Budapesti és Pest Megyei Mérnöki Kamara

MMK kötelező szakmai továbbképzés Gyengeáramú rendszerek I.

CCTV és vagyonvédelmi rendszerek

A biztonság fogalma

Vkinek, vminek (veszélytől, kártól, jogtalan beavatkozástól, bántódástól való) védett állapota, helyzete. (MÉK)

A biztonság a fizikai veszély hiányát, vagy az e veszéllyel szembeni védelmet jelenti. (UNESCO)

A biztonság célja

Olyan környezet biztosítása, amely hozzájárul az ember harmonikus, békés fejlődéséhez, az egyén kiegyensúlyozott életének, egészségének megóvásához, jó közérzetének kialakításához, az életfeltételek, a megteremtett javak fennmaradásához.

A biztonság és a kényelem összege állandó!

Tehát, ha valamelyik növekszik, a másik szükségszerűen csökken!

A biztonság és a kényelem összege állandó!

Ennek szellemében kell a biztonságvédelmet felépíteni és a fennálló, biztonságot veszélyeztető kockázatokkal ARÁNYOS védelmet megteremteni!

A biztonság területei

- Fizikai biztonság
- Műszaki, technikai biztonság
- Logikai biztonság
- Szervezeti (humán) biztonság

Fizikai biztonság

- élőerős őrzés, fegyveres őrzés
- mechanikai védelem (falak, rácsok, ajtók, ablakok)
- hagyományos biztonságtechnikai rendszerek (behatolás- és támadásjelző, beléptető, videomegfigyelő, riasztásátviteli, távfelügyeleti rendszerek)
- levél és csomagellenőrzés
- gépjármű behajtás kontrollja fizikai akadállyal
- villám- és túlfeszültség-védelem
- villámhárítók
- többszintű túlfeszültség levezetők
- biztonsági zónák galvanikus (jellemzően optikai) elválasztása

Fizikai biztonság

- passzív tűzvédelem
  - nem, vagy nehezen éghető anyagok alkalmazása
  - dohányzás és nyílt láng használat tiltása
- vízbetörés és oltóvíz elleni védelem
  - épület elhelyezése
  - épület szerkezeti kialakítása
  - vízmentes oltórendszer
- mechanikai rezgések elleni védelem
- elektromágneses kompatibilitás (electromagnetic compatibility - EMC)

Műszaki technikai biztonság

- tápáramellátás
  - külső tápáramellátás
    - kétirányú betáplálás jelentősen független elosztói hálózatokból
    - saját, a telephelyen belül található transzformátor állomás
  - szünetmentes tápegységek (Uninterruptible Power Supply – UPS)
  - szükségáramforrások
    - autonóm (más közművektől független) aggregátorok
- klimatizálás és légtechnika
  - hűtés
  - páratartalom szabályozás
- aktív tűzvédelem
  - tűz- és füstjelzés
  - automatikus tűzoltórendszerek
  - oltógáz, oxigén kiszorítás
- automatikus üzemfelügyelet
- kábelmenedzsment
  - külső adatkapcsolatok redundáns, független nyomvonalakon

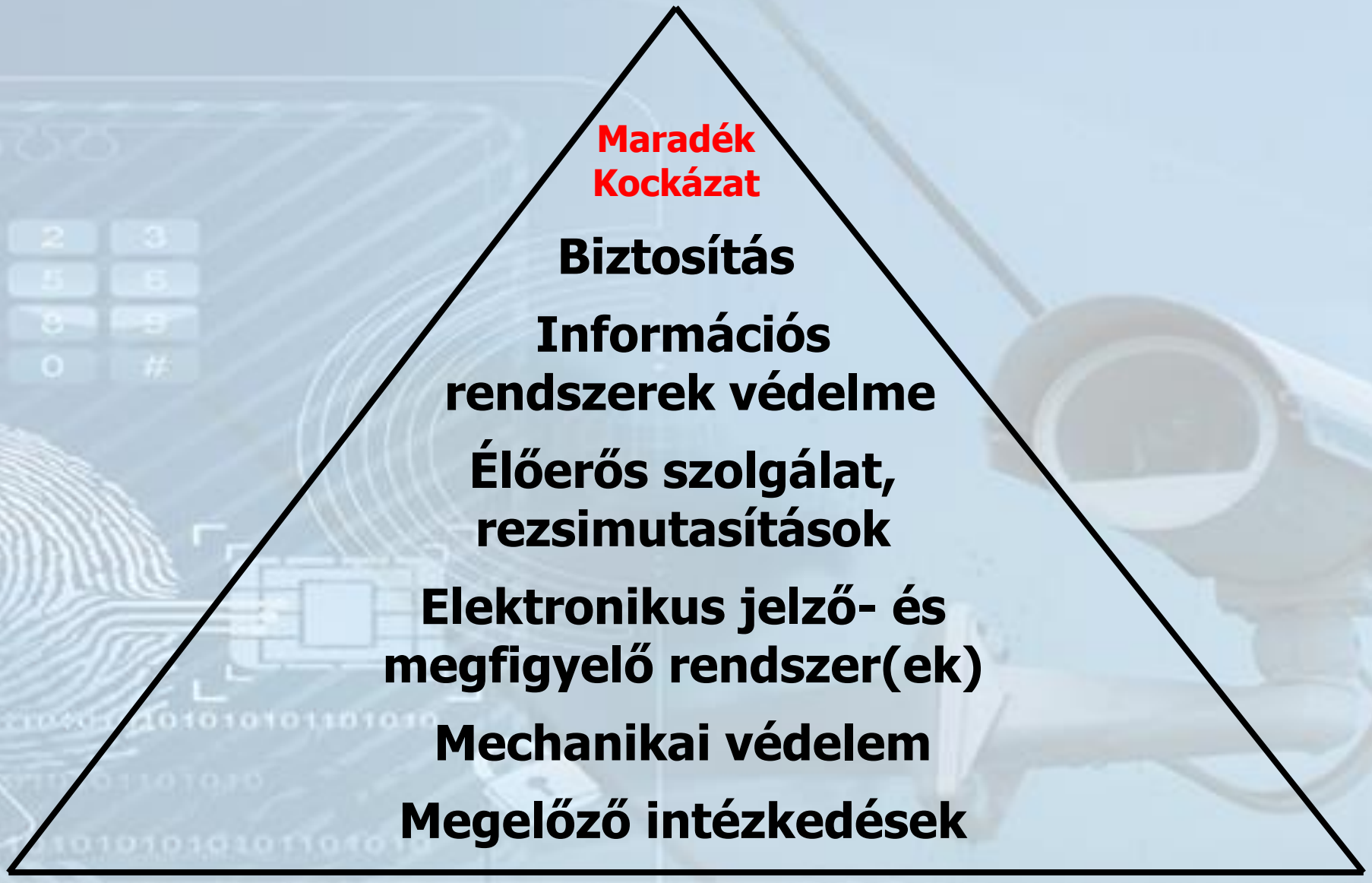
Logikai biztonság

- hozzáférés szabályozás
- információtechnológiai eszközök és eljárások
- védelmi rendszerek log elemzése
- titkosítási algoritmusok
- fizikai és IT környezet változáskezelés
- karbantartás és hibaelhárítás menedzsment
- fizikai adathordozók kezelése
- javítás, csere, selejtezés, megsemmisítés

Szervezeti (human) biztonság

- menedzsment-kontroll,
- vállalati célkijelölés, erőforrástervezés, a magatartás befolyásolás és a beszámolás,
- a kontrolling pénzügyi, számviteli szakterülete: számviteli ellenőrzés, könyvvizsgálat, függetlenített belső ellenőrzés, minőségbiztosítás, alapfolyamatok elemzése, hibákat feltáró, visszacsatoló eszközrendszerek termék és szolgáltatás szabványok szerinti előállítása,
- etikus szervezeti magatartás (pl. biztonsági kultúra fogalomköre),
- szándékos visszaélések feltárása és megakadályozása, fraud menedzsment,
- csalás elleni stratégia (CAFS),
- biztonságtudatosság megteremtése.

Komplex védelem, Biztonságvédelmi háromszög



Elektronikus jelző- és megfigyelő rendszerek

- Behatolás- és támadásjelző rendszerek;
- beléptető rendszerek;
- videomegfigyelő rendszerek;
- kombinált és integrált rendszerek;
- távfelügyeleti rendszerek;
- tűzjelző rendszerek.

Védendő objektumok

- lakóépület (lakás, családi ház, garázs, stb);
- középület (iskola, könyvtár, kórház, stb);
- speciális középület (múzeum, bemutató és kiállítóterem, vásár-, egyéb csarnok, stb);
- ipari objektum (gyár, erőmű repülőtér, stb);
- katonai objektum;
- kritikus infrastruktúra;
- pénzintézet;
- stb.

A védelem jellege

- Felület (héj) védelem
- Térvédelem
- Tárgyvédelem
- Személy (ember) védelme

- Beltéri védelem
- Kültéri védelem

Mi is az a szabvány?

Az 1995. évi XXVIII. törvény szerint:

1. számú melléklet (1) pont: *A szabványosítás* olyan tevékenység, amely *általános és ismételten alkalmazható megoldás*okat ad fennálló vagy várható problémákra azzal a céllal, hogy a rendező hatás az adott feltételek között a legkedvezőbb legyen.

4. § (1) *A szabvány* elismert szervezet által alkotott vagy jóváhagyott, *közmegegyezéssel elfogadott* olyan *műszaki* (technikai) *dokumentum*, amely tevékenységre vagy azok eredményére vonatkozik, és olyan általános és ismételten alkalmazható szabályokat, útmutatókat vagy jellemzőket tartalmaz, amelyek alkalmazásával a rendező hatás az adott feltételek között a legkedvezőbb.

Mi is az a szabvány?

A ***közmegegyezés*** nemzetközileg elfogadott meghatározása a következő:
" Közmegegyezés: olyan általános megegyezés, amelyet az jellemez, hogy a lényeges kérdésekben nincs fenntartott ellenvéleménye az érdekek egyik fontos csoportjának sem, továbbá, hogy az eljárás során minden érdekelt véleményét igyekeztek figyelembe venni, és megoldást találni minden ütköző álláspontra.
A közmegegyezés nem szükségképpen jelent egyhangú véleményt."
A közmegegyezés tükrözi a szabványok önkéntes jellegét. Ez biztosítja azt, hogy a szabványt az érintett felek támogatják, és elkészítésével önkéntes elkötelezettséget vállaltak a szabvány használatára.

Magyar Szabványügyi Testület

A Műszaki Bizottság azonosító jele: **MSZT/MB 816**

A Műszaki Bizottság neve: **Riasztórendszerek**

MSZ EN 50130-x	Elektromágneses összeférhetőség és Környezetállósági vizsgálati módszerek;
MSZ EN 50131-x	Behatolás- és támadásjelző rendszerek;
MSZ EN (IEC) 62676-x	Video-megfigyelőrendszerek biztonsági alkalmazásokhoz;
MSZ EN (IEC) 60839-11-x	Elektronikus beléptető rendszerek;
MSZ EN 50134-x	Segélyhívó rendszerek;
MSZ EN 50136-x	Riasztásátviteli rendszerek;
MSZ EN 50518	Riasztásfogadó központok;
MSZ EN 50661-x	Kültéri héjvédelmi biztonsági rendszerek;
MSZ EN 16763	A tűzvédelmi és biztonsági rendszerekre vonatkozó szolgáltatások;
MSZ EN (IEC) 62820-x	Épületek intercom-rendszerei;

Behatolás- és támadásjelző rendszerek

Egy behatolás- és támadásjelző rendszer részegységei, alkotóelemei:

- **központ / bővítő modulok;**
- **tápegységek;**
- **kezelőegységek;**
- **automatikus érzékelők;**
- **kézi jelzésadók (támadásjelző);**
- **kiegészítő I/O modulok;**
- **az eszközök összeköttetését biztosító hálózat. Az összeköttetés általában vezetékes, de egyre inkább használatosak a vezeték nélküli, azaz a rádiós megoldások.**

- **Alapvetően megkülönböztetünk kültéri és beltéri rendszereket!**

Biztonsági fokozatok

1. fokozat: Alacsony kockázat
A behatolónak vagy a rablónak vélhetően kevés ismerete van a behatolás- és támadásjelző rendszerekről, és csak korlátozott mennyiségű, könnyen hozzáférhető szerszámok állnak rendelkezésükre.

2. fokozat: Alacsony és közepes közötti kockázat
A behatolónak vagy a rablónak vélhetően korlátozott ismerete van a behatolás- és támadásjelző rendszerekről, és általánosan használatos szerszámokkal továbbá hordozható műszerekkel rendelkezik (pl. egy multiméter).

3. fokozat: Közepes és magas közötti kockázat
A behatoló vagy a rabló vélhetően jártas a behatolás- és támadásjelző rendszerekben, és a szerszámok, hordozható elektronikus készülékek széles körű választékával rendelkezik.

4. fokozat: Magas kockázat
Akkor alkalmazandó, ha a biztonság minden más tényezőnél előbbre való. A behatoló vagy rabló vélhetően képes részletesen megtervezni egy behatolást vagy rablást, rendelkezik ehhez erőforrásokkal, és rendelkezik a berendezések teljes skálájával, beleértve olyan eszközöket is, amelyekkel a behatolás- és támadásjelző rendszer alapvető fontosságú részegységeit helyettesítheti.

Behatolás- és támadásjelző rendszerek

Jellegzetességek:

- **Minden automatikus érzékelő folyamatosan működik, csak a központi funkciót ellátó eszközök státuszállapotától függ, hogy az adott esemény kivált-e valamilyen értesítést.**
- **Az értesítés lehet helyi vagy távoli.**
- **Vegyük figyelembe, hogy az érzékelők valamilyen fizikai jelenséget, változást alakítanak át villamos jellé és az aktív eszközök (pl.: mozgás és üvegtörés érzékelők) elemzik azt!**
- **A passzív eszközök „csak kapcsolgatnak” (nyitás és rezgésérzékelők)**
- **A hatékonyan üzemelő rendszer létrehozásához elengedhetetlen és szükségszerű az alkalmazott eszközök működési elvének alapvető ismerete!**

Behatolás- és támadásjelző rendszerek

Jellegzetességek:

- **Fontos a védendő területen a kockázatfelmérés és kockázatértékelés elvégzése és ez alapján kell, hogy történjen a biztonsági fokozatokba sorolás.**
- **Emellett nagyon fontos figyelembe venni a védendő objektum jellegét, sajátosságait, üzemel(te)évelkapcsolatos ismérveket.**
- **Ne feledjük, a rendszer megrendelőjének felelőssége az „arányos” védelem kialakítása (kockázat<->biztonsági fokozat).**
- **Az üzemeltetés során fontos a rendszeres karbantartás, sok környezeti változás befolyásol(hat)ja a hatékony működést!**
- **A téves riasztások száma jelentősen befolyásolja a rendszerek általános megítélését, működésének hatékonyságát!**

Beléptető rendszer

- Komplex elektromechanikai-informatikai rendszer, amely telepített ellenőrző/áthaladási pontok segítségével lehetővé teszi objektumokban történő személy- és járműmozgások hely-, idő- és irány szerinti engedélyezését vagy tiltását, az események nyilvántartását, visszakeresését.
- Felügyeli és kijelzi az ellenőrző/áthaladási pontok állapotát.
- Rendkívüli helyzetekre automatikusan reagál (pl.: tűz).
- A fizikai alkotóelemeken kívül tartalmazza azokat az intézkedéseket és apparátusokat melyek a rendszer hatékony üzemeltetéshez és a beléptetés felügyeletéhez szükségesek!

Beléptető rendszer szükségessége

- A védett terület biztonsága megköveteli
- Biztonságos (nehezen hamisítható) belépési kulcsra van szükség
- A belépőt azonosítani kell
- Tudni kell a védett területen tartózkodók számát
- Limitálni kell a védett területen tartózkodók számát
- Azonosítani kell a védett területen tartózkodókat
- Ki kell zárni a belépési jogosultság átruházásának lehetőségét
- Ki kell zárni, hogy jogosult beengedjen jogosulatlant
- Ki kell zárni a belépési kulcsok illetéktelenek általi felhasználását
- A belépést időben korlátozni kell
- Tudni kell, hogy az azonosított hol tartózkodik
- Tudni kell, hogy valaki mikor ment be, és mikor távozott
- Tudni kell, hogy egy adott területen ki, mennyi ideig tartózkodott
- Folyamatosan változik a belépésre jogosultak köre
- Egy átjáróhoz háromnál több kulcs kell
- Egy személynek háromnál több kulcsra van szüksége
- A belépésért díjat kell fizetni
- A védett területen való tartózkodásért (időarányos) díjat kell fizetni
- A védett területre való belépés különleges technológiai eljárást igényel

Beléptetés fázisai

Áthaladni szándékozó azonosítása

Belépési jogosultság kezelése - hely, idő, irány

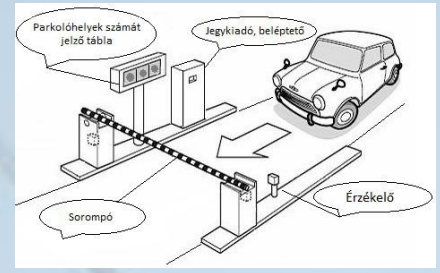
Működtető vezérlése (áthaladás engedélyezése)

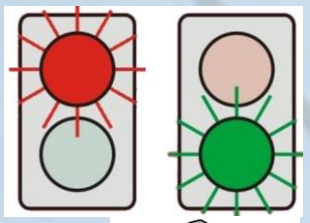
Áthaladás detektálása, visszazárás

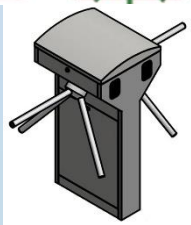
A rendszer folyamatos felügyelete

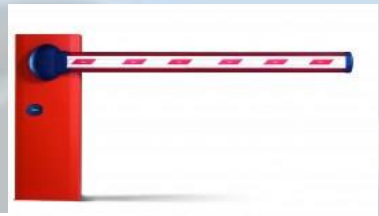
Események rögzítése, tárolása

Kommunikáció

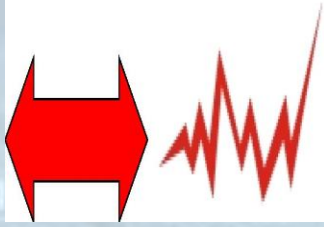








Behatolás	2006.02.10. 09:47:00	110. Fejlesztés		0
Ki normál	2006.02.10. 09:45:00	Első bejárat	Kiss Kálmán	694
BE normál	2006.02.10. 09:45:00	110. Fejlesztés	Laczkó Tünde	2537
Ki külső munkára	2006.02.10. 09:44:00	Főbejárat	Kerecsényi Kornél	2513



Beléptető rendszer biztonsága

- Azonosítás biztonsága
  - Azonosításra használt eszközök, jellemzők, adatok és adat utak (pl. RF kommunikáció, olvasó vezetékek, stb.) védelme megismerés, másolás, ismétlés, lopás, átadás ellen
- Akadályozás (védett tér elhatárolás) biztonsága
  - Mechanikai ellenállás, leküzdhetőség (a beléptető kapuk, valamint a beléptető rendszer részét nem képező, de a védett teret elválasztó határoló szerkezetek is)
  - Vezérlések, állapot jelzések manipulálása (kijátszás, szabálytalan nyitás, nyitott állapotban tartás)
  - Szingularizáció (egy azonosítás, egy áthaladás)
  - Vészhelyzet állapotok (vésznyitó, tűzjelző, stb.) téves aktiválása

Beléptető rendszer biztonsága

- Rendszer üzemeltetés biztonsága, önvédelme
  - Szabotázs védelem (részegységek, vezetékhálózatok megbontása)
  - Rendellenes használat észlelése, szankcionálása (pl. zárás akadályozása, vésznyitó működtetés, stb.)
  - Kommunikáció titkossága (pl. olvasó, vezérlő, felügyeleti rendszer)
  - Energia ellátás
- Informatikai támadások elleni védelem
  - Külső támadások (IP hálózat)
  - Belső adat utak (állapot jelzések, vezérlések, részegységek közötti kommunikáció)
- Hibatűrés
  - Viselkedés hibaállapotban (nyitott, zárt)
  - Informatikai kapcsolat részleges-teljes elvesztése
  - Részegységek meghibája (tápellátás, olvasó, vezérlő, szerver, adatbázis, kezelői munkaállomás hiba)
- Rezsim intézkedések, reagáló erő

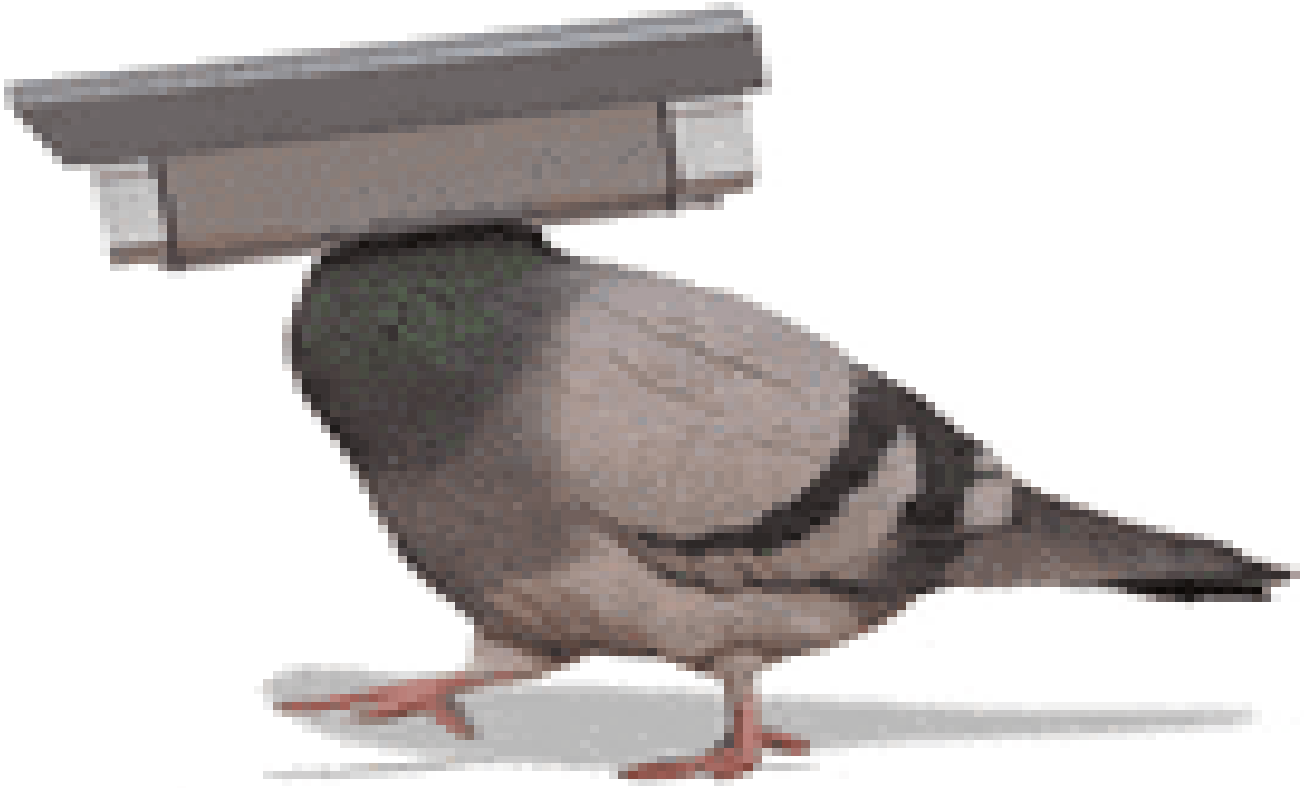
Azonosítások összehasonlítása

	N Kombinációk száma	FAR_{eff} Hamis elfogadás	FRR Hamis elutasítás
PIN **Tudok valamit**	10^{Digit} 4 – 6 digit	Grade1,2<10^{-3} Grade3,4 tilos 5*2*USER/N	0
Kódkulcs **Van valamim**	10^{12} (40 bit)	USER/10^{12}	10^{-7}
Biometrikus **Vagyok valamilyen**	∞	Grade3<0,3% Grade4<0,1% (MSZ EN 60839)	10^{-2} MSZ EN 50133

Videó megfigyelő rendszerek

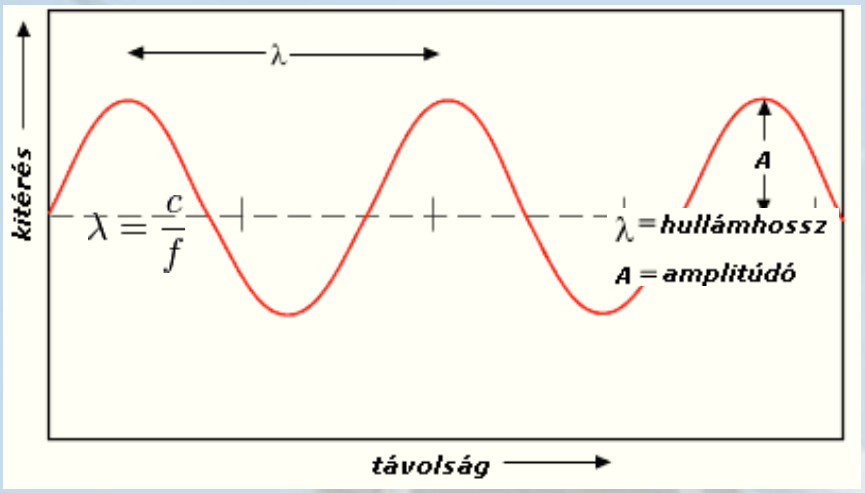
Video Surveillance Systems

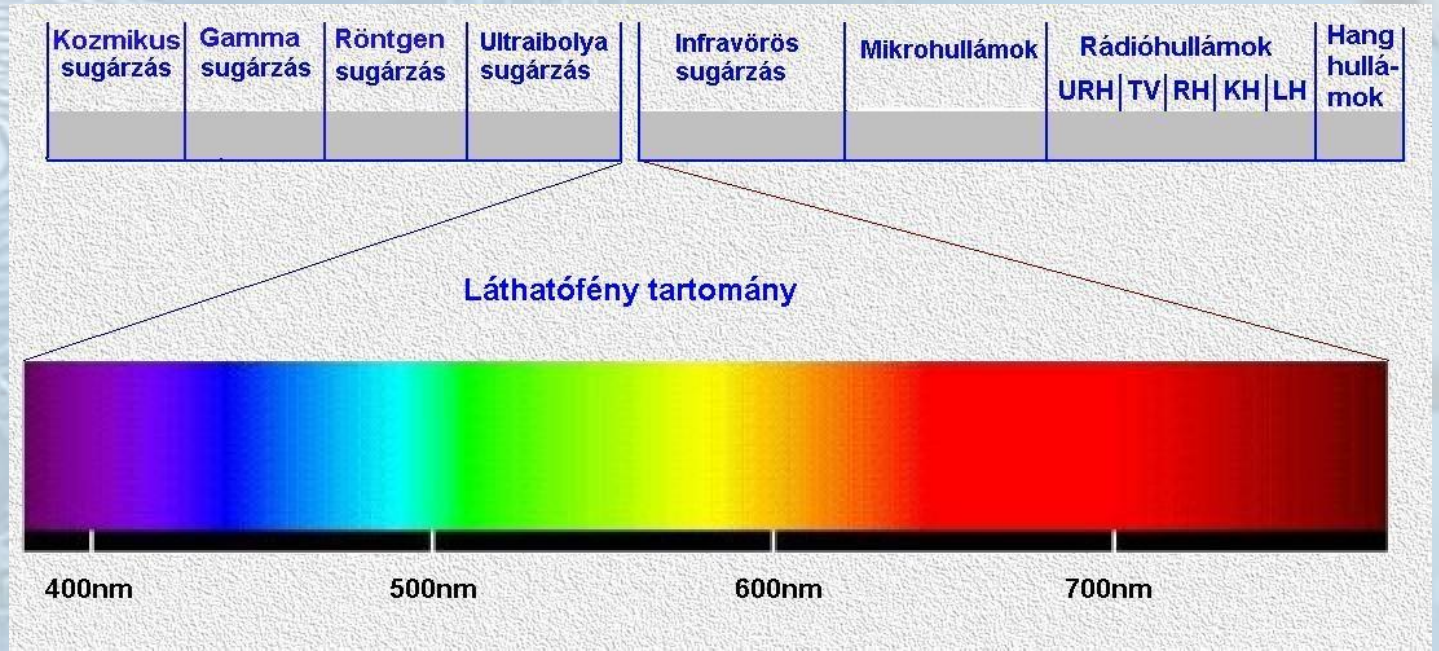
Született: CCTV



A fény (általános iskola, 8, osztály, Fizika tantárgy)

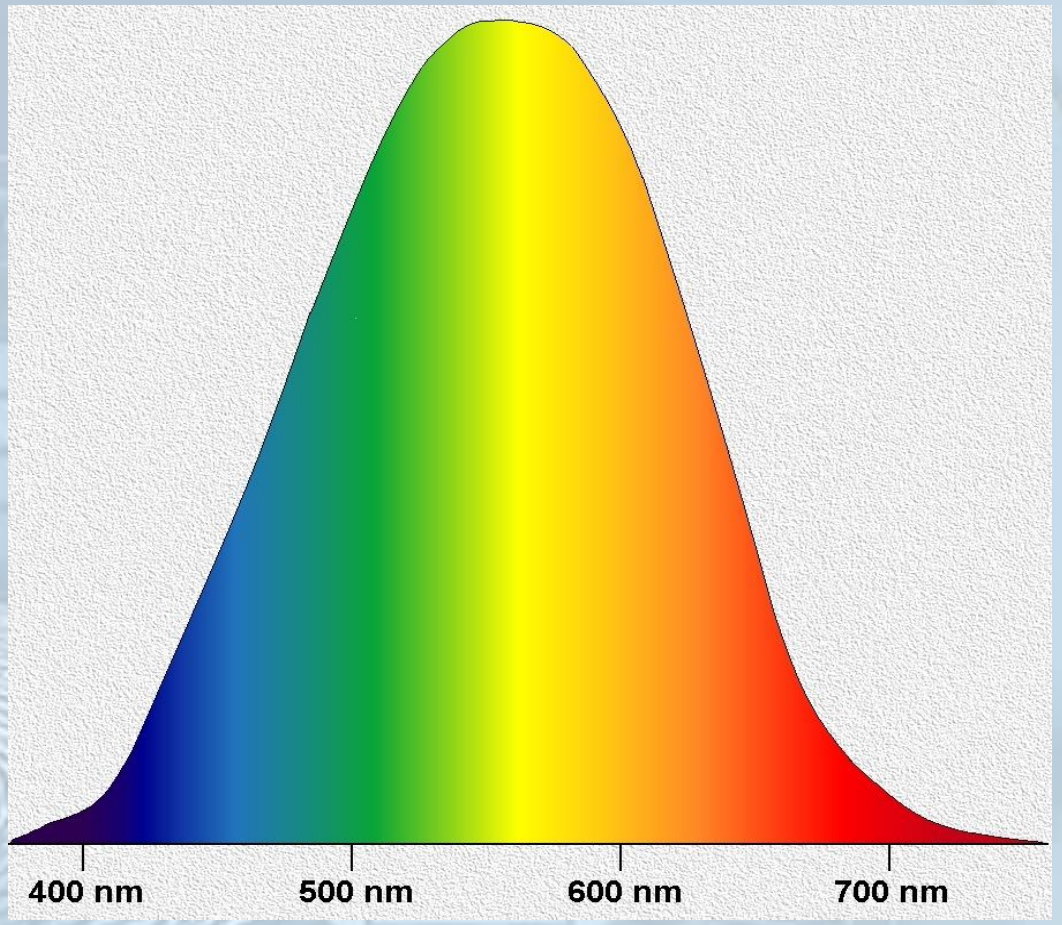
Név	Hullámhossztartomány	Frekvenciatartomány
Hosszúhullám	3km - 600m	10^5 - $5 \cdot 10^5$ Hz
Középhullám	600m - 200m	$5 \cdot 10^5$ - $1{,}5 \cdot 10^6$ Hz
Rövidhullám	100m - 10m	$3 \cdot 10^6$ - $3 \cdot 10^7$ Hz
Ultrarövidhullám	7,5m - 3m	$4 \cdot 10^7$ - 10^8 Hz
Mikrohullám	1,2m - 3mm	$2{,}5 \cdot 10^8$ - 10^{11} Hz
Infravörös fény	600µm - 780nm	$5 \cdot 10^{11}$ - $3{,}8 \cdot 10^{14}$ Hz
Látható fény	780nm - 380nm	$3{,}8 \cdot 10^{14}$ - $7{,}9 \cdot 10^{14}$ Hz
Ultraibolya fény	380nm - 100pm	$7{,}9 \cdot 10^{14}$ - $3 \cdot 10^{18}$ Hz
Röntgensugárzás	37nm - 6pm	$8{,}1 \cdot 10^{15}$ - $5 \cdot 10^{19}$ Hz
Gamma-sugárzás	27pm - 0,5pm	$1{,}1 \cdot 10^{19}$ - $6 \cdot 10^{20}$ Hz
Kozmikus sugárzás	0,02pm - 0,0002pm	$1{,}5 \cdot 10^{22}$ - $1{,}5 \cdot 10^{24}$ Hz

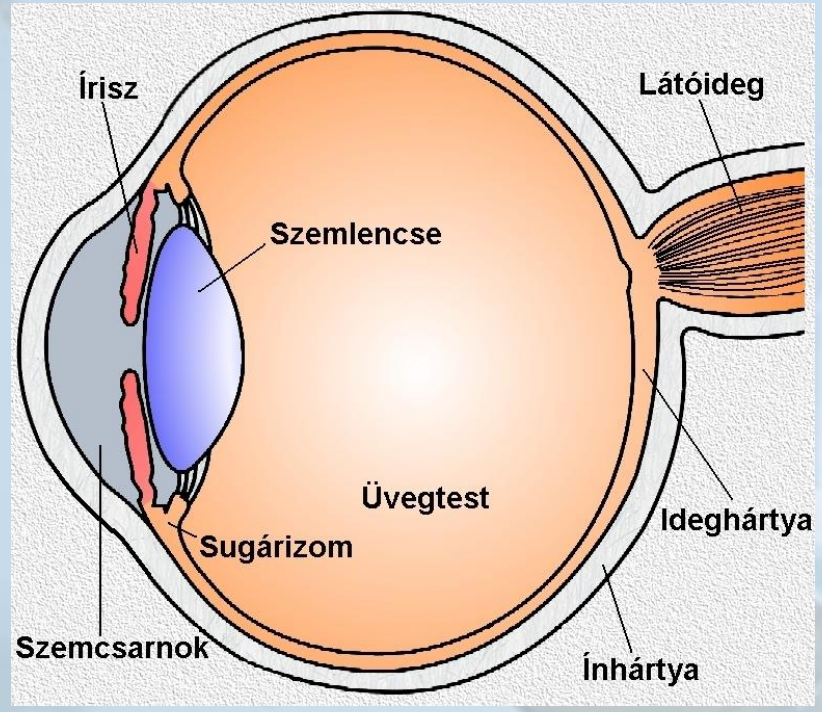




A λ hullámhossz és az *f* (frekvencia) között fordított arányosság van. A hullámhosszt megkapjuk, ha a hullámsebességét (*c*) elosztjuk a frekvenciával.

Átlagos emberi szem spektrális érzékenysége

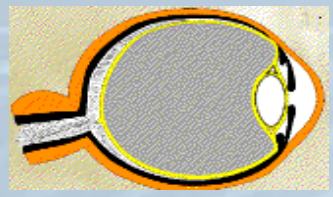




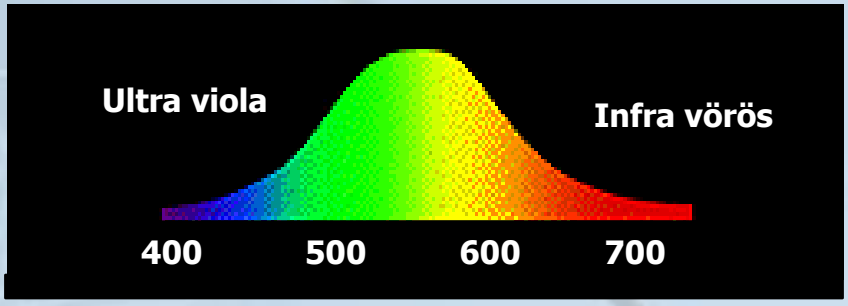
A látott tárgy képét a szemlencse az ideghártya síkjára vetíti. A szemfenéken elhelyezkedő (kb. 0,5mm vastag) ideghártya több rétegből áll. Az ideghártyán áthaladó fény a pálcikák és csapok rétegében okoz ingerhatást. A *pálcikák a gyenge fény felfogására alkalmasak* (már kb. 10^{-12} lux megvilágításnál érzékelnek), és nagy felbontást biztosítanak. A szín feldolgozásában feltehetőleg nem játszanak szerepet.

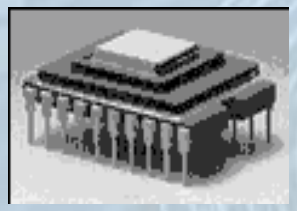
A *színes látást az ún. csapok biztosítják*, melyből három típus (kék-, vörös-, és zöldérzékelő) található. A csapok kb. 0,1 lx megvilágításnál kezdenek el működni. A legérzékenyebben az 555 nm hullámhosszúságú fényre reagálnak.

Spektrális érzékenységek

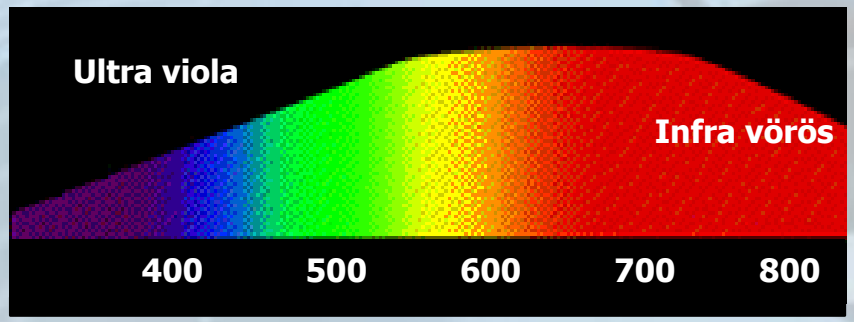


Emberi szem



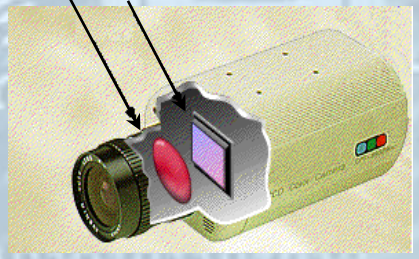


Fekete-fehér CCD

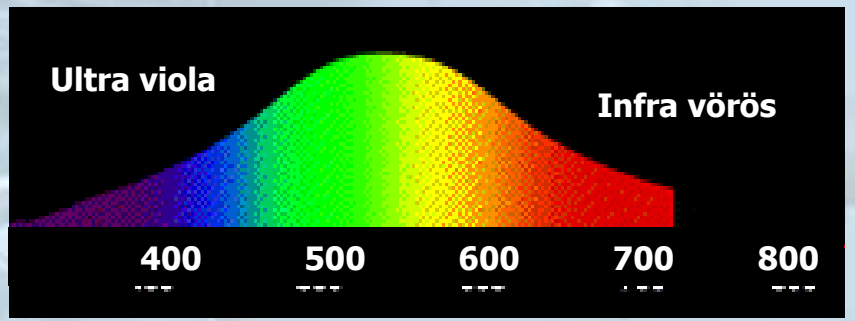


infra szűrő

CCD elem



Színes kamera



Zártláncú TV rendszer

Closed **C**ircuit **T**ele**V**ision

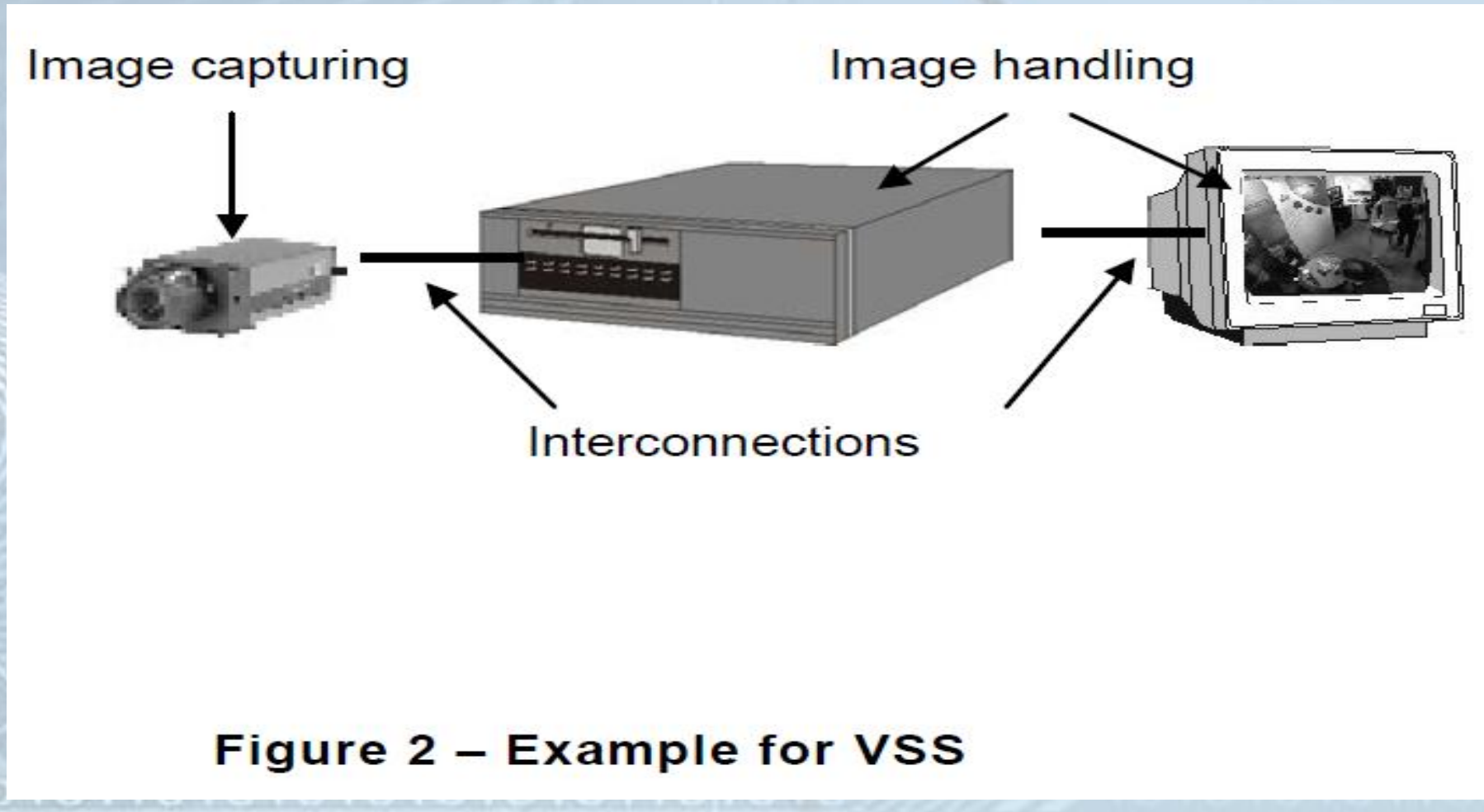
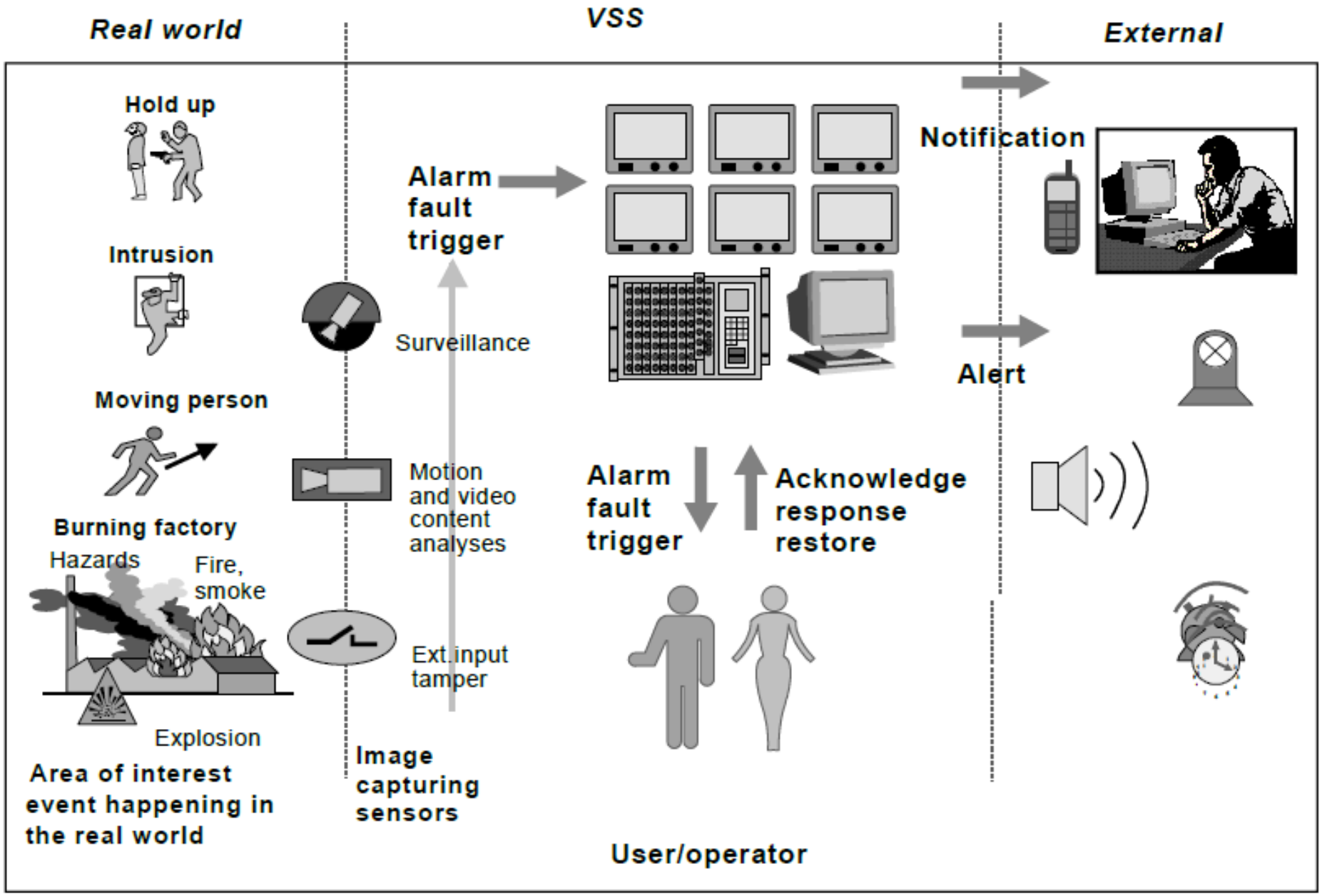


Figure 2 – Example for VSS

Egy valós videotechnikai megfigyelőrendszer



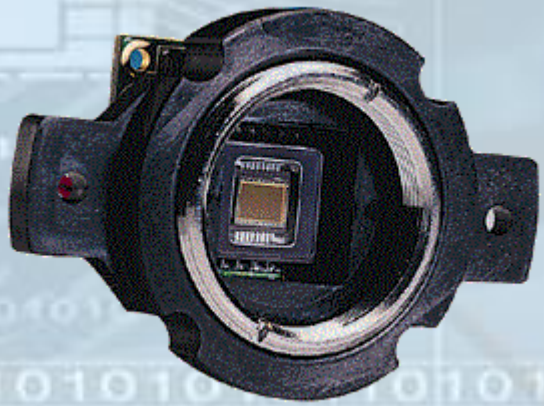
Videotechnikai megfigyelőrendszer biztonsági fokozatai MSZ EN 62676-1-1:2014

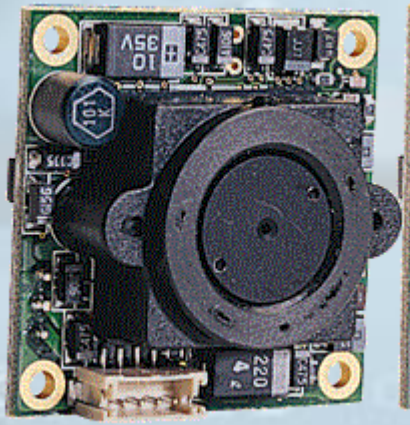
Következmények alatt értjük a személyi sérülést, halált, a személyi tulajdon károsodását, vagy elvesztését, az információ elvesztését és a környezet károsítását.

Valószínűség alatt értjük a következmények előfordulásának valószínűségét, de hatással vannak rá a riasztórendszerek, az élőerős őrzésvédelem, a fizikai védelem (zárak, kerítések, stb.) és a területre jellemző általános kockázati tényezők (társadalmi nyugtalanság, környezeti katasztrófa, stb.)

MSZ EN 62676-1-1:2014 Kockázati tényezők, és biztonsági fokozatok

Kamerák





PTZ (Speed Dome) kamerák

Kamerák

Színes

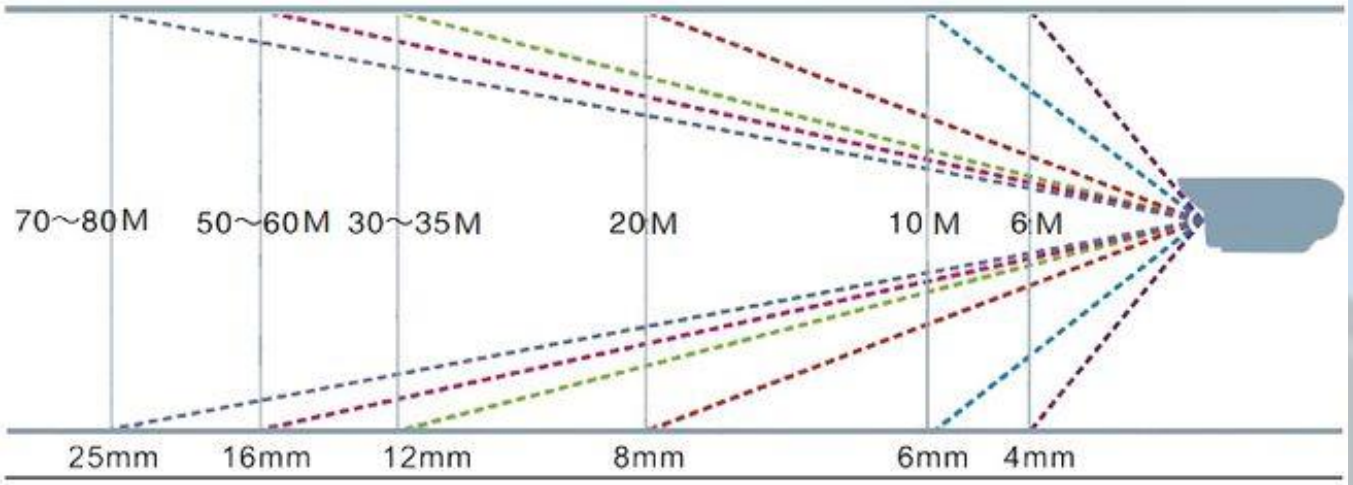
Fekete-fehér

B&W

Day/night

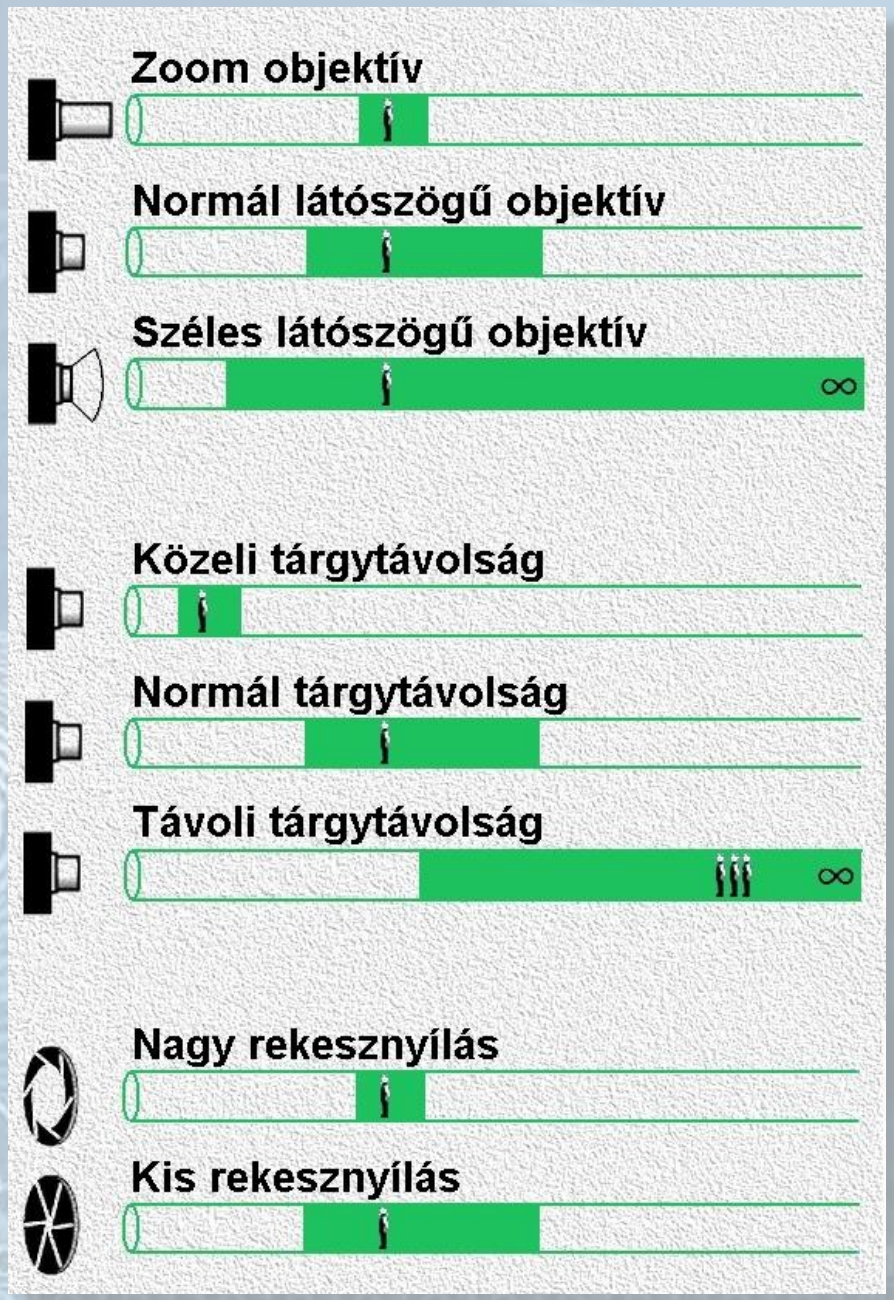
- „valós”
- elektronikus

Lens Size	2. 5mm	2. 8mm	3. 6mm	4mm	6mm	8mm	12mm	16mm	25mm	60mm
View Angle	100°	90°	75°	70°	60°	40°	30°	20°	12°	5°
see clearly the number plate from	1.5M	2M	2.5M	3M	5M	7M	10M	20M	25M	50M
Cover Distance			5	6	10	20	30~35	50~60	70~80	



Pictures taken by the same camera with different size lens

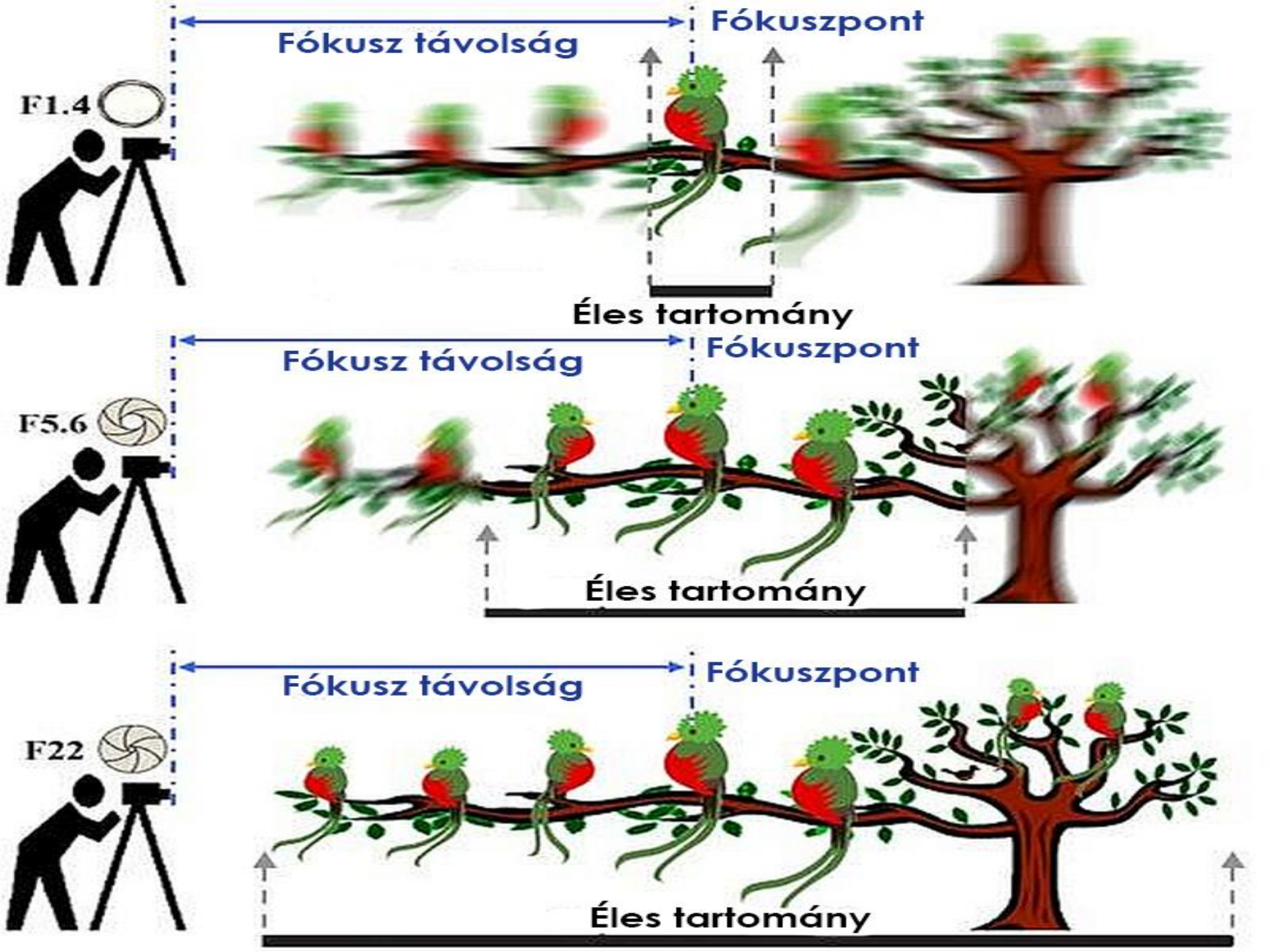
Deep of Field (mélységélesség)



A mélységélesség akkor a legnagyobb, ha széles látószögű az optikánk, és/vagy nagy a tárgytávolság, és/vagy kicsi a rekesznyílás.

Közeli tárgyról általában a mélységélesség egyforma nagyságú a tárgy előtt és mögött.
Normál látószögű objektívet, kis rekeszértékkel használva a tárgy mögött kétszer olyan távolságról kapunk éles képet, mint előtte.
Távoli tárgy-, és fókusztávolság-gal, valamint rekeszeléssel elérhetjük, hogy a tárgy mögött a mélységélesség a végtelenig tartson. Ezt a beállítási távolságot hiperfókusztávolságnak nevezzük.

Az általunk leginkább befolyásolható (megfelelő világítással) az írisz kis rekeszértéken tartása.


Fókusz távolság
Fókuszpont
F1.4
Éles tartomány
Fókusz távolság
Fókuszpont
F5.6
Éles tartomány
Fókusz távolság
Fókuszpont
F22
Éles tartomány

Megvilágítás

Látható fény (kívánatos lenne minden rendszerben, de bizonyos körülmények, sajátos elvárások miatt nem mindenhol és nem mindig alkalmazható).
Infra megvilágítás (850-940nm), a 940nm-nek a hatásfoka 30-40% kisebb!

m

*Turn on the 850nm and 940nm in the office with light on, then use **phone camera to observe** it .*

- As left image see the 850nm IR with light glow showed.

*Turn the office **light off** and close the curtain, then **use phone camera to observe** it .*

- As right image see the 850nm IR with very obvious and strong light shadow under camera observing ; while the beside 940nm only observed in slight red dot.

Wide Dynamic Range

Ma az IP kamerákban a WDR funkció jelentős szerepet játszik!
A WDR funkció használata a képet jelentősen zajosítja, törekedjünk kompromisszumra!

Csőkamera

360º-os, panoráma (panoramic), halszem (fisheye) kamerák

Hő (thermal) kamera

Hő (thermal) kamera

Testhőmérséklet / Maszk ellenőrző kamera

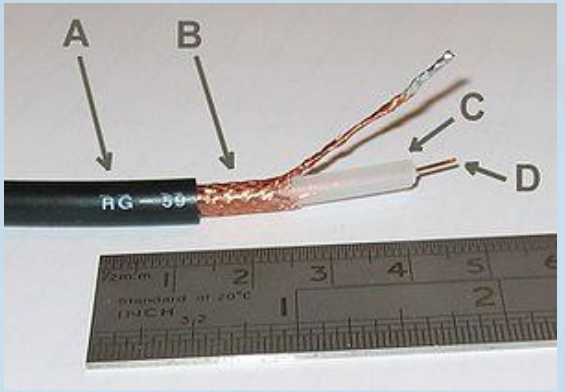
alhua TECHNOLOGY

DH-TPC-BF3221
Thermal Camera

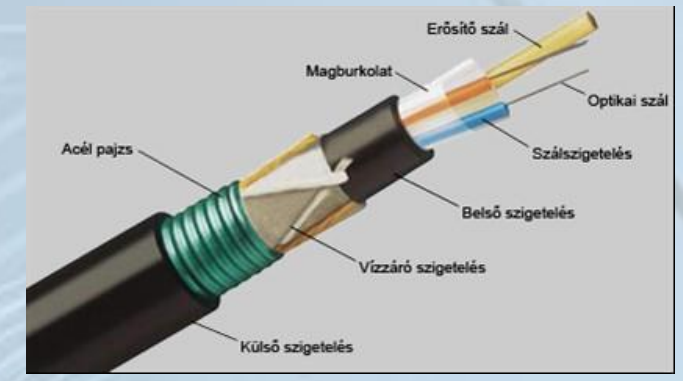
&

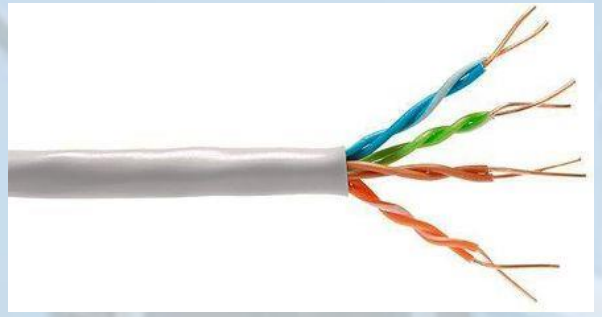
Blackbody

Képátviteli eszközök



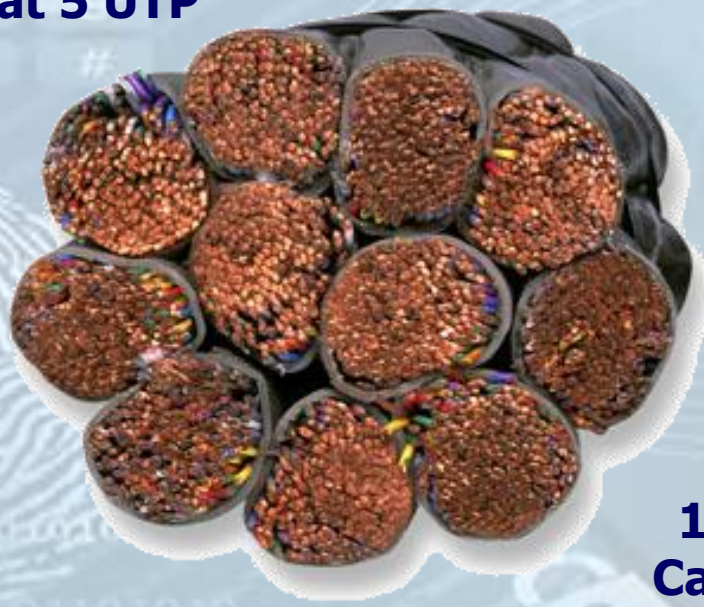
- Koaxiális kábelen
- Optikai kábelen
- Csavart érpáron
- Mikrohullámú képátvitelen
- RF képátvitelen (rádióhullám, WIFI)
- Infravörös képátvitelen
- Lézeres képátvitelen



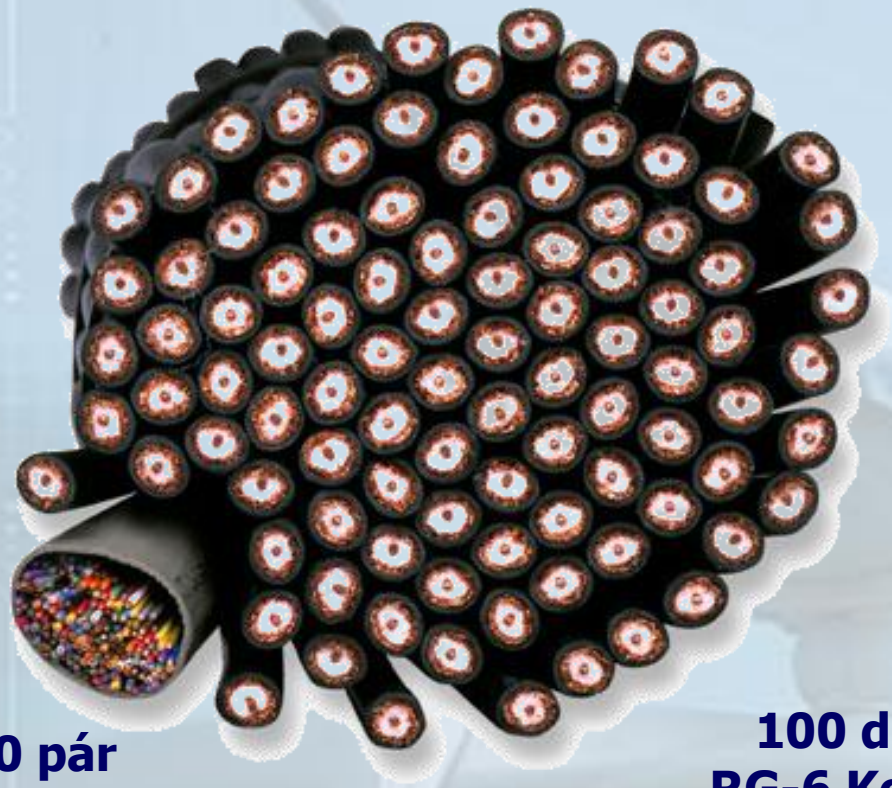


Csavart érpáras képátvitel előnyei

1100 pár
Cat 5 UTP



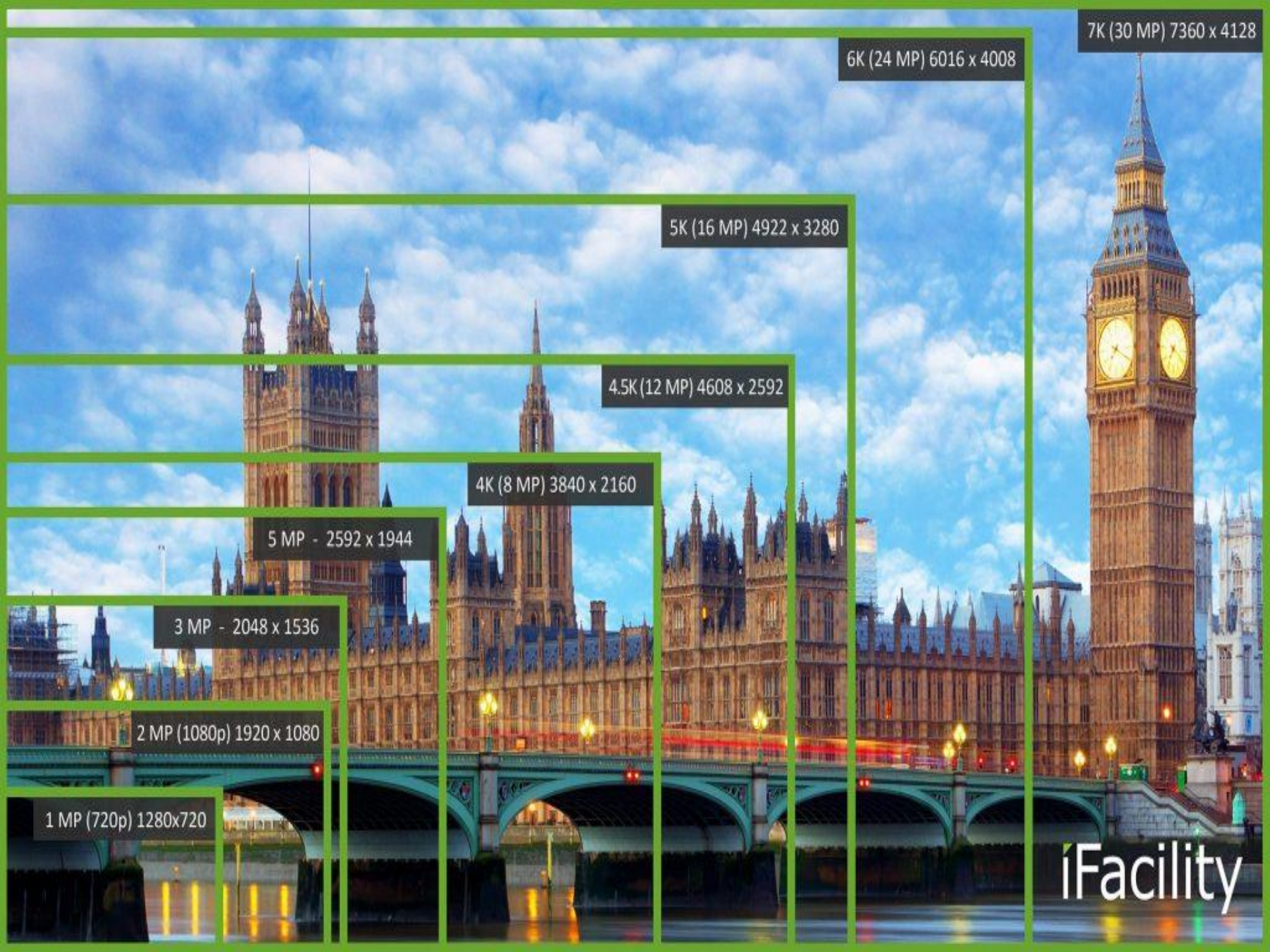
100 pár
Cat 5 UTP



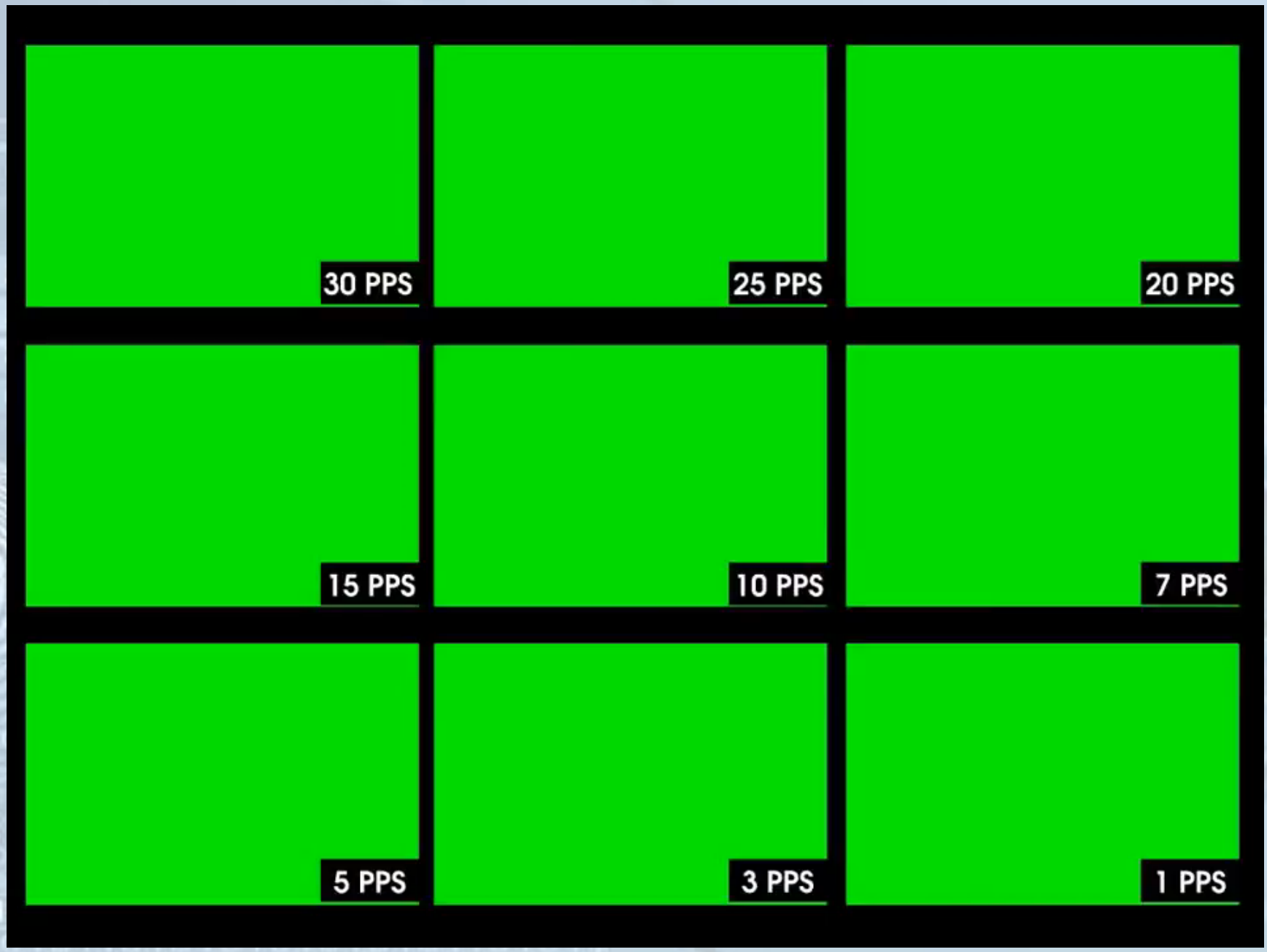
100 db
RG-6 Koax

Digitalizálás

- Analóg videó jelek digitalizálásakor nagy mennyiségű adat keletkezik, ezért célszerű tömörítést alkalmazni.
- Mozgókép tömörítésre két fő módszer ismeretes:
  -minden képet továbbítunk egymás után
  -egy-egy referenciaképet továbbítunk, utána csak a változásokat
- Befolyásoló tényezők:
  -milyen képfelbontás szükséges (Mpx)?
  -milyen képfrekvencia szükséges (FPS)?
  -milyen minőségű képre van szükség (CR)?
  -mekkora sávszélesség áll rendelkezésre (BW)?


7K (30 MP) 7360 x 4128
6K (24 MP) 6016 x 4008
5K (16 MP) 4922 x 3280
4.5K (12 MP) 4608 x 2592
4K (8 MP) 3840 x 2160
5 MP - 2592 x 1944
3 MP - 2048 x 1536
2 MP (1080p) 1920 x 1080
1 MP (720p) 1280x720
iFacility

Legfontosabb IP kamera paraméterek (FPS-PPS)



IP rendszerek kialakulása

- Fejlesztés kezdete: USA, 60-as évek, katonai és kormányzati célra hozták létre.
- Egyetemek bekapcsolódása révén, a felhasználói kör folyamatosan bővült..
- TCP/IP (Transmission Control Protocol) kialakulása.
- Az IP szerepe a csomagok mozgatása a node-k között.
- IP cím szerepe az egyértelmű azonosítás a hálózaton: pl. 4 byte-os cím (pl.: 142.133.44.134) (IPv4 esetén 32 bites, IPv6 esetén 128 bites bináris szám)
- TCP szerepe az adatok hiba nélküli továbbítása.
- Csomagkapcsolt hálózat.

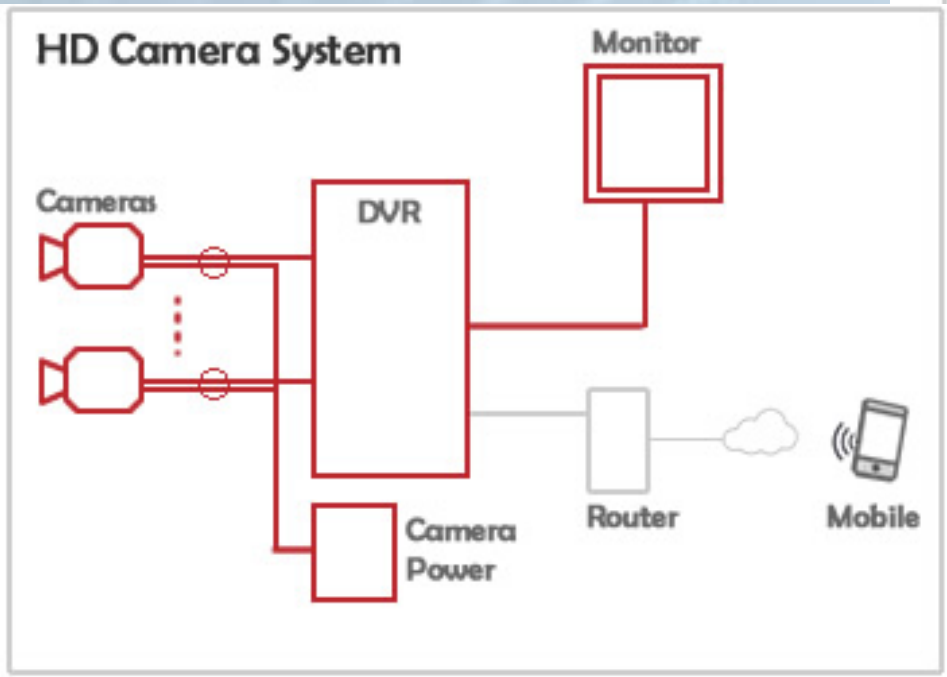
Videójelek továbbítása IP hálózaton

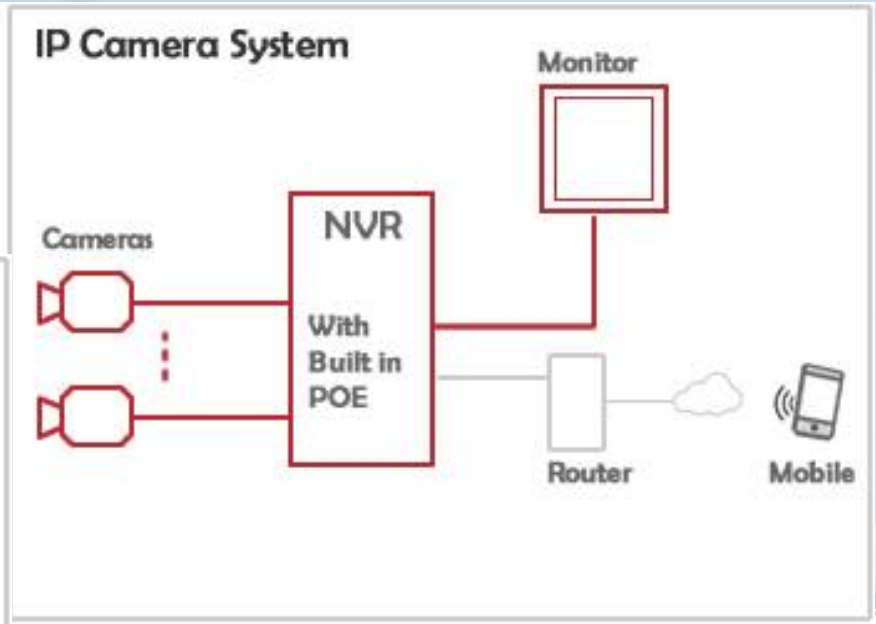
- Az analóg videojel digitalizálása valamelyik eljárással;
- a digitális információ csomagokra bontása;
- a csomagok „megcímzése”;
- a csomagok továbbítása a hálózaton keresztül;
- a vevő oldalon a csomagokból az információ újbóli összerakása;
- az információ feldolgozása, tárolása, esetleg visszaalakítása analóg jellé.

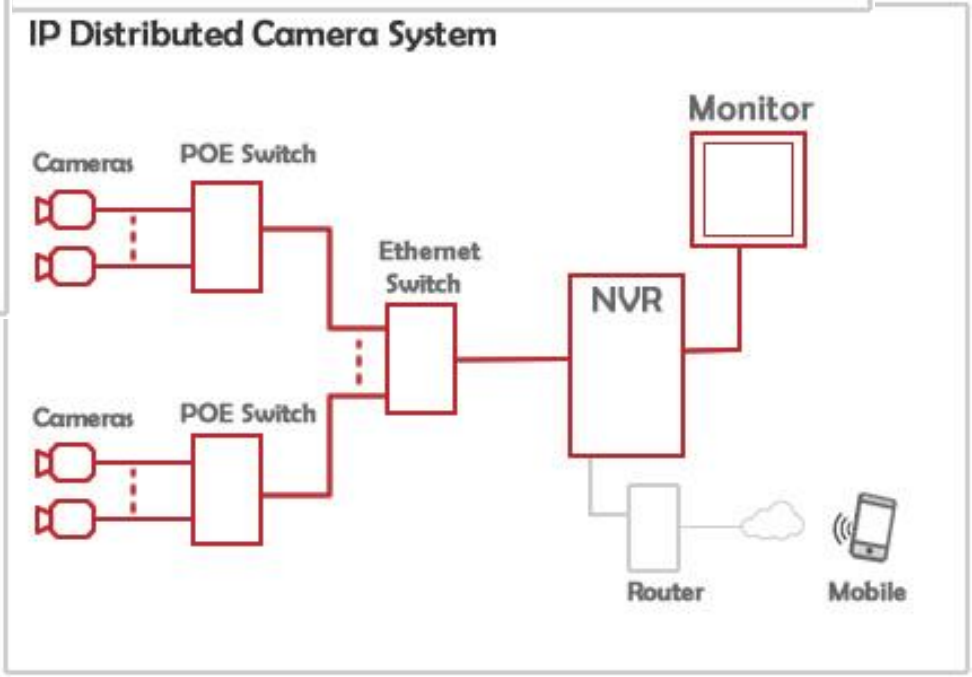
IP kamera

- A kamera és a "számítógép" egy „dobozba, készülékházba” integrálható, melynek eredménye az IP kamera.
- Az IP kamera önmaga végzi a digitalizálást, a tömörítést és a jeltovábbítást.

Analóg HD vs IP videorendszer







Analog HD vs IP video megfigyelő rendszer

Szempontok	Analóg HD	IP
felbontás	4k (8MP)	7k (30MP)
minőség	TVI, CVI és AHD valós idejű tömörítetlen analóg jel, bár a távolsággal csökken a minőség	a nagyobb felbontású, élesebb kép az IP hálózaton késleltetést szenved, mely így nem teljesen valós idejű
bekerülési kts	ma még talán olcsóbb	csökkennek az árak, hamarosan összemérhető lesz

Analog HD vs IP video megfigyelő rendszer

Szempontok	Analóg HD	IP
analitikák	Kameraoldalon ritka, rögzítőben (DVR) azonos az IP-vel, *mozgásérzékelés, intelligens követés, rendszámolvasás, tűzészlelés, szabotázs észlelés, intelligens keresés*, stb.	Kamera és rögzítőoldali (NVR), nagyon széleskörű, rendszerfüggő, hogy hol a praktikusabb, *arcfelismerés, „kóválygás, mászkálás" emberszámlálás, eltöltött idő észlelés, határvonal átlépés elleni védelem, stb.*

Analog HD vs IP video megfigyelő rendszer

Szempontok	Analóg HD	IP
vezeték nélkül?	felárral, max. 1-4 csatorna	WIFI, 8-16+ csatorna
tömörítés	H264, H264+, H265!	ua, csak nincs tömörítetlen (RAW) video
sávszélesség igény	nincs, mivel analóg videojel átvitel van valós időben, bár a felvételek máshol történő élő megjelenítése és a visszajátszás már igényel sávszélességet	alapvetően sávszélességigény van a kamerától a rögzítőig, + az élőkép megjelenítés, és a visszajátszás is igényel sávszélességet (WIFI)

Analog HD vs IP video megfigyelő rendszer

Szempontok	Analóg HD	IP
távolságok	450-500m	100m x X
tápellátás /adatátvitel	TOC /POC RG59, RG6	POE táp, video, adatátvitel
távoli megtekintés	élő és visszajátszott képekre	élő és visszajátszott képekre
távoli backup	ma már igen, csak 1 IP cím kell x db kamerához	Alapvetően megoldható egy redundáns rögzítés
telepítés	egyszerű -> közepes	egyszerű -> bonyolult (inform. ismeret szükséges) *több, mint 32 kam., különálló hálózat*

Analog HD vs IP video megfigyelő rendszer

Szempontok	Analóg HD	IP
hibakeresés	egyszerű, a rendszer miből áll: kamera, átviteli út (RG59, RG6, balun), DVR…	egyszerű->nehéz a LAN hálózati aktív eszközök plusz problémákat hordozhatnak, ezek táplálása hogyan biztosított, stb.
karbantartás, hibaelhárítás	egyszerű, cseréhez egy képfelvétel kell	egyszerű->közepes a képen túl a kamera ip beállításait is ismerni kell.

AI/VCA Intelligens videó rendszerek

This video shows a Forensic Search using the IVA 4.0 head detector capability.

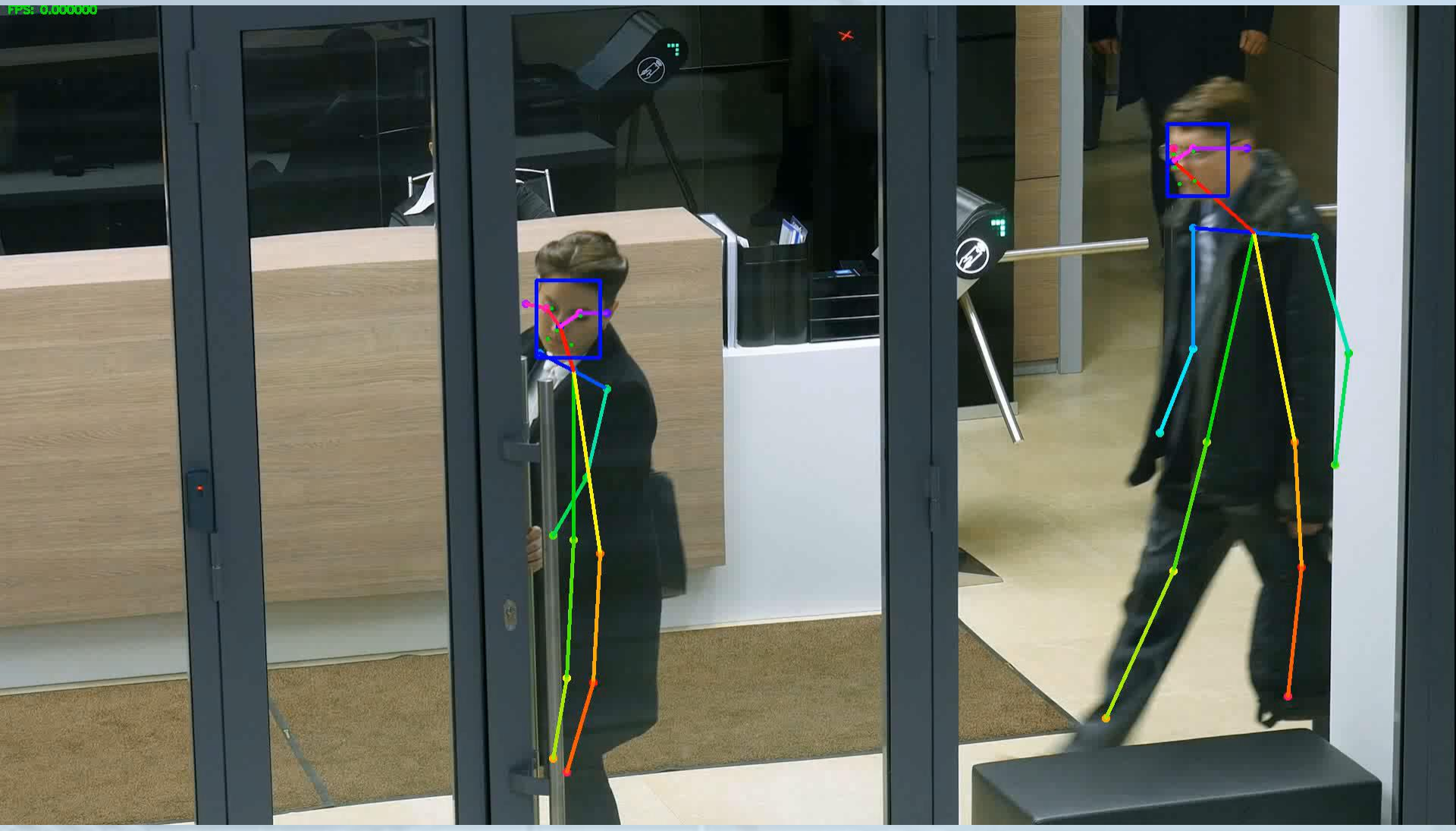
The story is that between 16:00 and 20:00 there was an "event" that a person wearing red clothes stole an object from this particular area.

During this video the suspect will found by narrowing down the search from:

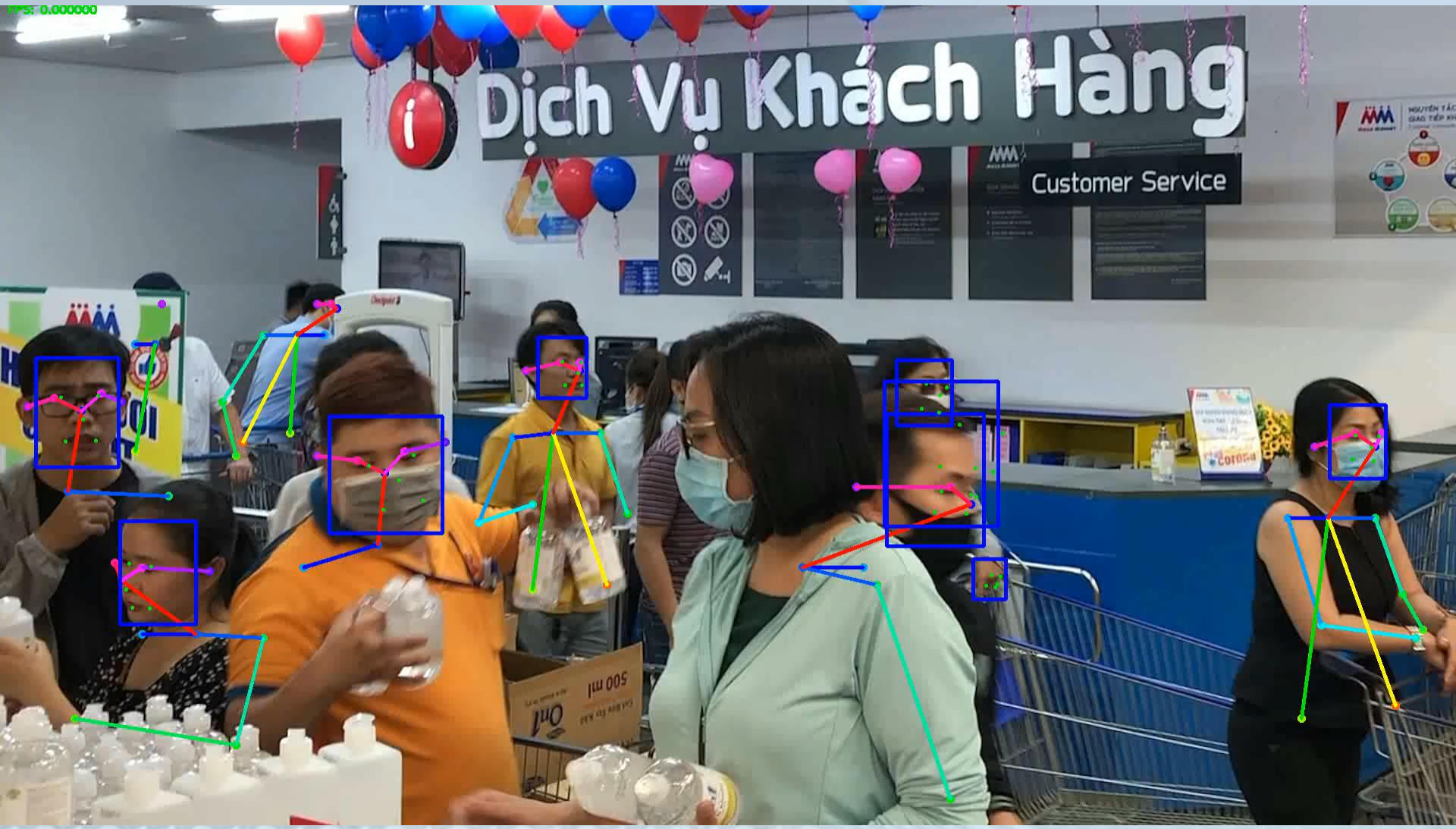
- All objects
- Objects which are human
- Objects which are human with red color

AI/VCA Intelligens videó rendszerek

AI/VCA Intelligens videó rendszerek
(Overview of AI in security)



AI/VCA Intelligens videó rendszerek (human pose estimation)



AI/VCA Intelligens videó rendszerek
(Overview of AI in security)

AI/VCA Intelligens videó rendszerek
(Overview of AI in security)

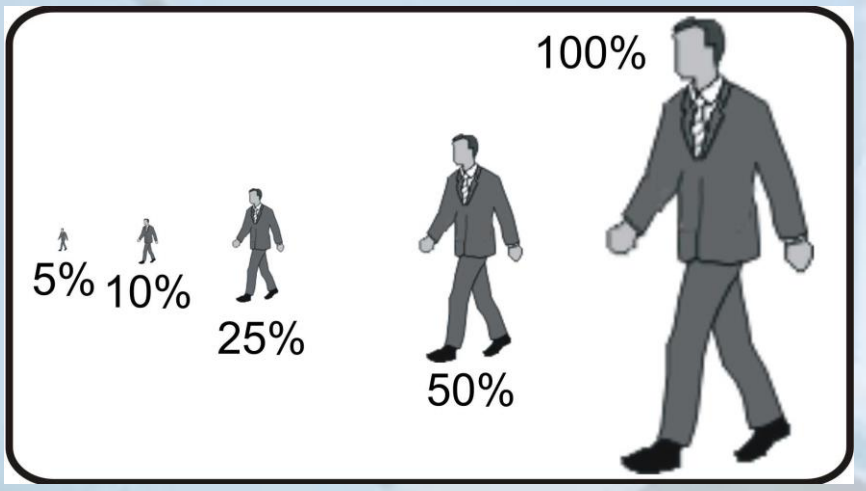
AI/VCA Intelligens videó rendszerek
(Overview of AI in security)

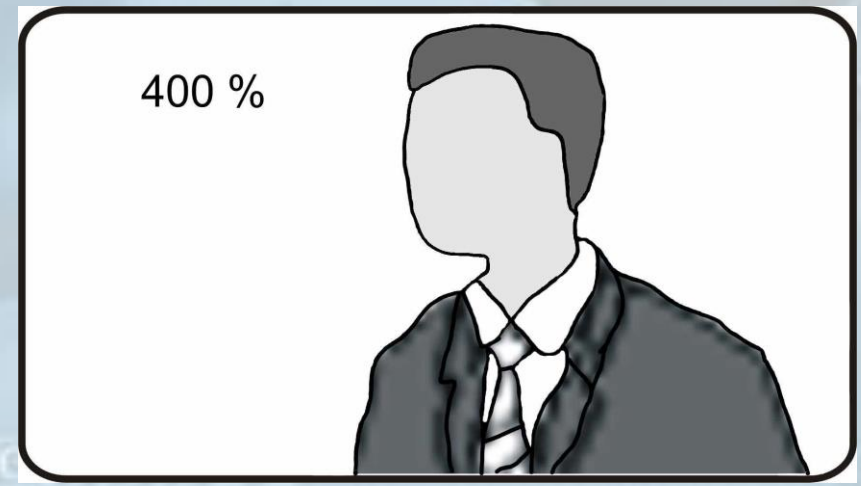
AI/VCA Intelligens videó rendszerek
(human pose estimation)

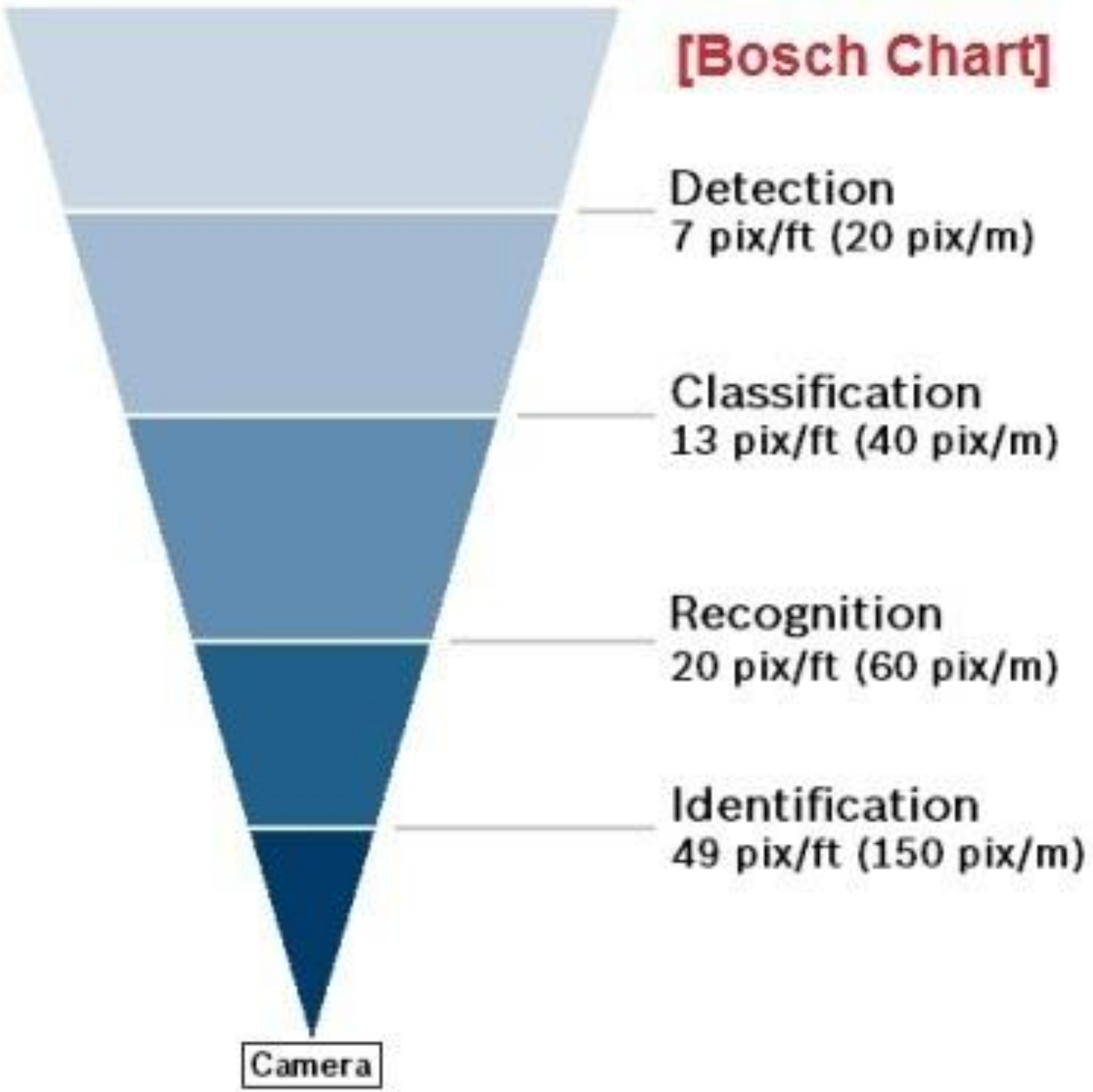
Látószög, „megfigyelési cél” helyes megválasztása

Az MSZ EN 62676-4:2015 szerinti alapvető megfigyelési célok, mint

- **monitor or crowd control** áttekintés, vagy tömegfelügyelet (képernyőmagasság 5%, vagy 80 mm/pixel);
- **detect,** észlelés (képernyőmagasság 10%, vagy 40 mm/pixel);
- **observe,** megfigyelés (képernyőmagasság 25%, vagy 16 mm/pixel);
- **recognise,** felismerés (képernyőmagasság 50%, vagy 8 mm/pixel);
- **identify,** azonosítás (képernyőmagasság 100%, vagy 4 mm/pixel);
- **inspect,** kivizsgálás (képernyőmagasság 400%, vagy 1 mm/pixel)







Note: Based on human-sized target, 1.6 ft x 5.9 ft (0.5 m x 1.8 m)

Pixel density (meters)

Detection:
4 px/face
25 px/m

Recognition:
20 px/face
125 px/m

Identification
(Good conditions):
40 px/face
250 px/m

Identification
(Challenging conditions):
80 px/face
500 px/m

Jogi keretek

2004. évi I. Törvény a sportról (2022.01.07)

71. §; 72. §; 72/A. §; 72/B. § beléptetés szabályai! (részletek!)

72. § (2a) A (2) bekezdés a) pontjától eltérően, ha a sportrendezvény biztonsági kockázatának változása miatt beléptető rendszert kell alkalmazni, de a jegyértékesítés a biztonsági kockázat változása előtt megkezdődött és az nem névre szóló jegyértékesítésként történt, ugyanezen a módon a jegyértékesítés a biztonsági kockázat változását követően folytatható.

(3) Ha a beléptetéskor a belépőjegy vagy a bérlet birtokosának személyes adatai nem egyeznek a személyazonosság igazolására alkalmas igazolványban szereplő adatokkal, a beléptetést meg kell tagadni.

72/A. § (1) Beléptető rendszer alkalmazása esetén a szervező személyazonosításra alkalmas, fényképpel ellátott, kedvezményekre jogosító kártya (a továbbiakban: klubkártya) kiváltását is kötelezővé teheti.

(2) A szervező jogosult - a klubkártya tulajdonosa személyazonosítása céljából - a klubkártya tizennegyedik életévét betöltött tulajdonosának képmásából, ujjnyomatából, íriszképéből vagy vénalenyomatából (a továbbiakban együtt: biometrikus adat) generált, vissza nem fejthető alfanumerikus kódot (a továbbiakban: biometrikus sablon) kezelni.

Jogi keretek

2004. évi I. Törvény a sportról (2022.01.07)

71. §; 72. §; 72/A. §; 72/B. § beléptetés szabályai! (részletek!)

72/A. § (4) A szervező a beléptetéskor a rendező útján

b) a (2) bekezdésben meghatározott esetben a belépőjegy vagy a bérlet birtokosának személyazonosságát úgy ellenőrizheti, hogy a belépőjegy vagy a bérlet birtokosa biometrikus adatát rögzíti, abból biometrikus sablont képez és azt összeveti a klubkártya tulajdonosa szervező által nyilvántartott biometrikus sablonjával.

(6) A beléptetést követően, valamint a beléptetés megtagadása esetén a beléptetés során rögzített személyes adatokat haladéktalanul törölni kell. Ha a beléptetés megtagadására a 71. § (1) bekezdés e) pontjában (*nem áll a 73. § (1) bekezdése szerinti kizárás, a sportrendezvények látogatásától eltiltás büntetés, a szabálysértési kitiltás, vagy a 76/A. § (1) bekezdése szerinti, külföldi sportszervezet, hatóság, bíróság hasonló tartalmú döntésének hatálya alatt*) foglaltak miatt kerül sor, a beléptetés során rögzített személyes adatokat a szervező legfeljebb 30 napig kezelheti.

Jogi keretek

2004. évi I. Törvény a sportról (2022.01.07)

72/B. § (2) A belépőjegy, bérlet, valamint klubkártya értékesítésekor a sportrendezvényre ezekkel belépésre jogosult személy

a) nevét,

b) anyja nevét,

c) születési helyét és idejét,

d) lakcímét, és

e) - a 72/A. § (2) bekezdésében meghatározott esetben - biometrikus sablonját a szervező, valamint az a)-d) pontban meghatározott adatokat a szervező által megbízott, sportesemény-szervező tevékenységet folytató szervezet a belépőjegy, a bérlet, illetve a klubkártya érvényességének lejáratát követő 3 munkanapig nyilvántartja, ezt követően törli. Az a)-c) pontban meghatározott adatokat a szervező, valamint a szervező által megbízott, sportesemény-szervező tevékenységet folytató szervezet a belépőjegyen, a bérleten, illetve a klubkártyán feltüntetheti. A klubkártyán a képmás is szerepelhet.

Jogi keretek

2004. évi I. Törvény a sportról (2022.01.07)

72/B. §

(3) A 72/A. § (2) bekezdésében meghatározott esetben a szervező, valamint a szervező által megbízott, sportesemény-szervező tevékenységet folytató szervezet a klubkártya értékesítésekor rögzíti a biometrikus adatot, amelyből haladéktalanul biometrikus sablont képez. A biometrikus sablont

a) a szervező nyilvántartásba veszi, ezt követően a biometrikus adatot haladéktalanul törli, vagy

b) a szervező által megbízott, sportesemény-szervező tevékenységet folytató szervezet haladéktalanul továbbítja a szervező részére nyilvántartásba vétel céljából, ezt követően a biometrikus sablont és a biometrikus adatot haladéktalanul törli.

(5) A (2) bekezdésben meghatározott határidőn belül a (4) bekezdés szerinti személyes adatot megkeresésre vagy adatkérésre a bíróság, az ügyészség, a nyomozó hatóság vagy a szabálysértési hatóság részére büntető- vagy szabálysértési eljárásban bizonyítási eszközként való felhasználás céljából továbbítani lehet.

Jogi keretek

2004. évi I. Törvény a sportról (2022.01.07)

74. § (1) A szervező - rendező alkalmazása esetén a rendező - és az utazó sportszervezet képviselője a sportrendezvények biztonságáról szóló kormányrendelet hatálya alá nem tartozó versenyrendszerben szervezett, valamint a normál és fokozott biztonsági kockázatú sportrendezvény ideje alatt - annak helyszínén, a beléptetésre váró szurkolók által elfoglalt közterületen és a nézők részére kijelölt parkolókban - a résztvevők személyi és vagyonbiztonsága érdekében jogosult, a labdarúgás sportág tekintetében a fokozott, valamint valamennyi kiemelt biztonsági kockázatú sportrendezvény ideje alatt köteles a résztvevőket a rendőrség által meghatározott helyszínekre, a rendőrség által meghatározott számban elhelyezett, valamint a szervező vagy - rendező alkalmazása esetén - a rendező testére rögzített, a résztvevők egyedi azonosítását lehetővé tevő minőségű felvételt biztosító kamerával megfigyelni és a felvételt rögzíteni.

(2) A kamerával való megfigyelésről, a kamerák elhelyezkedéséről és a rögzített adatok kezeléséről a nézőt a sportlétesítményen kívül és annak területén jól látható hirdetményen, a belépőjegyen, bérleten, illetve a klubkártyán piktogramok felhasználásával, valamint magyar, angol nyelven is tájékoztatni kell.

Jogi keretek

2004. évi I. Törvény a sportról (2022.01.07)

(3) A szabálysértési eljárás, valamint a büntetőeljárás megindításához és lefolytatásához szükséges adatok és információk biztosítása céljából a sportrendezvény befejezését követően a szervező, utazó sportszervezet köteles a rendőrség által a sportrendezvény befejezését követő 120 órán belül megtehető felszólításban megjelölt ideig megőrizni a sportesemény biztosítása során rögzített felvételeket. A rendőrség a szervezőt, a rendezőt, az utazó sportszervezetet a felvételeknek a felszólítást követő legfeljebb 60 napig történő tárolására szólíthatja fel. Amennyiben a felszólításra vagy az (5) bekezdés szerinti adatigénylésre nem kerül sor, a szervező, a rendező, az utazó sportszervezet a rögzített adatokat a rögzítést követő 120 óra elteltével megsemmisíti.

(4) Amennyiben a rendőrség a kamerák által rögzített valamely adatot igényli, ennek a szervező haladéktalanul köteles eleget tenni.

Jogi keretek

2004. évi I. Törvény a sportról (2022.01.07)

(5) Az (1) bekezdés szerint rögzített felvételekből a jogszabályban meghatározott nemzetbiztonsági, bűnüldözési, szabálysértési, illetve igazságszolgáltatási feladatai ellátása céljából a nemzetbiztonsági szolgálat, a rendőrség, a bíróság, az ügyészség, a nyomozó hatóság, az előkészítő eljárást folytató szerv, a szabálysértési hatóság, valamint az érintett személy igényelhet adatot. Az (1) bekezdés szerint rögzített felvétel a szervező, valamint az utazó sportszervezet által, a sportrendezvényen történő részvételből való kizárás, közigazgatási hatósági eljárás megindítása, valamint polgári jogi igény érvényesítése érdekében felhasználható az eljárás jogerős befejezéséről szóló értesítés kézhezvételét, vagy a kizárás hatályának leteltét követő harmadik munkanapig.

(6) A kamerával felvett adatokat a sportrendezvény területén erre a célra létesített helyiségben a szervező, a rendező, illetve a rendező szerv képviselője egyidejűleg és folyamatosan figyelemmel kíséri. A rendőrség, illetve a nemzetbiztonsági szolgálat e feladattal megbízott képviselője ennek során jelen lehet. Amennyiben a rendőrség, illetve a nemzetbiztonsági szolgálat igényli, a szervező, a rendező, valamint a rendező szerv képviselője a sportrendezvény ideje alatt köteles biztosítani a hozzáférést a kamerával történő megfigyeléshez.

Jogi keretek

Info törvény (2022.01.07)

GDPR rendelet (2022.01.07)

3/2019. számú iránymutatás a személyes adatok videoeszközökkel történő kezeléséről (2022.01.07)

NAIH: az Európai Adatvédelmi Testület GDPR értelmezései (2022.01.07)

UEFA

- **Az UEFA (UEFA EURO 2020 Tournament Requirements) szabályzatának 7. fejezete elvárásokat és javasolt megfigyelési helyszíneket sorol fel, mint ajánlás [ennek alapja a Guide to Safety at Sports Grounds Sixth Edition (ISBN 978-1-9164583-0-7) ("The Green Guide")]:**
- **A VSS rendszer legyen:**

a) **digitális;**
b) **színes;**
c) **legyenek PTZ (gyorsdóm) kamerák;**
d) **legyen alkalmas a képek digitális rögzítésére, visszajátszására, illetve álló- és mozgóképek exportálására.**

- **A megfigyelési célok tekintetében pedig a következő helyszíneket jelöli meg, mint megfigyelési célok:**

a) **külső és belső biztonsági zónák;**
b) **valamennyi be- kijárat, különösen a biztonsági forgókeresztek;**
c) **minden nyilvános gyülekezőhely;**
d) **minden nézőtéri ülőhely;**
e) **minden öltöző bejárat, valamint a stadion vezérlőtermének bejárata.**

- **Meghatározza azt is, hogy a stadion minden biztonsági rendszerének (a vészvilágítástól a CCTV-ig) legalább 3 órás szünetmentes tápellátásról kell üzemelnie.**

MLSZ

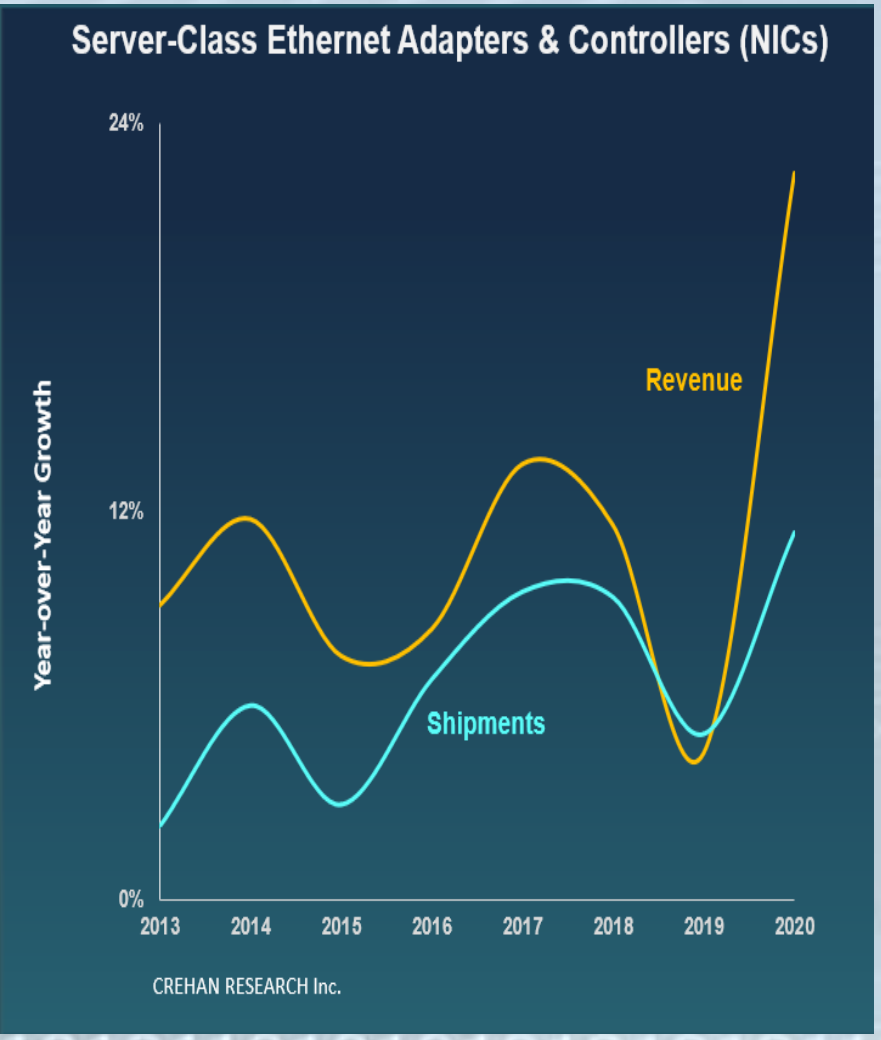
- A magyar Stv. végrehajtási utasítása alapvetően az MLSZ Biztonsági Szabályzatában (v2/2021) és a Klubkártya és Futballkártya Használati Tájékoztató (v13b 2021.09.14) található.
- A szabályzatok tartalmazzák a biztonsági rendszerek üzemeltetési rendjével, a biztonsági zónákkal kapcsolatos elvárásokat.
- Tartalmazzák a beléptetésre vonatkozó szabályokat, az ezzel kapcsolatos eljárások módját, a rendezvényről való kizárási feltételeket.
- Szabályozzák a videomegfigyelő rendszer üzemeltetési szabályait a felvételek megőrzési határidejeit, illetve a megőrzendő felvételek kezelésének rendjét.
- Tartalmazzák a 4 éves biztonságtechnikai fejlesztési tervekkel kapcsolatos elvárásokat, az eljárási rendet.
- A 4. számú melléklet még arra is mintát biztosít, hogy milyen forma gyomtatványon kérhetők ki a stadion videotechnikai megfigyelőrendszerével készült kamerafelvételei.

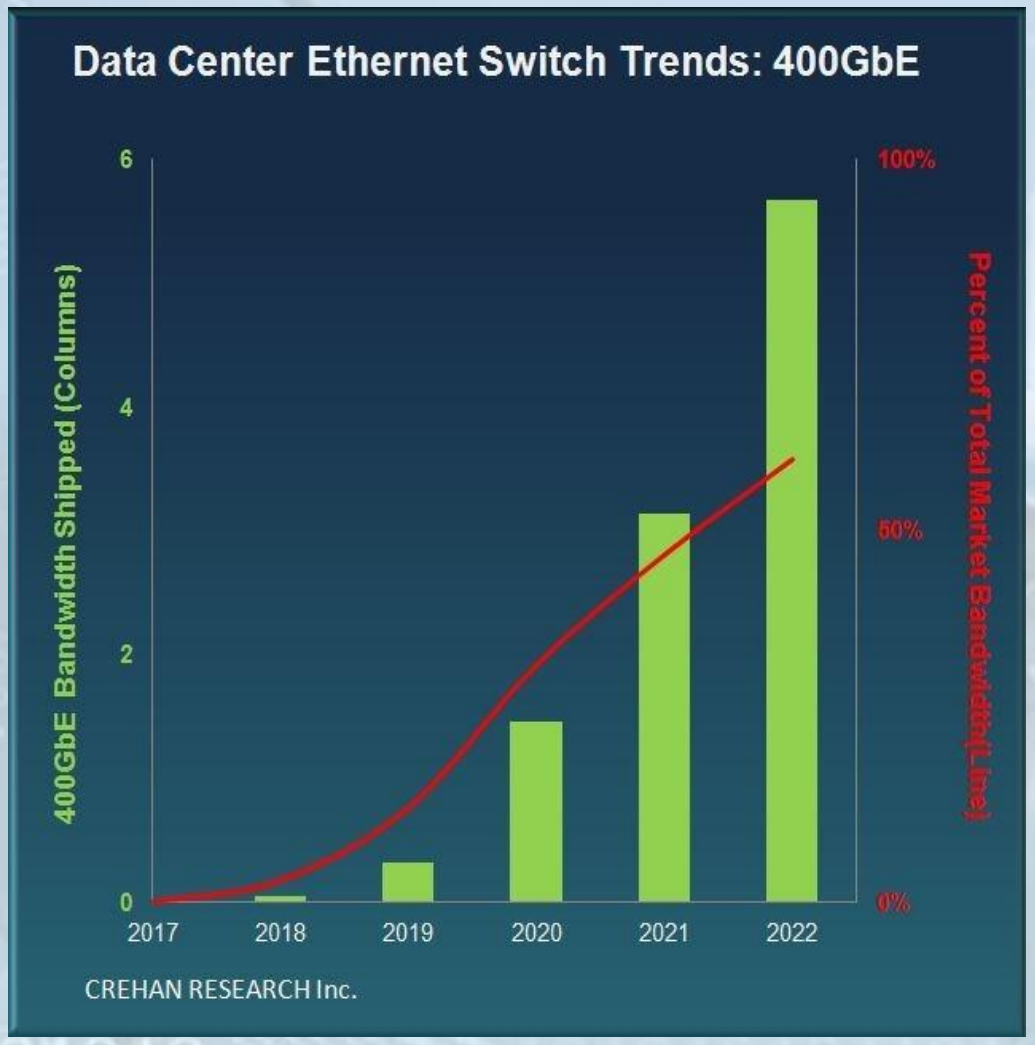
Alkalmas-e a videotechnikai megfigyelőrendszer a bűnmegelőzésre, bűnfelderítésre általánosan?

Gondolatok:

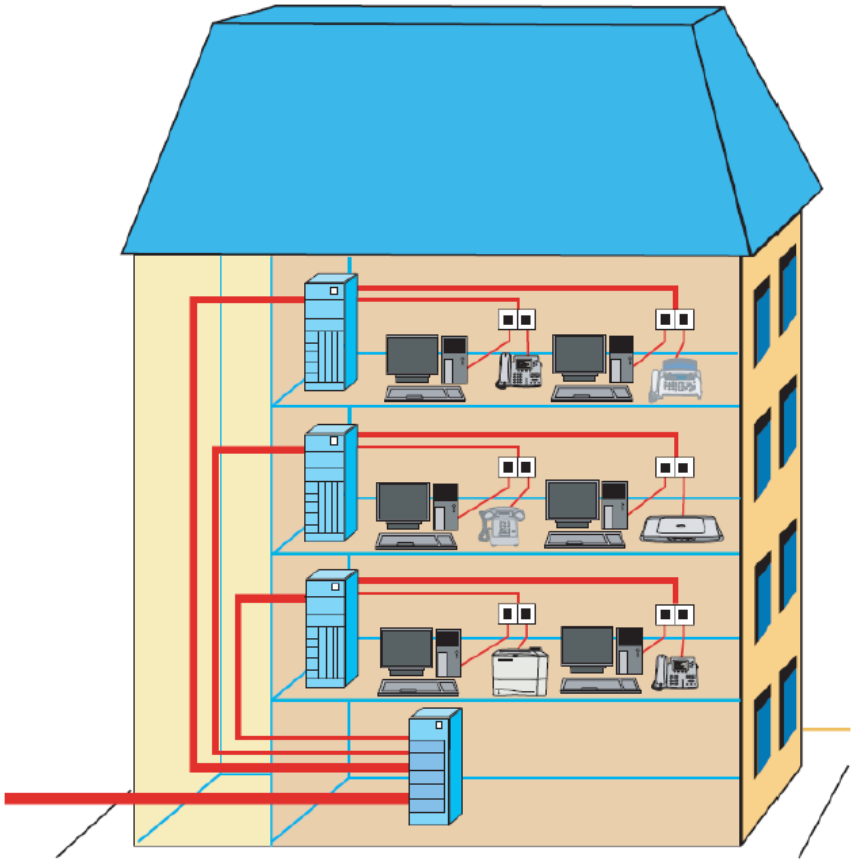
- **A VSS (CCTV) rendszerek hasznosak „lehetnek” a bűnmegelőzésben és nyomozásban (kiszorítás, alkalmazkodás);**
- **Figyelembe veendő a VSS rendelkezésre állása és tényleges hasznossága a nyomozások, bűnfelderítések során;**
- **Értékelni a szerepüket is nyilván csak meglétük, működésük időszakában lehet, nem létező rendszernek a hasznossága, hasznosíthatósága is nulla;**
- **De az is igaz lehet, hogy a nem megfelelő lefedettség, a nem optimális képkivágás, vagy az alacsony felbontás miatt nem hasznosíthatóak a felvételek;**
- **Logikailag nyilván a bűnügyileg fertőzött területen lehet „megtérülő” beruházás a megfigyelőrendszer telepítése;**
- **Az is előfordulhat, hogy azért nem vizsgálja a hatóság a felvételeket, mert más forrásból szerzett bizonyítékokkal rendelkezik, így nincs rá szüksége;**
- **Az AI/VCA sokat segíthet a jövőben a hasznosság terén, kiválthatja a leggyengébb láncszemet, az embert…(akár rögzített felvételek esetén is alkalmazható, nem fárad el, nem vonja el a figyelmét semmi, nincs magánélete…stb.)**

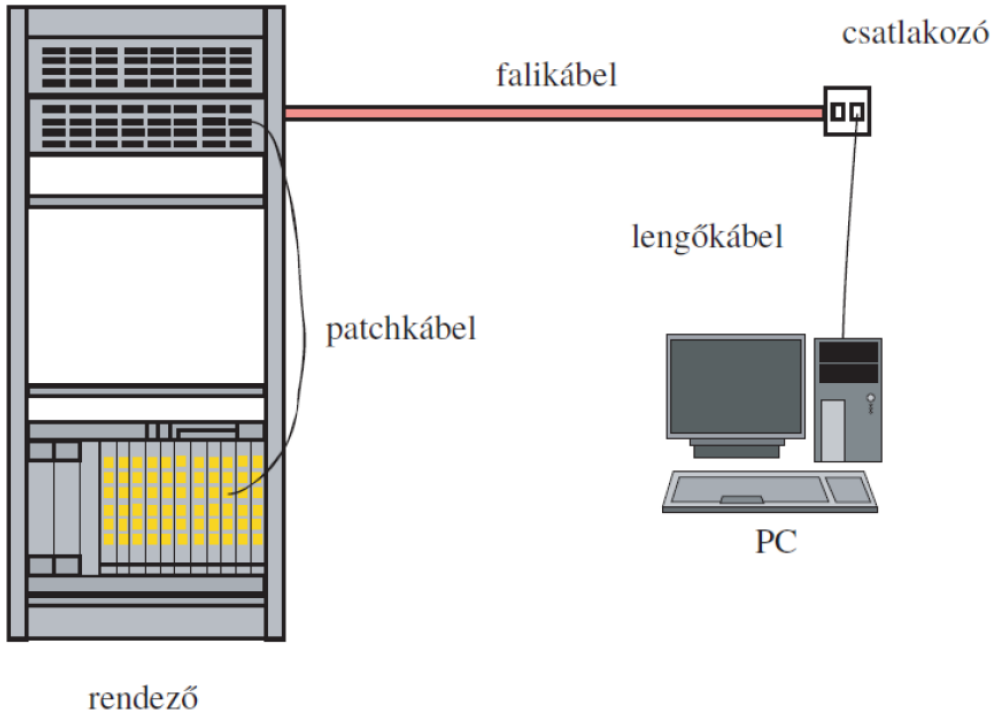
Adatszerverek sávszélességi trendje





Mi az a strukturált kábelezés?

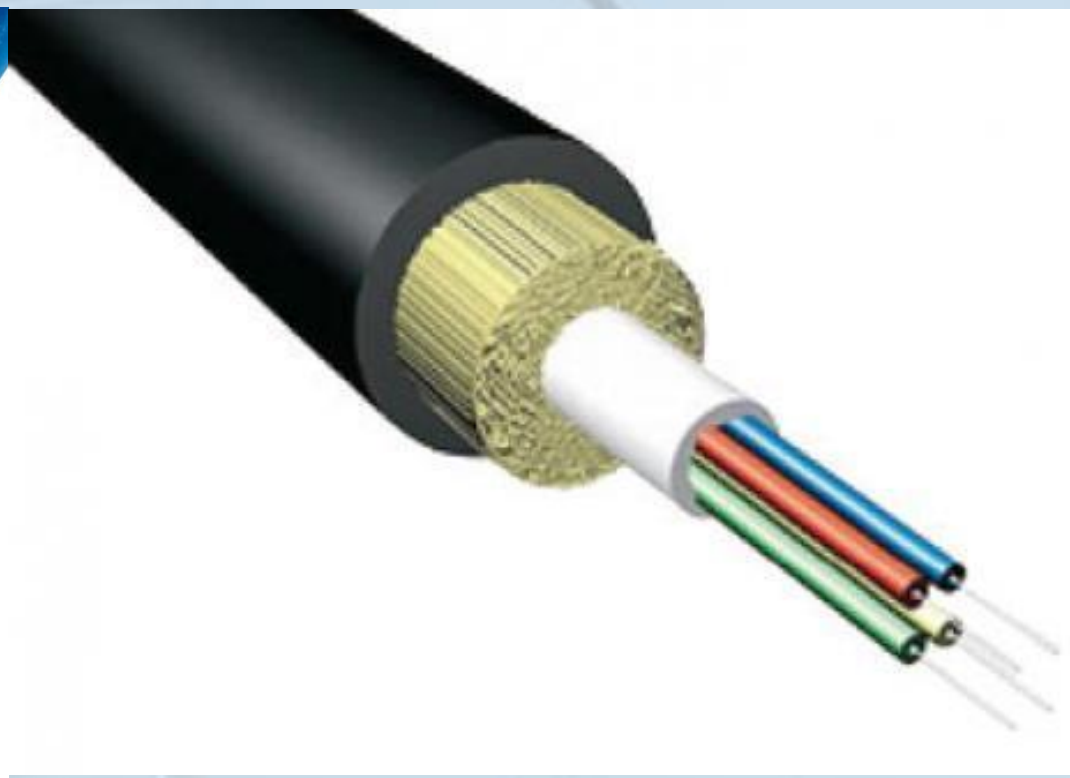




Egy kis vezetékes strukturált hálózati összefoglaló

Réz alapú

Optikai



Mit jelent a **CAT**x?

Cat xx ()	kábel ()	sebesség ()	megjegyzés ()
Cat 1	-	0.4 MHz	telefon és modem vonalak
Cat 2	-	4 MHz	régi terminál rendszerek pl.: IBM 3270
Cat 3	UTP	16 MHz	10BASE-T; 100BASE-T4; Ethernet vonalak
Cat 4	UTP	20 MHz	nem használatos
Cat 5	UTP	100 MHz	100BASE-TX; 1000BASE-T; Ethernet; általában használatos hálózatok
Cat 5e	UTP	100 MHz	100BASE-TX; 1000BASE-T; Ethernet; hasonló mint a Cat 5, de jobb minőséget biztosít

Mit jelent a **CAT**x?

Cat xx ()	kábel ()	sebesség ()	megjegyzés ()
Cat 6	UTP	250 MHz	10GBASE-T Ethernet; leggyakrabban használt kábel Finnországban
Cat 6A	U/FTP, F/UTP	500 MHz	komolyabb árnyékolás mint a Cat 6-nál, más szabvány szerint készül
Cat 7	F/FTP, S/FTP	600 MHz	10GBASE-T Ethernet. POTS/CATV/1000BASE-T
Cat 7A	F/FTP, S/FTP	1000 MHz	10GBASE-T Ethernet. POTS/CATV/1000BASE-T
Cat 8/8.1	U/FTP, F/UTP	1600-2000 MHz	40GBASE-T Ethernet. POTS/CATV/1000BASE-T (ANSI/TIA-568-C.2-1, ISO/IEC 11801 3rd Ed.)
Cat 8.2	F/FTP, S/FTP	1600-2000 MHz	40GBASE-T Ethernet. POTS/CATV/1000BASE-T (ISO/IEC 11801 3rd Ed.)

A komponensek teljesítmény-kategóriája	A kábelezés teljesítmény-osztálya	Támogatott átviteli protokollok	Felhasználási terület				Disztribúciós szolgáltatások az épületben
			irodai	ipari	lakó-épületek	adat-központok	
Cat. 5	D	Protokollok 1 (lásd Megjegyzés*)	✗	✓	✓	✗	✗
Cat. 6	E	Protokollok 2 (lásd Megjegyzés**)	✓	✓	✓	✗	✗
Cat. 6_A	E_A	Protokollok 1 (lásd Megjegyzés*) Protokollok 2 (lásd Megjegyzés**) FC 100 MByte/s Ethernet 2,5GBASE-T Ethernet 5GBASE-T	✓	✓	✓	✓	✓
Cat. 7	F	Protokollok 1 (lásd Megjegyzés*) Protokollok 2 (lásd Megjegyzés**) FC 100 MByte/s Ethernet 2,5GBASE-T Ethernet 5GBASE-T	✓	✓	✓	✓	✓

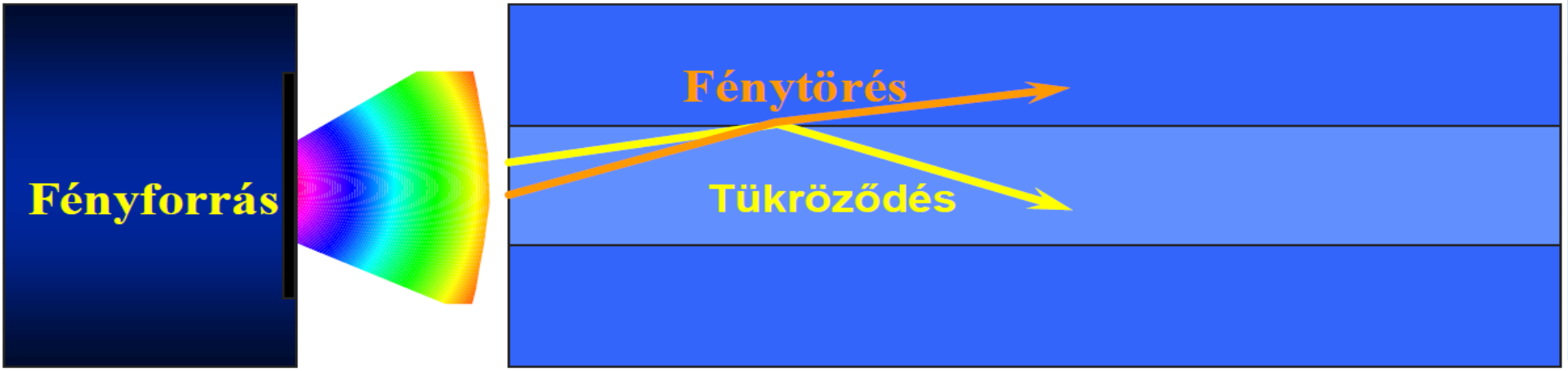
A komponensek teljesítmény-kategóriája	A kábelezés teljesítmény-osztálya	Támogatott átviteli protokollok	Felhasználási terület				Disztribúciós szolgáltatások az épületben
			irodai	ipari	lakó-épületek	adat-központok	
Cat. 7_A	F_A	Protokollok 1 (lásd Megjegyzés*) Protokollok 2 (lásd Megjegyzés**) FC 100 MByte/s Ethernet 2,5GBASE-T Ethernet 5GBASE-T	✓	✓	✓	✓	✓
Cat. 8.1	I	Protokollok 1 (lásd Megjegyzés*) Protokollok 2 (lásd Megjegyzés**) FC 100 MByte/s Ethernet 2,5GBASE-T Ethernet 5GBASE-T Ethernet 25GBASE-T Ethernet 40GBASE-T	✗	✗	✗	✓	✗
Cat. 8.2	II	Protokollok 1 (lásd Megjegyzés*) Protokollok 2 (lásd Megjegyzés**) FC 100 MByte/s Ethernet 2,5GBASE-T Ethernet 5GBASE-T Ethernet 25GBASE-T Ethernet 40GBASE-T	✗	✗	✗	✓	✗

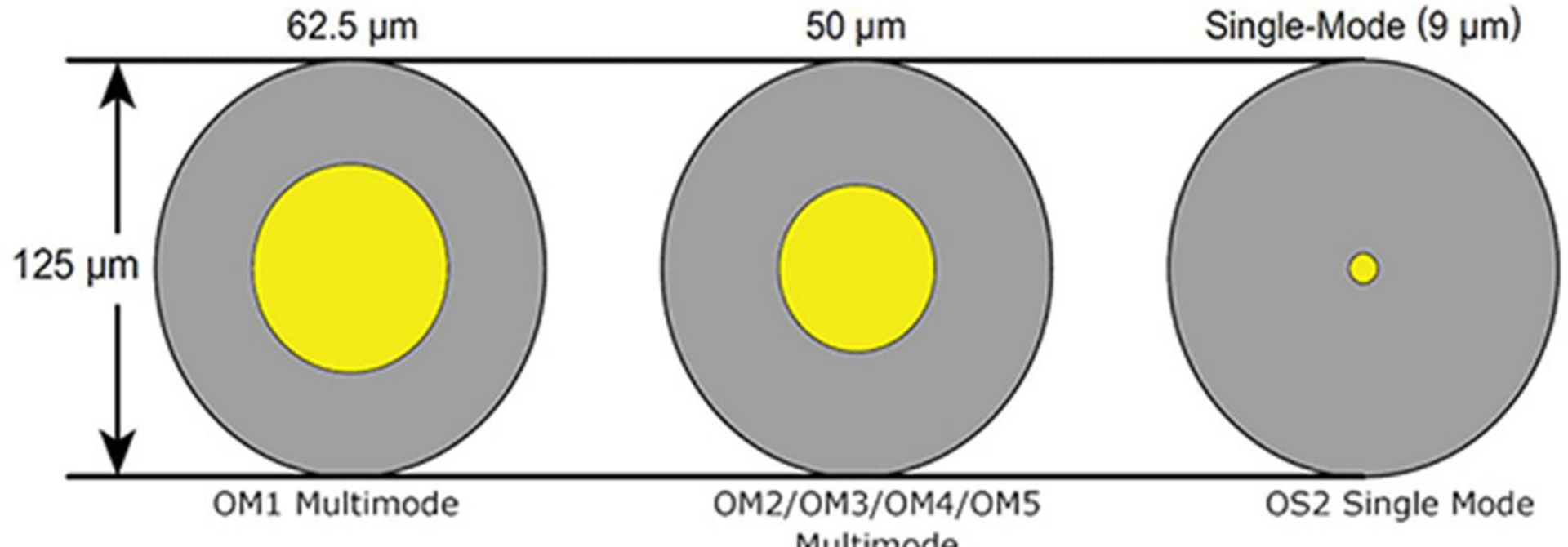
Megjegyzés*: Garantált működőképességű protokollok a Cat. 5 kategóriához: **Ethernet 10BASE-T, Ethernet 100BASE-TX, Ethernet 1000BASE-T, Fibre Channel 1 Gbit/s, Firewire 100 Mbit/s, PoE Type 1, PoE Type 2, PoE Type 3, PoE Type 4**

Megjegyzés**: Garantált működőképességű protokollok a Cat. 6_A kategóriához: **Ethernet 10GBASE-T, Fibre Channel 2 Gbit/s,**

Optikai alapú adatátvitel

Alapelv:

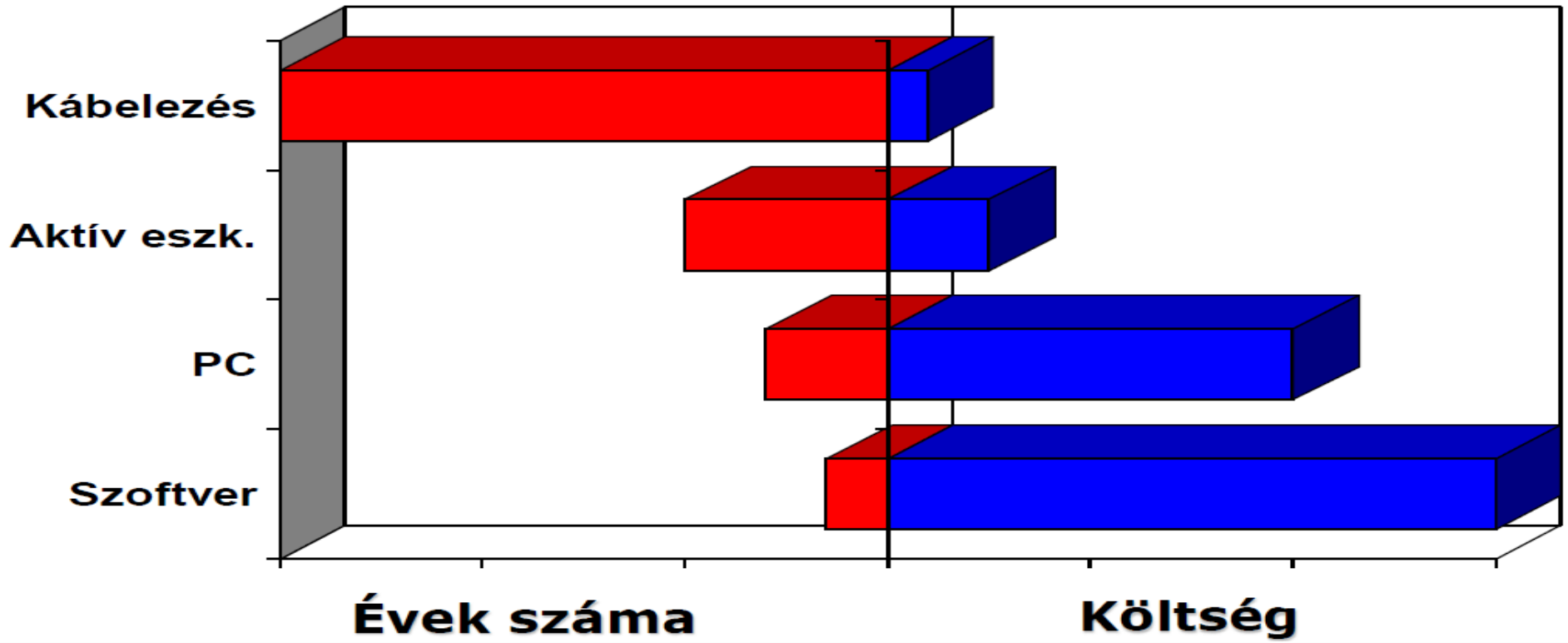




Áthidalható távolságok az IEEE optikai szabványai szerint

Table 1. IEEE Fiber Optic Standards			
Standard	**Data Rate (Mbps) +**	**Cable Type**	**IEEE Standard Max.Distance**
10Base-FL	10	Multi-mode: 850nm; 50/125µm or 62.5/125µm	2 km
100Base-FX	100	Multi-mode: 1300nm; 50/125µm or 62.5/125µm	2 km
100Base-SX*	100	Multi-mode: 850nm; 50/125µm or 62.5/125µm	300 m
100Base-LX	100	Single-mode: 1310nm, 1550nm; 9/125µm	100 km
1000Base-SX	1000	Multi-mode: 850nm; 62.5/125µm Multi-mode: 850nm; 50/125µm	220 m 550 m
1000Base-LX	1000	Multi-mode: 1300nm; 50/125µm or 62.5/125µm Single-mode: 1310nm; 9/125µm	550 m 2 km
1000Base-LH*	1000	Single-mode: 1550nm; 9/125µm	70 km

A trend



Cable Type	Description	Price*
Fiber optic cable	50ft LC to LC duplex 9/125 single mode fiber patch cable	~ $7-8
Twisted pair cable	50ft Cat6 24AWG snagless-booted UTP Ethernet network patch cable	~ $8-9
Coaxial cable	50ft RG6 digital shielded coaxial cable	~ $10-13

Itt az IoT !?

Mi az az IoT?

- Képzeljünk el egy világot, ahol nem csak az emberek, de a tárgyak is kapcsolatban állnak egymással és velünk!
- Egy világot, ahol körülöttünk minden reagál a változásokra, az autók, a közlekedési lámpák, az épületek és a közutak mind kommunikálnak egymással.
- Kontinenseken át követhetjük a vagyontárgyainkat, még a felhasználó előtt észlelhetjük a gyártási hibákat, szabályozhatjuk energiafogyasztásunkat – és még hosszan sorolhatnám, mi mindent tesz lehetővé az IoT, magyarul

"a dolgok internet(j)e".

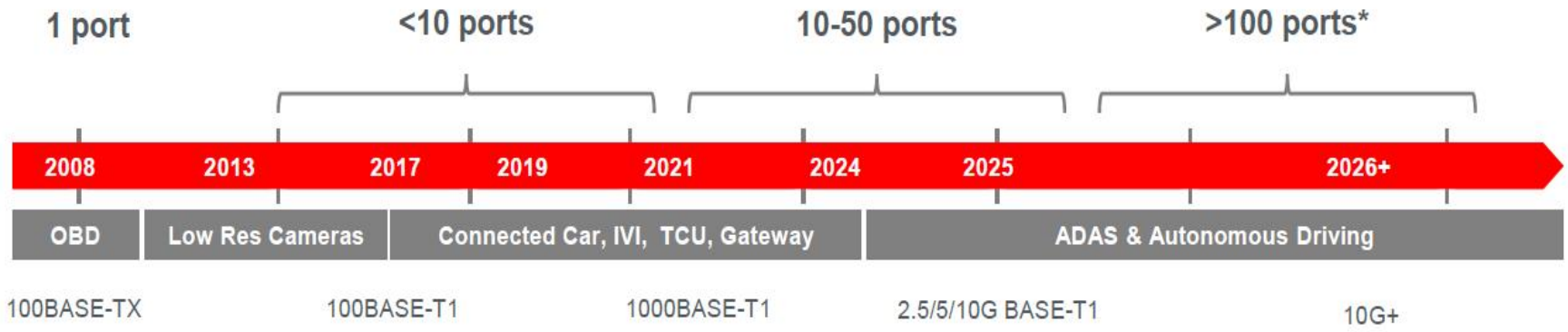
Jön az IoT !?

Mi az az IoT?

- A dolgok internet(j)e (angolul: Internet of Things, rövidítve: IoT) lényegében olyan különböző, egyértelműen azonosítható elektronikai eszközöket jelent, amelyek képesek felismerni valamilyen lényegi információt, és azt egy internet alapú hálózaton egy másik eszközzel kommunikálni.
- A dolgok internet(j)e egyik gyakorlati alkalmazása az ún. okosotthon, vagyis az egymással és a működtető személlyel hálózati kapcsolatban álló, egyes fizikai tárgyakba és eszközökbe beágyazott elektronika gyűjtőfogalma, amelyet szoftverek és érzékelők (szenzorok) tesznek lehetővé.
- A közlekedés biztonságát növelik a hálózatba kapcsolt autók (connected cars). Az ilyen kocsik állandó internetkapcsolattal rendelkeznek és valós időben kaphatnak információt a környezetükben lévő egyéb járművek mozgásáról, az általános forgalmi helyzetről, az időjárásról, stb. Ha baleset történik, akkor a beépített automatikus segélyhívó rendszer értesíti az erre kijelölt központot, amely szükség esetén segítséget küld a bajba jutott autósnak, akinek ismeri a tartózkodási helyét.

Az Ethernet (vezeték nélküli!) szabványok trendje pl. a járműiparban!

Trends in Automotive Ethernet



*Average Ethernet ports per vehicle

Biztonsági (integrált) felügyeleti rendszerek

Biztonsági (integrált) felügyeleti rendszerek

Több különböző biztonságvédelmi rendszert integráló, közös megjelenítő- és kezelőfelületen hozzáférhető komplex biztonságfelügyeletet biztosító, emberből, hardverből, szoftverből és az alkotóelemek összeköttetését biztosító hálózatból álló rendszer!

Biztonsági (integrált) felügyeleti rendszerek

A felügyelt rendszerek lehetnek:

- **tűzjelző rendszer;**
- **beléptető rendszer;**
- **behatolás- és támadásjelző (riasztó) rendszer;**
- **videomegfigyelő rendszer;**
- **áruvédelmi rendszerek;**
- **hangosítás, vészvilágítás;**
- **egyéb, gépészeti, épületfelügyeleti rendszerek;**

Lehetnek:

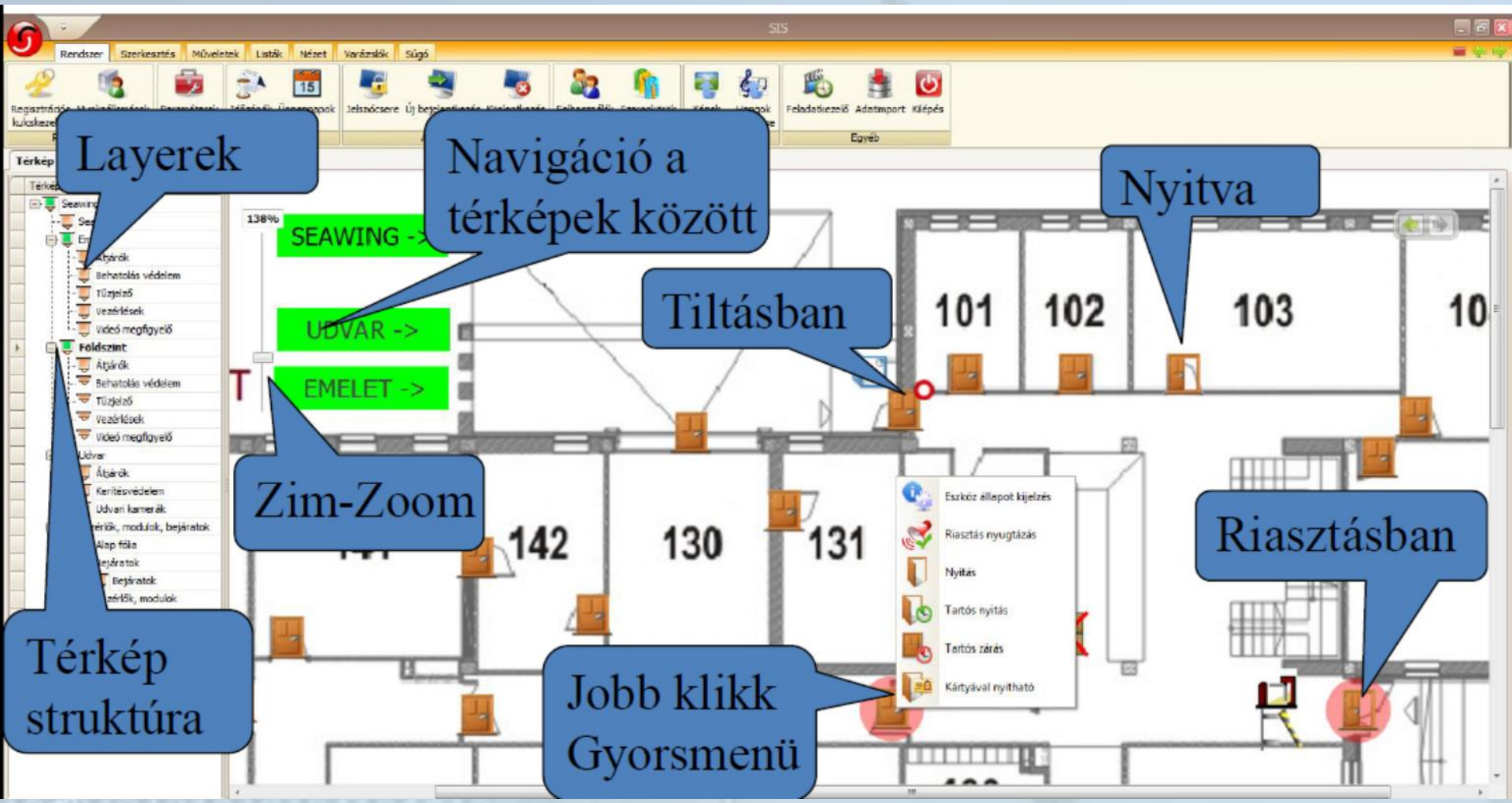
- **gyártó specifikus és**
- **open platform rendszerek**

Biztonsági (integrált) felügyeleti rendszerek

Mikor van létjogosultságuk:

- **Nagy kiterjedésű, komplex objektumok;**
- **Nagy eszközszámú rendszerek;**
- **Egymástól nagy távolságban lévő objektumhálózat;**
- **Összetett felépítésű rendszerek;**
- **Ahol fontos a beavatkozás hatékonysága;**
- **Emberi felügyelet nélküli objektumok esetén távoli felügyeletként;**
- **Távfelügyeletként.**

Biztonsági (integrált) felügyeleti rendszerek



Biztonsági (integrált) felügyeleti rendszerek

Mik az előnyök?

- Egyszerű kezelhetőség;
- Komplex információkat szolgáltat;
- Kényszerkapcsolatok létrehozása;
- Felhasználói korlát nélküli működés;
- Nagy földrajzi távolságok esetén komplex felügyelet, statisztika készítés;
- Megfelelő rezsim utasítás foganatosítása;

Biztonsági (integrált) felügyeleti rendszerek

Mik az előnyök?

- Több helyszíni diszpécserszolgálat (kliens);
- Egyedi jogosultsági szintek;
- Korlátlan eseménynapló;
- Időszinkron!
- Hibák, események kezelése, jelentése
- Globális kártyakezelés

Biztonsági (integrált) felügyeleti rendszerek

Az üzemeltetés feltételei:

- **Integrálható biztonsági rendszerek;**
- **Megfelelő IT hálózat és redundancia;**
- **Pontos és dokumentált telepítés;**
- **Folyamatos karbantartás, frissítés;**

A biztonságos működtetés feltételei:

- **Kizárólag HTTPS kommunikáció;**
- **„Driver Sandboxing” – környezet megteremtése;**
- **Aláírt kódok;**
- **Auditáció;**
- **Biometria támogatás;**

Biztonsági (integrált) felügyeleti rendszerek (csak példák!)

- BVMS 10.1
- C4
- IdentiControl
- IFR
- IFTER EQU
- inVIEW
- Kantech Entrapass™ SE
- PACOM Graphical Management System
- Seawing Integrated Solution (SIS)
- Siwenoid
- Supervising Business Integration (SBI)
- Stanley (ISS)
- TMS Pro

Köszönöm megtisztelő figyelmüket!

Móré Attila okl. biztonságtechnikai mérnök,
biztonságtechnikai szakértő
MMK: 01-8793, 01-59870
SZVMSZK: 2-002
igazságügyi szakértői jelölt
more.attila.777@gmail.com
+36 30 222 9225