, que són fonamentals per a l'aplicació del DB SI. La normalització recolza la protecció contra incendis.

Detecció i alarma d'incendis

Criteris de disseny

- **Compliment normatiu:**

- El disseny del sistema ha de complir els requisits establerts al CTE-DB SI (Secció SI 4) i al RIPCI.
- El contingut del projecte ha de ser conforme al que estableix la norma UNE 157001, sens perjudici del que estableixin les administracions competents.

- **Suport en normes UNE:**

- Les normes UNE i UNE-EN, com les de la sèrie UNE-EN 54 (implicada a l'Annex SIG que llista normes relacionades amb l'aplicació del DB SI), són fonamentals per al disseny.

- **Enfocaments de disseny:**

- Es pot seguir un enfocament prescriptiu basat en el compliment directe de les especificacions normatives.
- Es pot optar per un Disseny Basat en Prestacions (DBP), que és una metodologia única per a cada edifici analitzat.

Detecció i alarma d'incendis

Criteris de disseny

- **Comunicació:** La central ha de transmetre els senyals a una CRA i al PSIM del CCS de Calabria 66 i al PSIM del CSS del Palau Sant Jordi.
 - La via principal serà un mòdul de comunicació bidireccional TCP/IP (Ethernet), que permet connexió a múltiples destinacions i avisos.
 - Es comptarà amb una via de suport mitjançant un mòdul de comunicació GPRS/3G per garantir la comunicació en cas de fallada de la xarxa IP.
- **Alimentació:** El sistema inclourà fonts d'alimentació supervisades i bateria de respatller per assegurar-ne el funcionament davant de talls de subministrament elèctric. La instal·lació elèctrica del sistema ha de complir el Reglament Electrotècnic de Baixa Tensió.

Detecció i alarma d'incendis

Disseny Basat en Prestacions (DBP)

- **Concepte de DBP:**
 - És una metodologia de treball estructurada aplicable a qualsevol estudi prestacional.
 - Permet l'estudi precís de les conseqüències d'un incendi en un edifici concret.
- **Metodologia del DBP:**
 - Fase inicial d'anàlisi dels riscos de l'incendi sovint mitjançant avaluació probabilística.
 - Generació d'una matriu de risc per ubicar-hi riscos i assignar un índex de risc global.
 - Avaluació dels escenaris més desfavorables amb índex de risc global sever.
- **Pilars de l'anàlisi prestacional:**
 - Utilització de mètodes analítics o models informàtics (models de zona) per obtenir temperatures i lleis temps-temperatura.
 - Consideració de paràmetres com la geometria, característiques de tancaments i propietats del combustible.

Detecció i alarma d'incendis

Zonificació i àrees de detecció obligatòria

- **Propòsit de la Zonificació:**

- La zonificació del sistema d'alarma d'incendi facilita la ràpida identificació de la ubicació de l'incendi per part dels serveis d'emergència.
- Permet una notificació ràpida als ocupants.

- **Criteris Generals de Zonificació:**

- El sistema s'ha de zonificar per correspondre amb la distribució de l'edifici.
- Això pot incloure la zonificació per planta o per àrea d'ús.
- Es recomana crear zones separades per al pavelló esportiu principal, les sales auxiliars i les àrees exteriors.

Detecció i alarma d'incendis

Elements de detecció: Tipus de detectors i detecció de gasos

- **Tipologies de detectors d'incendi:**

- **Detectors de fum:** Inclouen iònics, fotoelèctrics i de detecció per aspiració (ASD). Crucials per a la detecció primerenca del fum.
- **Detectors de calor:** De temperatura fixa o velocitat d'augment. Adequats on el fum no és apropiat.
- **Detectors multisensor:** Combinen tecnologies de fum i calor.
- **Detectors de flama:** Detecten la presència de flames.

- **Dispositius d'activació manual:**

- Cal instal·lar punts de trucada manuals (polsadors).
- Ubicació: prop de totes les sortides i en ubicacions estratègiques al llarg de les rutes d'evacuació.

- **Consideració de detecció de Gasos:**

- Els detectors de monòxid de carboni (CO) són importants en àrees amb fonts potencials de CO, per exemple en aparcaments interiors o subterranis.

Detecció i alarma d'incendis

Elements de detecció: Selecció i ubicació per zones

Zona	Tipus de detector recomanat	Justificació de la selecció
Pavellons	Detector de fum fotoelèctric o detector multisensor	Detecció primerenca d'incendis latents a àrees grans
Oficines	Detector de fum fotoelèctric	Detecció primerenca a àrees d'oficina
Cuines/Office	Detector de calor (velocitat d'augment)	Menys propens a falses alarmes per vapor o fum
Vestuaris amb dutxes	Detector de calor (temperatura fixa)	Adequat per a ambients humits
Magatzems d'equips	Detector de fum fotoelèctric, o detector de fum per aspiració (ASD) per a àrees d'alt valor	Detecció primerenca en materials emmagatzemats, ASD per a detecció molt primerenca d'actius
Passadissos i zones de circulació	Detector de fum fotoelèctric o detector multisensor	Detecció primerenca a rutes d'evacuació

Detecció i alarma d'incendis

Integració amb altres sistemes: Sistemes complementaris

- **Integració amb la seguretat general:**

- El disseny de la seguretat en grans pavellons esportius inclou l'avaluació de riscos en àrees com l'emergència i l'evacuació.
- La detecció és part del pla general de seguretat.

- **Integració amb sistemes d'evacuació:**

- La detecció d'incendis està estretament lligada als sistemes d'evacuació.
- Els plans d'evacuació són rellevants i esmentats en el context del RIPCI.
- Les rutes d'evacuació s'han de detallar al projecte.

- **Sistemes de senyalització i enllumenat d'emergència:**

- El RIPCI considera els sistemes de senyalització luminiscent. Els instal·ladors es poden encarregar de col·locar senyals i plànols d'evacuació.
- La senyalització ha de ser coherent amb l'evacuació.
- L'enllumenat d'emergència ha d'entrar en funcionament davant de fallades de tensió, i és crucial a les rutes d'evacuació. Els itineraris accessibles per a persones amb discapacitat requereixen senyalització específica.

Detecció i alarma d'incendis

Integració amb altres sistemes: Requisits per al sistema d'incendis

- **Connexió a Central Receptora d'Alarmes (CRA):** Per ser plenament operatiu i permetre una gestió professional dels senyals, el sistema de detecció d'incendis ha d'estar connectat a una CRA degudament enregistrada i autoritzada. Això és fonamental per a la recepció, la verificació i la gestió d'alarmes les 24 hores. Les comprovacions de manteniment d'un sistema de detecció d'incendis inclouen el test de connexió a la CRA.
- **Infraestructura de xarxa i cablejat adequats:** Un cablejat correcte i una infraestructura de xarxa apta són crucials per a l'exercici i la gestió dels sistemes de seguretat, inclòs el de detecció d'incendis. Els problemes i errors en els equips sovint es deuen a infraestructures deficientes o de baixa qualitat. És vital utilitzar materials de qualitat i sota estàndards normatius per assegurar una major seguretat i evitar pèrdues o sorolls al senyal.
- **Suport per a comunicació bidireccional:** L'evolució dels sistemes de detecció d'incendis inclou centrals bidireccional avançades. La comunicació bidireccional és important perquè la CRA pugui monitoritzar l'estat del sistema, verificar senyals (incloent-hi videoverificació) i gestionar el sistema remotament.

Detecció i alarma d'incendis

Integració amb altres sistemes: Requisits per al sistema d'incendis

- **Capacitat d'integració amb altres sistemes:** el sistema de detecció d'incendis ha de tenir la compatibilitat o les interfícies necessàries per integrar-se amb altres sistemes de seguretat com la videovigilància (VMS), la gestió d'informació de la seguretat física (PSIM) i el control de processos (SCADA). Això permet que els sistemes intercanviïn informació i actuïn de manera conjunta.
- **Fiabilitat dels elements de detecció i control:** l'eficàcia de la integració depèn de la fiabilitat dels elements individuals.
- **Manteniment regular del Sistema:** Un requisit fonamental per assegurar el funcionament correcte i la integració eficaç és el manteniment regular del sistema de detecció d'incendis, així com dels sistemes de videovigilància i control d'accessos amb què s'integra.

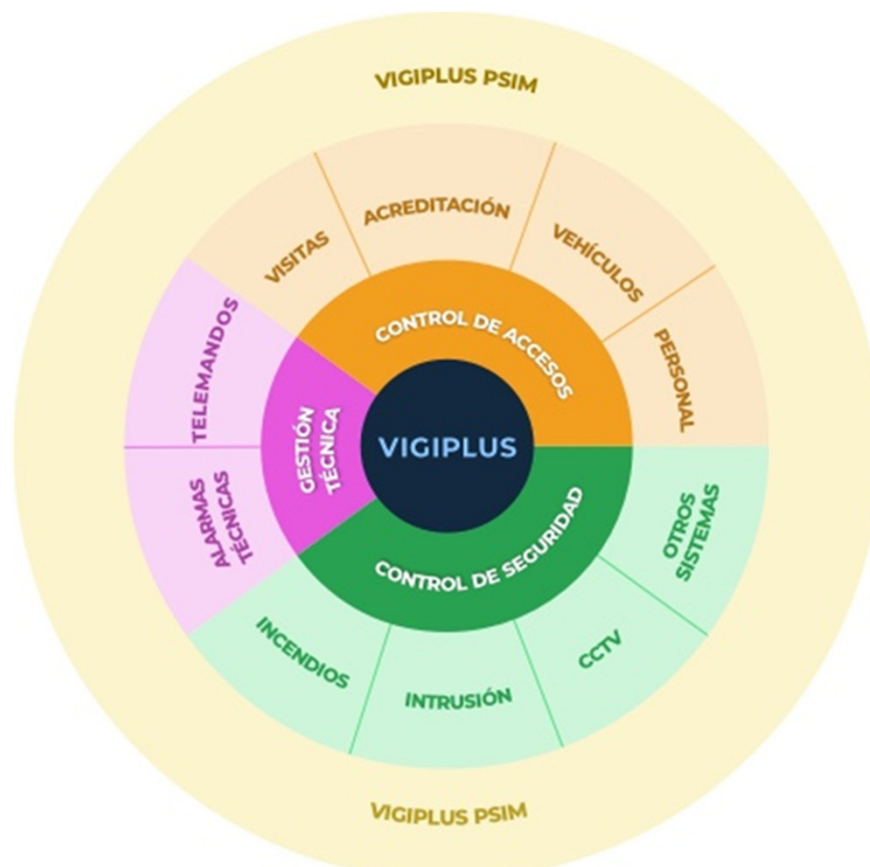
Subsistemes auxiliars

- Inclou SAls, servidors milestones, Racs, Switz i d'altres elements de TIC's i Sistemes.
- Barreres i portes automàtiques per operar en remot.
- porta-armes i integració amb sistemes intel·ligents d'edificis (BMS).
- Altres subsistemes auxiliars a concretar.

PSIM

(Physical Security Information Management)

- Plataforma de gestió que integra tots els subsistemes en una única interfície per al control i anàlisi d'incidents (Vigiplus)



Centre de Control de Seguretat: Comunicacions i gestió centralitzada

- Centres de control amb interfícies gràfiques per a la gestió remota i coordinada de la seguretat.
- Renovació Centre de Control Palau Sant Jordi de tota l'anella olímpica (Estadi Olímpic, Palau Sant Jordi, Sant Jordi Club, Explanada Olímpica).
- Connexió amb el Centre de Control de Seguretat de Calabria i Servei Central amb les Operacions. Operacions en remot.
- Creació UCO al Sant Jordi Club
- Millora i renovació UCO del Palau Sant Jordi