MAGYAR BIZTOSÍTÓK SZÖVETSÉGE

BIZTONSÁGTECHNIKAI ÚTMUTATÓ A BETÖRÉSES LOPÁS-RABLÁSBIZTOSÍTÁSI KOCKÁZATOK KEZELÉSÉRE

(AJÁNLÁS)

B.1. Fejezet

Behatolás- és támadásjelző rendszerek

Rendszerkövetelmények

kiadás	A dokumentum megnevezése	kiadva	visszavonva
0	Behatolás- és támadásjelző rendszerek - Rendszerkövetelmények	2007.01.19	2007.09.30.
1	Behatolás- és támadásjelző rendszerek - Rendszerkövetelmények	2007.10.01	

Tartalomjegyzék:

Bevezetés

Ez a **MABISZ ajánlás** az épületekben telepített behatolás- és támadásjelző rendszerekre határoz meg megfelelőségi követelményeket.

A behatolás- és támadásjelző rendszerek célja a felügyelt helyiségek biztonságának növelése. Hatásosságának fokozására a behatolás- és támadásjelző rendszereket megfelelő mechanikai-fizikai védelmi eszközökkel és eljárásokkal együtt kell alkalmazni. Ez különösen fontos a magasabb biztonsági osztályú behatolás- és támadásjelző rendszerek esetén.

Ezen ajánlás rendeltetése, hogy segítse a biztosítók, a behatolásjelző eszközöket gyártó vállalatok, a felhasználók és a rendőrség munkáját az adott helyiségekben kívánt védelem teljes és pontos meghatározása érdekében, de nem határozza meg a technológia típusát, az érzékelés mértékét vagy fokozatát, és nem fedi le az egyedi telepítés összes követelményét sem.

A behatolás- és támadásjelző rendszerek tervezőinek számításba kell venniük a helyiségek jellemzőit, az ott tárolt értékeket, a behatolás kockázatának fokát és bármely más tényezőt, ami befolyásolhatja a behatolásjelző rendszer hatékonyságának és felépítésének megválasztását.

A behatolásjelző rendszerek részegységeinek vizsgálatára vonatkozó előírások a vonatkozó **MABISZ részegység-ajánlásokban** találhatók.

Az behatolás- és támadásjelző rendszereket és részegységeiket **biztonsági fokozatokba** soroljuk a kívánt biztonsági szint szerint. A biztonsági fokozatok figyelembe veszik a kockázati szintet, ami a helyiségek típusától, a bennük tárolt értékektől és a várható tipikus behatolótól képzettségétől, felszerszámozottságától függ.

Ez az ajánlás olyan behatolás- és támadásjelző rendszerekre állapít meg követelményeket, amelyeket épületekben telepítenek, és vezetékes vagy vezeték nélküli összeköttetést használnak.

Ez az ajánlás nem tartalmaz követelményeket kültéri behatolás- és támadásjelző rendszerekre.

Az itt leírt követelményeket az épületben telepített behatolás- és támadásjelző rendszerek olyan részegységeire is alkalmazni kell, amelyeket rendeltetésszerűen az épület külső szerkezetére szerelnek (pl. kültéri hangfény-jelző, kezelő-kijelző egység)

Ez az ajánlás a behatolás- és támadásjelző rendszerek tervezésének és telepítésének menetet követik.

A ***J függelék*** folyamatábra formájában írja le az ebben az ajánlásban leírt főbb eljárásokat és dokumentációkat.

Azoknak, akik a behatolás- és támadásjelző rendszerek tervezéséért, telepítéséért, üzemeltetéséért és karbantartásáért felelősek, ismerniük kell a többi **MABISZ ajánlást** is a behatolás- és támadásjelző rendszerekkel kapcsolatban – különösen azokat, melyek a rendszer teljesítményéért, a behatolás- és támadásjelző központok, kezelők, érzékelők, figyelmeztető eszközök, tápegységek és az átjelzők minőségével kapcsolatosak.

1./ Alkalmazási terület

Ez az **ajánlás** segítséget ad a behatolás- és támadásjelző rendszerekkel szemben támasztott követelmények meghatározására a behatolás- és támadásjelző rendszerek megfelelő tervezésének biztosítása érdekében – mind a megkívánt felülvizsgálati előírásoknak való megfelelésnek, mind a rendszer megfelelő biztonsági fokozatának megállapításának érdekében, melyek a felügyelet szintjének megállapításához szükségesek. (A behatolás- és támadásjelző rendszerek követelményeit az **MSZ EN 50131-1** szabvány tartalmazza.)

Ez az **ajánlás**: segítséget nyújt azon behatolás- és támadásjelző rendszerek kiválasztásáért felelős személyeknek, és lehetővé teszi ezen behatolás- és támadásjelző rendszerekkel szemben elvárt teljesítményszint biztosítását és biztosítja, hogy megfelelnek a behatolás- és támadásjelző rendszerek működéséi környezeti teltételeinek.

2./ Hivatkozások

Ez az **ajánlás** évszámmal ellátott vagy évszám nélküli hivatkozással előírásokat tartalmaz más kiadványokból.

Ezeket a hivatkozásokat a szöveg megfelelő helyen idézi, a kiadványokat a következő felsorolás tartalmazza.

Évszámmal ellátott hivatkozások esetén ezen kiadványok bármelyikének módosítása vagy átdolgozott kiadása csak akkor vonatkozik erre az ajánlásra, ha ennek módosítása vagy átdolgozott kiadása azt már tartalmazza.

Évszám nélküli hivatkozások esetén a hivatkozott kiadvány legutolsó kiadását kell alkalmazni.

A hatályos szabványok jegyzéke az ***A.1. függelékben*** található.

Az egyes létesítmények, tevékenységek kockázati osztályokba sorolása az ***A.2. függelékben*** található.

3. Szakkifejezések és rövidítések

3.1. Szakkifejezések

Az **ajánlásban** használt szakkifejezetések az **A.3. függelékben** találhatóak

3.2. Rövidítések:

Ez az **ajánlás** a következő rövidítéseket használja:

ARC	Alarm Receiving Centre	**riasztásfelügyeleti központ**
ACE	Ancillary Control Equipment	**kiegészítő vezérlőberendezés**
ATE	Alarm Transmission Equipment	**riasztásátviteli berendezés**
ATS	Alarm Transmission System	**riasztásátviteli rendszer**
CIE	Control and Indicating Equipment	**vezérlő- és kijelző-berendezés**
IAS	Intruder Alarm System(s)	**behatolásjelző rendszer**
I&HAS	Intruder & Hold up Alarm Sytem(s)	**Behatolás- és támadásjelző rendszer**
PS	Power Supply	**tápegység**
WD	Warning Device	**figyelmeztető eszköz**
PIR	Passive Infra-Red	**passzív infravörös**

4. A behatolás- és támadásjelző rendszer **biztonsági fokozatba és védelmi osztályba sorolása**

A biztonsági fokozatba és a védelmi osztályba sorolás az **ajánlás *A fejezetében*** található.

5. Környezeti megfelelőség

A rendszerek környezeti osztályát azon környezeti körülmények határozzák meg, melyek között működik.

A behatolás- és támadásjelző rendszer az ***MSZ EN 50131-1 szabvány*** környezeti megfelelőségi követelményeinek feleljen meg

6. Funkcionális követelmények

A behatolás- és támadásjelző rendszer telepítése, működése és karbantartása a gyártó előírásinak megfelelően történjen és alkalmazkodnia kell a behatolás- és támadásjelző rendszer működésének várható környezeti feltételihez (lásd ***12. fejezet***).

6.1. Általános követelmények

6.1.1, Jelzésfeldolgozás:

A behatolás- és támadásjelző rendszer tartalmazzon eszközöket behatolók és szabotázs érzékelésére és a jelen ajánlás követelményeinek teljesítéséhez szükséges hibák felismerésére.

Más események is érzékelhetők, ha ez nem befolyásolja hátrányosan a behatolók és a szabotázs kötelező érzékelését és a hibák felismerését.

Ha egy érzékelő és a behatolás- és támadásjelző rendszer központja közötti összeköttetés megszakad, a behatolás- és támadásjelző rendszer központjának a behatolás és szabotázs jelzésének között különbséget kell tudni tenni.

1. MEGJEGYZÉS: Fentiek olyan esetekre vonatkozhatnak, amikor az összeköttetés közvetlenül egy mechanikus vagy mágneses kapcsolón (érintkezőn), vagy egy érzékelő jelfogóján, vagy egy szabotázsérzékelő kapcsolón (érintkezőn) keresztül van kialakítva.

Amikor egy összeköttetést behatolás- vagy szabotázsjelzés kiváltása céljából alakítanak ki, az eredményül kapott jelzésnek vagy behatolás-, vagy pedig szabotázsjelzésnek kell lennie

2. MEGJEGYZÉS: A fenti esetben a vezérlő- és kijelző-berendezés ténylegesen az érzékelő részét képezi, minthogy a vezérlő- és kijelző-berendezés közvetlenül figyeli meg az összeköttetésnek az érzékelőként működő részét.

PÉLDA: fémfólia üvegen, közvetlenül hozzáerősített huzalozás, cső és huzalkeretek.

6.1.2. Behatolás-érzékelés

A behatolás- és támadásjelző rendszer csak olyan érzékelőket tartalmazzon, amelyek megfelelnek a környezeti feltételeknek és az alkalmazásoknak. Az érzékelőkben egynél több technológia is alkalmazható.
1. PÉLDA: Passzív infravörös és mikrohullámú vagy ultrahangos technológia.

Behatolásjelzést vagy üzenetet akkor kell létrehozni, amikor egy érzékelő a megkívánt időtartamon át aktív állapotban van.

Az egyes érzékelők logikailag csoportosíthatók (év/vagy kapcsolat), hogy egy vagy több behatolásjelzési feltétel létre jöjjön.

Egyedi érzékelő úgy is kiépíthető, hogy egynél több aktiválásra legyen szükség ahhoz, hogy behatolásjelző jelzést vagy üzenetet hozzon létre.

Jelen ajánláshoz az érzékelők a következőképpen sorolhatók osztályba:

(a) típus: Egyszerű állapotváltoztatós eszközök.
2. PÉLDA: Mechanikusan vagy mágnesesen működtetett kapcsolók.

(b) típus: Aktív részegységeket tartalmazó eszközök.
3. PÉLDA: mozgás- vagy rezgésérzékelők.

A behatolás- és támadásjelző rendszer tartalmazzon olyan eszközt a felhasználó számára, amely egy érzékelő működőképességének vizsgálatára szolgál.
4. PÉLDA: hallható vagy látható jelzés az érzékelő működésekor.

Egyedi azonosításról kell gondoskodni minden **(b)** típusú érzékelőnél; melynek csak akkor kell rendelkezésre állnia, ha azt a felhasználó kívánja.
***5. PÉLDA*:** Az érzékelőn lévő LED kijelző.

Ha a behatolás-érzékelők a tartomány vagy az érzékenység beállítására szolgáló eszközzel rendelkeznek, egyik biztonsági fokozatban se legyen lehetséges a tartományt vagy az érzékenységet a maximális tartomány vagy érzékenység 25 %-a alá csökkenteni.

A **3. és 4. biztonsági fokozatban** a mozgás érzékelésére tervezett behatolásjelző érzékelőknek tartalmazniuk kell olyan eszközt, amely a megadott tartomány jelentős csökkenésének érzékelésére szolgál.

Egy érzékelő látóterének beállító eszközeihez való hozzáférés ne legyen lehetséges jogosulatlan személyek számára. Másik lehetőség, hogy rendelkezzék a jogosulatlan beállítás érzékelésére szolgáló eszközzel. Ha látótér beállítás lehetséges, akkor gondoskodni kell annak véletlenszerű működtetési kockázatának minimalizálásáról. A jogosulatlan beállítást szabotázsként kell kezelni.

6.1.3. Hibák felismerése

A behatolás- és támadásjelző rendszer biztonsági fokozatától függően a jelen ajánlás követelményeinek teljesítéséhez szükséges hibafeltételek felismeréséhez gondoskodni kell megfelelő eszköz/eszközök kiépítéséről. Eszközről kell gondoskodni az alábbi hibák jelzésére:

- általános hiba;
- elsődleges tápellátás hibája;
- másodlagos tápellátás hibája;
- riasztásátviteli rendszer hibája (ahol értelmezhető).

Egyéb hibák is felismerhetők és kijelezhetők, ha ezek nem befolyásolják hátrányosan a kötelező hiba-felismeréseket.

PÉLDA: hiba egy érzékelőben.

6.1.4. Kompatibilitás

A behatolás- és támadásjelző rendszerben lévő részegységeknek egymással összeférhetőknek és együttműködésre képeseknek kell lenniük, és meg kell felelniük a rájuk vonatkozó környezeti besorolásnak.

6.1.5. Működés

A behatolás- és támadásjelző rendszert úgy kell tervezni, hogy a helytelen működésből eredő hibák minimalizálása mellett tegyék lehetővé a felhasználónak a megfelelő jogosultsági szint elérését a behatolás- és támadásjelző rendszer helyes működtetése céljából. Részleges élesítés vagy hatástalanítás megengedett.

6.1.6. Jogosultsági szintek

A behatolás- és támadásjelző rendszer mindegyik biztonsági fokozata esetén négy jogosultsági szintnek kell rendelkezésre állni a behatolás- és támadásjelző rendszer funkcióihoz való hozzáférés érekében. A ***B.1. 01. sz. táblázat*** határozza meg, milyen funkcióknak kell hozzáférhetőknek lenniük az egyes jogosultsági szinteken.

A négy jogosultsági szint a következő:

1. szint: Hozzáférés bárki által.

Az 1. szinten hozzáférhetőnek megkövetelt kezelőszerveknek nem lehet hozzáférés korlátozása.

2. szint: Hozzáférés bármely felhasználó által.

A működési állapotra hatással lévő kezelőszervek (a behatolásjelző rendszer konfigurálásának megváltoztatása nélkül).
PÉLDA: helyszínre jellemző adatok.

A 2. szinten hozzáférhetőnek megkövetelt kezelőszervekhez, vagy a 2. szinten láthatónak megkövetelt kijelzőkhöz való jogosultság korlátozása kulccsal, vagy kóddal működtetett kapcsoló, vagy zár, vagy más egyenértékű eszköz segítségével történik. A 2. szintű kulcsok vagy kódok nem biztosíthatnak hozzáférést a 3. vagy a 4. szinthez.

3. szint: Hozzáférés a szerviz-személyzet által.

Hozzáférés valamennyi, a behatolásjelző rendszer konfigurálására hatással lévő kezelőszervhez (az eszközök gyári felépítésének megváltoztatása nélkül).

A 3. szinten hozzáférhetőnek megkövetelt kezelőszervek vagy a 3. szinten láthatónak megkövetelt kijelzőkhöz való jogosultság korlátozása kulccsal, vagy kóddal működtetett kapcsoló, vagy zár, vagy más egyenértékű eszköz segítségével történik. A 3. szintű kulcsok, vagy kódok nem biztosítanak hozzáférést a 4. szinten.

4. szint: Hozzáférés a gyártó / telepítő / karbantartó által.

Hozzáférés részegységekhez az eszköz megváltoztatása céljából.

A 4. szinten hozzáférhetőnek megkövetelt kezelőszervek vagy a 4. szinten láthatónak megkövetelt kijelzőkhöz való jogosultság korlátozása kulccsal, vagy kóddal működtetett kapcsoló, vagy zár, vagy más egyenértékű eszköz segítségével történik.

A 3. vagy a 4. szinten való hozzáférést mindaddig meg kell gátolni, amíg a hozzáférést a felhasználó a 2. szintű hozzáféréssel meg nem engedi.

A 2., 3. és 4. szinten való hozzáférés távolról is elérhető, ha a megfelelő jogosultsági szintek távolról is elérhetők. Az egyes szinteken elérhető funkciók az ***1. fejezetben*** találhatóak.

6.1.7. Jogosultság

A behatolásjelző rendszer funkciói elérésének engedélyezését korlátozni kell jogosultsági kódokkal vagy ezekkel egyenértékű eszközökkel.

MEGJEGYZÉS: A behatolásjelző rendszer tulajdonosának korlátlan jogosultsága van a behatolásjelző rendszer felett. A jogosultság átruházható másokra.

6.1.8. Élesítés és hatástalanítás

A behatolás- és támadásjelző rendszernek olyan eszközzel kell rendelkezni, amellyel a felhasználó(ka)t az élesítéshez és a hatástalanításhoz való hozzáférését megfelelő jogosultsági szinttel korlátozni lehet.

Eszközről kell gondoskodni ahhoz, hogy egy felhasználó a megfelelő jogosultsági szinten képes legyen a behatolásjelző rendszert élesíteni és hatástalanítani, mégpedig úgy, hogy a helytelen működtetés lehetősége a legkisebb legyen.

6.1.9. Élesítés

Valamennyi biztonsági fokozatban a behatolás- és támadásjelző rendszernek, vagy egy részének az élesítése jogosított művelettel elérhetőnek kell lennie, feltéve, hogy a behatolás- és támadásjelző rendszer összes funkciója nyugalmi állapotban van.

A behatolás- és támadásjelző rendszer biztonsági fokozatától függően - amikor az élesítést kielégítő módon végrehajtották - egy jelzést kell létrehozni, amely azt mutatja, hogy a behatolás- és támadásjelző rendszert, vagy egy részét élesítették. E jelzést időben legfeljebb 180 másodpercre kell korlátozni.

A behatolás- és támadásjelző rendszer nem lehet élesíthető, amíg az érzékelők nem kerülnek nyugalmi állapotba.

Ha a behatolás- és támadásjelző rendszer olyan érzékelőket tartalmaz, amelyek képesek arra, hogy a megadott érzékelési tartomány jelentős lecsökkenését észleljék, az ilyen tartománycsökkenésnek meg kell akadályoznia az élesítést, hacsak ezt nem bírálják felül.

6.1.9.1. Élesített állapot

Ha a behatolás- és támadásjelző rendszer élesített, a bejárati, és/vagy kijárati útvonalon keresztül a felügyelt területhez a hozzáférést meg kell akadályoznia, vagy pedig jelzést kell adnia.

6.1.10. Hatástalanítás

Valamennyi biztonsági fokozatban a behatolás- és támadásjelző rendszernek, vagy egy részének a hatástalanítása csak jogosított művelettel legyen elvégezhető.

Ha a felügyelt területhez hozzáférés szükséges, a behatolás- és támadásjelző rendszer hatástalanításához egy útvonalat kell meghatározni a belépési ponttól a hatástalanításhoz szükséges eszközig. Ha a helyes belépési eljárást kezdeményezték, a rendszer csak a meghatározott útvonalon lévő érzékelőket hagyja figyelmen kívül azért, hogy a hatástalanításra szolgáló eszközhöz hozzá lehessen férni.

A hatástalanításra legfeljebb 45 másodpercet szabad megengedni.

Ha a hatástalanítás nem fejeződik be a meghatározott időn belül, riasztási állapotot kell jelenteni.

A hatástalanítást legfeljebb 30 másodpercig kell jelezni.

Ha riasztási állapot jön létre a hatástalanítási eljárás során, a riasztási állapotot csupán egy belső figyelmeztető eszközzel kell jelezni vagy jelenteni.

Ha a behatolásjelző rendszer távfelügyeleti átjelzést is tartalmaz, a riasztási állapotot mindaddig nem kell távjelezni, amíg a kijelző vagy a belső figyelmeztető eszköz legalább 30 másodpercig nem működött.

6.1.11. A behatolás- és támadásjelző rendszer riasztási állapot utáni visszaállítása

A behatolás- és támadásjelző rendszernek tartalmaznia kell a behatolás- és támadásjelző rendszernek, vagy egy részének a riasztási állapotot követő visszaállítására szolgáló eszközt.

A visszaállító eszközhöz való hozzáférést a 2. szinthez való hozzáféréssel rendelkező felhasználókra kell korlátozni.

A behatolás- és támadásjelző rendszer bármelyik biztonsági fokozata távolról visszaállítható lehet, feltéve, hogy a 2. szinten a hozzáférés elérhető és információ áll rendelkezésre a riasztás okának meghatározásához.

6.1.12. Szabotázs-riasztási állapot utáni visszaállítása

A behatolás- és támadásjelző rendszer rendelkezzen olyan eszközzel, amellyel a behatolás- és támadásjelző rendszer visszaállítható normál állapotába egy szabotázs-riasztást követően.

Egy szabotázs-riasztás jelentését követően a behatolás- és támadásjelző rendszer a következő jogosultsági szinteken legyen visszaállítható:

- 1. és 2. fokozat esetén: a 2-es jogosultsági szinten,
- 3. és 4. fokozat esetén: a 3-as jogosultsági szinten.

6.1.13. Tiltási művelet

A behatolás- és támadásjelző rendszer tartalmazhat olyan eszközt, amely egyedi funkciók vagy funkciócsoportok tiltásához szükséges.

A tiltó eszközhöz való hozzáférést a 2-es jogosultsági szintű felhasználókra kell korlátozni.

A tiltási állapotot meg kell szűntetni, amikor a behatolásjelző rendszer hatástalanított.

6.1.14. Kizárás

A behatolás- és támadásjelző rendszer tartalmazhat olyan eszközt, amely egyedi funkciók vagy funkciócsoportok kizárásához szükséges.

A kizárási jogosultságot a következő szintű felhasználókra kell korlátozni:

1. és 2. fokozat esetén: a 2-es jogosultsági szinten,
3. és 4. fokozat esetén: a 3-as jogosultsági szinten.

6.1.15. Egyéb műveletek

A behatolás- és támadásjelző rendszer tartalmazhat olyan eszközt, amely a jelen ajánlásba kifejezetten nem tartozó más műveletek végrehajtásához szükségesek.

Más műveleteket, amelyek nem befolyásolják a riasztás-jelzések vagy üzenetek feldolgozását, a megfelelő jogosultsági szintű felhasználóknak kell végrehajtaniuk.

Más műveleteket, amelyek közvetlenül vagy közvetve befolyásolják a I behatolás- és támadásjelző rendszer funkcióit, a 3-as jogosultsági szintű felhasználónak kell végrehajtania.

6.1.16. Jelzésfeldolgozás

A jelzések vagy üzenetek feldolgozásának függenie kell a behatolás- és támadásjelző rendszer állapotától és a jelzés vagy üzenet típusától.

1. PÉLDA: egy szabotázsjelzés vagy üzenet feldolgozása attól függően módosul, hogy a behatolásjelző rendszert élesítették-e vagy sem.

Ezen kívül a feldolgozás a behatolás- és támadásjelző rendszer konfigurálásától is függ.
2. PÉLDA: figyelmeztető eszköz vagy riasztásátviteli rendszer megléte.

A ***B1 3. sz. táblázat*** tartalmazza a behatolási, a szabotázs és a hibajelzések, és/vagy üzenetek feldolgozására vonatkozó követelményeket.

6.1.17. Behatolás-jelzések vagy üzenetek

A behatolásjelző érzékelőktől származó jelzéseket, és/vagy üzeneteket az ***1. fejezet*** szerint kell feldolgozni. Egy riasztási állapot jelentését követően a behatolásjelző rendszer folytathatja éles állapotbeli működését, ha a külső figyelmeztető eszköz működésének leghosszabb időtartama korlátozva van.

MEGJEGYZÉS: A riasztást fogadó központnak jelentett többszörös riasztási, szabotázs vagy hibaállapotokat fel kell dolgozni a nem kívánatos válasz elkerülése érdekében.

6.1.18. Szabotázsjelzések

A behatolás- és támadásjelző rendszer biztonsági fokozatától függően a szabotázsjelzést az ***1. fejezet*** szerint kell feldolgozni.

A 3-as és 4-es biztonsági fokozatú behatolásjelző rendszerekben - ha lehetséges - a szabotázsjelzést okozó feltételt tiltani lehet.
PÉLDA: amikor egy szabotázs érzékelő meghibásodott, az érzékelőt tiltani lehet és a behatolásjelző rendszer többi részét pedig mindaddig működtetni, amíg a hibás érzékelőt meg nem javítják

6.1.19. Hibajelzések

A behatolás- és támadásjelző rendszer biztonsági fokozatától függően a hibajelzéseket a ***B 1.1. fejezet*** szerint kell feldolgozni.

6.1.20. Kijelzések

Minden, az ***1. fejezetben*** bemutatott kötelező kijelzőeszközt együtt, ugyanabban a helyiségben kell elhelyezni.

Járulékos kijelzésekről lehet gondoskodni más helyiségekben.

A kijelezni kívánt feltételeknek mindaddig hozzáférhetőknek kell lenniük a kijelzőeszköz számára, amíg nyugtázásuk megtörténik.

A kijelzőeszközöknek meg kell felelniük az ***MSZ EN 60073*** szabvány és a ***CLC/TS 50131-4: 2006*** műszaki előírás követelményeinek.
1. MEGJEGYZÉS: Az ***MSZ EN 60073*** követelményei csak a fényjelzőkre és a hangfényjelzőkre vonatkoznak.

2. MEGJEGYZÉS: Az ***MSZ EN 60073*** színes fényjelzők használatára vonatkozó követelményeket tartalmaz, amelyek nem szükségszerűen alkalmazandók, amikor a színt nem a kijelzők megkülönböztetésére használják.

PÉLDA: monokromatikus folyadékkristály kijelző alkalmazása

Az érzékelő aktív állapotát mutató jelzéseinek vagy üzeneteinek egyedi kijelzéséről a **(b)** típusú érzékelők esetén gondoskodni kell, vagy az érzékelőn, vagy pedig a vezérlő- és kijelző-berendezésen, vagy a kiegészítő vezérlő- berendezésnél. Az **(a)** típusú érzékelőket nem kell ellátni egyedi kijelzővel, azonban minden tíz db. **(a)** típusú érzékelőt közös kijelzőeszközzel kell ellátni. A szabotázs, vagy a hiba kijelzése hallható lehet, ha a behatolás- és támadásjelző rendszer hatástalanított állapotban, vagy hatástalanítás közben van.

6.1.21. Jelentés

A riasztási állapotot a behatolás- és támadásjelző rendszer állapotától, biztonsági fokozatától és a riasztási állapot típusától függően. jelenteni kell

A jelentést vagy a figyelmeztető eszköz, vagy pedig egy riasztásátviteli rendszer hajtja végre.

6.1.22. A biztonsági fokozat szerinti követelmények

A jelentés eszközének függnie kell a behatolás- és támadásjelző rendszer biztonsági fokozatától, és meg kell felelnie legalább az ***1. fejezetben*** megadott követelményeknek.

A behatolás- és támadásjelző rendszer biztonsági fokozatától függően - amikor a behatolás- és támadásjelző rendszer riasztásátviteli rendszert tartalmaz - a riasztásátviteli rendszernek a ***B.3. fejezet*** szerinti működési követelményeket kell teljesítenie.

A jelentés eszköze kiegészíthető nem kötelező eszközzel, feltéve, hogy az ilyen eszközök nem gátolják a kötelező eszköz helyes működését.
PÉLDA: hálózatról meghajtott szirénák.

Amikor egy riasztásátviteli rendszert figyelmeztető eszközzel egészítenek ki, akkor a figyelmeztető eszköz működtetésében legfeljebb 10 perc késleltetés lehet.

A figyelmeztető eszköz működése megszakítható, feltéve, hogy a riasztásátviteli rendszerhez vagy más fogadó állomáshoz egy a riasztásátviteli úton át érkező jelentést a riasztásátviteli rendszer riasztásfogadó állomása a késleltetési időn belül nyugtázza.

Ha a riasztásátviteli úton hibát érzékelnek, a figyelmeztető eszközök késleltetései automatikusan meg kell, hogy szűnjenek - feltéve, hogy valamennyi lehetséges átviteli úton a hiba vagy hibák érzékelése megtörténik.

A hangot adó figyelmeztető (hangjelző-) eszközöknek legalább 90 másodpercig működniük kell. A leghosszabb működési idő 3perc lehet.

A behatolás- és támadásjelző rendszernek rendelkeznie kell olyan eszközzel, amely lehetővé teszi látható figyelmeztető (fényjelző) eszközök használatát a hangjelző eszközök kiegészítése céljából. A hangjelző eszközökre vonatkozó időkorlátozásokat a látható figyelmeztető eszközökre nem szükséges alkalmazni. Az elsődleges tápáramforrás hibáinak jelentését legfeljebb 1 óráig lehet késleltetni.

6.1.23. Szabotázs kialakulásával szembeni biztonság

6.1.23.1. Szabotázs elleni védelem

A behatolás- és támadásjelző rendszer egységeit el kell látni olyan eszközzel, amely meggátolja a belső elemekhez való hozzáférést, a szabotázs kockázatának minimalizálása céljából. A szabotázs elleni védelemre vonatkozó követelmények változhatnak a behatolás- és támadásjelző rendszer biztonsági fokozatától és attól függően, hogy a behatolás- és támadásjelző rendszer adott egysége a felügyelt területen belül vagy kívül helyezkedik-e el.

A behatolás- és támadásjelző rendszer azon egységeinek, melyek az általa felügyelt helyiségeken kívül helyezkednek el, legyenek megfelelő eszközzel ellátva a szabotázs érzékelésére és az ellene való védelemre.

PÉLDA: kiegészítő vezérlőberendezés, figyelmeztető eszköz.

Valamennyi csatlakozási pontot és mechanikai, vagy elektronikus beállító szerkezetet a részegységek házán belül kell elhelyezni.

A ház kellően robusztus és zárt legyen, hogy meggátolja a belső részegységekhez való, látható sérülés nélküli, észrevétlen hozzáférést.

A vezérlő- és kijelző berendezés, a kiegészítő vezérlő- és kijelző berendezés, a riasztásátviteli rendszer és a figyelmeztető eszköz belső elemeihez való hozzáférésre szolgáló eszközök legyenek robusztusak és mechanikailag védettek. A szabályos hozzáféréshez speciális szerszám használatára legyen szükség.

Az érzékelők belső elemeihez való hozzáférésre szolgáló eszközök legyenek védettek, és a szabályos hozzáférés csak szerszámmal legyen lehetséges.

6.1.23.2. A szabotázs érzékelése

A szabotázs érzékelését a behatolás- és támadásjelző rendszer minden egységének a ***B alfejezetekben*** leírtak szerint kell tartalmaznia.

Az 1-es biztonsági fokozatban; ha a behatolás- és támadásjelző rendszer a jelzések, üzenetek vagy részegységek helyettesítése elleni védelemmel rendelkezik, a csatlakozó dobozokat nem kell ellátni szabotázs-érzékeléssel. A szabotázs-érzékelésnek működnie kell mind élesített, mind pedig hatástalanított állapotban valamennyi biztonsági fokozatban.

Az érzékelendő szabotázs eseményeket a ***B alfejezetekben*** sorolja fel biztonsági fokozatonként.

A felügyelt helyiségeken kívüli használatra tervezett kiegészítő vezérlő- és kijelző berendezésnek tartalmazniuk kell olyan eszközt, amely a vezérlő- és kijelző berendezés, és a kiegészítő vezérlő- és kijelző berendezés közötti jelzések vagy üzenetek helyettesítésének megakadályozására szolgál. Ezt a követelményt figyelmen kívül lehet hagyni, abban az esetben, ha az ilyen helyettesítés nem befolyásolhatja a behatolás- és támadásjelző rendszer helyes működését.

6.1.24. Összeköttetések

Az összeköttetések a célnak megfelelően legyenek megválasztva, és folyamatosan álljanak rendelkezésre ahhoz, hogy kommunikációs eszközül szolgáljanak a behatolás- és támadásjelző rendszer egységei között.

A behatolás- és támadásjelző rendszer részegységei közötti összeköttetéseket az alábbi módok valamelyikével lehet megvalósítani:

- különleges vezetékes összeköttetések;
- nem különleges vezetékes összeköttetések;
- vezeték nélküli összeköttetések.

6.1.24.1. Az összeköttetések és a kommunikáció megfigyelése

Az összeköttetéseket meg kell figyelni azért, hogy megbizonyosodjunk a behatolás- és támadásjelző rendszer egységei között fennálló kommunikációról, azért hogy a behatolás- és támadásjelző rendszer működéséhez szükséges behatolási-, szabotázs- vagy hibajelzések, és/vagy -üzenetek továbbítása lehetővé váljon.

A behatolás- és támadásjelző rendszer egységei közötti kommunikáció lehetőleg periodikus kommunikáció legyen.

A behatolás- és támadásjelző rendszer egységei közötti kommunikáció felügyeletéről gondoskodni kell a jelzések és/vagy üzenetek helyettesítésének érzékelése céljából. A megfigyelésre vonatkozó követelményeket a következő szakaszok határozzák meg.

6.1.24.2. A behatolás- és támadásjelző rendszer egységei közötti periodikus kommunikáció

A behatolás- és támadásjelző rendszer egységei közötti periodikus kommunikációnak a ***B.1. 01. sz. táblázat*** által meghatározott időkön belül kell lezajlania. A behatolás- és támadásjelző rendszer biztonsági osztályától függően a behatolás- és támadásjelző rendszer egységei közötti kommunikációnak az élesítési eljárás során kell megtörténnie.

Amikor a behatolás- és támadásjelző rendszer hatástalanított, a behatolás- és támadásjelző rendszer egységei közötti olyan kommunikáció esetén, amely nem jön létre a ***B.1. 01. sz. táblázatban*** meghatározott időkön belül, hibajelzésnek kell létrejönnie. Amikor a behatolás- és támadásjelző rendszer élesített, és a behatolás- és támadásjelző rendszer egységei közötti kommunikáció nem jön létre úgy, ahogy azt a ***B.1. 01. sz. táblázat*** előírja, szabotázs-jelzésnek kell létrejönnie.

Hordozható vezérlőberendezésnek nem kell teljesítenie a periodikus kommunikáció követelményeit.

B.1. 01. sz. táblázat: A behatolás- és támadásjelző rendszer egységei közötti periodikus kommunikáció

Kommunikációs periódusok	1. biztonsági fokozat óra	2. biztonsági fokozat óra	3. biztonsági fokozat óra	4. biztonsági fokozat perc
Élesítés alatt	Op	K	K	K
Gyakoriság	4	2	1	15

Jelmagyarázat. Op = Választható; K = Kötelező

MEGJEGYZÉS: A kommunikáció öltheti egy jelzés formáját, például egy áramét, amely egy mágnesesen működtetett kapcsolón vagy érintkezőn keresztül folyik, vagy pedig korszerűbb kommunikációra képes eszközök közötti üzenet formáját. Egy szokványos behatolás- és támadásjelző rendszerben, amely központi vezérlő- és kijelző berendezést tartalmaz, a kommunikáció rendszerint a központi vezérlő- és kijelző berendezés és a behatolás- és támadásjelző rendszer egyéb egységei között zajlik. Fennáll annak is a lehetősége, hogy központi vezérlő- és kijelző berendezés nélküli behatolás- és támadásjelző rendszert hoznak létre úgy, hogy a vezérlő- és kijelző berendezés funkcióit elosztják a többi egység között. Az ilyen típusú behatolás- és támadásjelző rendszerekben a kommunikáció a behatolás- és támadásjelző rendszer bármely vagy összes egységei között lehetséges.

6.1.24.3. Az összeköttetések rendelkezésre állásának megfigyelése

Az összeköttetéseket meg kell figyelni annak ellenőrzése céljából, hogy rendelkezésre állnak-e. A rendelkezésre állás ideje nem lehet kevesebb a ***B.1. 02. sz. táblázatban*** meghatározott időnél.

Amikor a behatolás- és támadásjelző rendszer hatástalanított, és az összeköttetések rendelkezésre állása nem teljesíti a ***B.1. 02. sz. táblázat*** követelményeit, hibajelzésnek kell létrejönnie.

Amikor a behatolás- és támadásjelző rendszer élesített, és az összeköttetések rendelkezésre állása nem teljesíti a ***B.1.02.sz. táblázat*** követelményeit, szabotázsjelzésnek kell létrejönnie.

B.1. 02. sz. táblázat: Az összeköttetések rendelkezésre állásának megfigyelése

Rendelkezésre állás	1. biztonsági fokozat s	2. biztonsági fokozat s	3. biztonsági fokozat s	4. biztonsági fokozat s
Legalacsonyabb rendelkezésre állás	60-ban 30	60-ban 30	20-ban 10	20-ban 10

1. MEGJEGYZÉS: A rendelkezésre állást 60 és 20 másodperces rögzített időszakon át mérik. Az összeköttetéseknek legalább a megfigyelési idő 50 %-ában rendelkezésre kell állniuk a kommunikáció eszközének biztosítására. Az összeköttetések számos ok miatt válhatnak hozzáférhetetlenné, többek között: vezetékes rendszerben a huzalozás sérülése miatt, megosztott összeköttetésekkel rendelkező rendszerekben az egyéb alkalmazásokból jövő zavarás miatt. Az összeköttetések rendelkezésre állásának csökkenéséért vagy megszűnéséért felelős körülményeket véletlen vagy szándékos okok idézhetik elő.

2. MEGJEGYZÉS: Valamennyi behatolás- és támadásjelző rendszerben létfontosságú a kommunikációs eszközök rendelkezésre állásának megfigyelése. A következő példák szemléltetik az összeköttetések megfigyelésének eszközeit a különféle típusú összeköttetéseket használó behatolásjelző rendszerekben:

Az összeköttetések típusai:

(a) Különleges vezetékes rendszerek*:*

A behatolás- és támadásjelző rendszer egységei közötti összeköttetésen át továbbított jelzés vagy üzenet, amikor is a jelzés vagy üzenet vételének hibája az összeköttetés vagy a részegység hibáját jelzi.

(b) Vezetékes összeköttetéseken osztozó rendszerek:

Mint az *(a)* pontban, de kiegészítésként vagy alternatív módon az összeköttetések megfigyelhetők abból a szempontból is, hogy a többi rendszer zavarja-e a jelátvitelt, illetve az összeköttetést rendelkezésre bocsátják-e.

(c) Vezeték nélküli rendszerek:

Mint az *(a)* pontban, de további vagy vagylagosan az összeköttetés (rádiófrekvenciás csatorna) olyan megfigyelése is lehetséges, mely kimutatja azokat a körülményeket, amelyek meggátolhatják az összeköttetésen keresztüli kommunikációt.

6.1.25. Helyettesítés megfigyelése

A behatolás- és támadásjelző rendszer biztonsági fokozatától függően megfigyelésről kell gondoskodni a behatolás- és támadásjelző rendszer egységeinek és a jelzések, és/vagy üzenetek helyettesítésének észlelése céljából. A megfigyelésnek ki kell elégítenie a ***B.1. 03. sz. táblázat*** követelményeit.

Amikor a behatolás- és támadásjelző rendszer hatástalanított és helyettesítést érzékel a rendszer, hibajelzést kell létrehozni.

Amikor a behatolás- és támadásjelző rendszer élesített és helyettesítést érzékel a rendszer, akkor szabotázsjelzést kell létrehozni.

B.1. 03. sz. táblázat: Helyettesítés megfigyelése

Megfigyelési követelmények	1. biztonsági fokozat	2. biztonsági fokozat	3. biztonsági fokozat	4. biztonsági fokozat
I&HAS részegységek helyettesítése	Op	Op	K	K
Jelzések, illetve üzenetek helyettesítése	Op	*Op*	K	K
Jelmagyarázat: Op = Választható; K = Kötelező				

6.1.25.1. Helyettesítés megfigyelése: időzítési követelmények

A helyettesítést a ***B.1. 04. sz. táblázatban*** megadott időn belül kell észlelni.

B.1. 04.sz. táblázat: Helyettesítés megfigyelése. Időzítés

Megfigyelési követelmények	1. biztonsági fokozat s	2. biztonsági fokozat s	3. biztonsági fokozat s	4. biztonsági fokozat s
I&HAS részegységek helyettesítése	Op	60	30	10
Jelzések, illetve üzenetek helyettesítése	Op	60	30	10
Jelmagyarázat: Op = Választható				

6.1.25.2. Megfigyelési időszakok

A megfigyelésnek a ***B.1. 05. sz. táblázatban*** meghatározott időszakokban kell aktívnak lennie.

B.1. 05. sz. táblázat: Összeköttetések megfigyelése

Aktív időszak	1. biztonsági fokozat	2. biztonsági fokozat	3. biztonsági fokozat	4. biztonsági fokozat
Élesítés alatt	Op	K	K	K
Élesített állapotban	K	K	K	K
Máskor	Op	Op	K	K
Jelmagyarázat: Op - Választható; K – Kötelező				

6.1.26. A behatolás- és támadásjelző rendszer időzítési tulajdonsága

6.1.26.1. Behatolás kimutatása és hibák felismerése: időzítési követelmények

A 400 ms-nál hosszabb aktív idejű behatolási jelzéseket és a 10 s-nál hosszabb ideig fennmaradó hibajelzéseket fel kell dolgozni.

MEGJEGYZÉS: A behatolási és hibaüzeneteknek csak annyi ideig kell fennállniuk, amennyi a kommunikáció biztosításához kell.

6.1.26.2. Feldolgozás

A behatolási, szabotázs és hibajelzéseket, és/vagy üzeneteket 10 másodpercen belül jelenteni kell.

6.1.27.. Eseménynaplózás

A behatolás- és támadásjelző rendszer biztonsági fokozatától függően, a ***B.1. 06. táblázatban*** meghatározott eseményeket kell naplózni.

A kötelezően naplózandó események tárolására szolgáló eszköznek védetteknek kell lennie a tartalom véletlen vagy szándékos törlése vagy változtatása ellen.

A naplózó eszköznek az ***1. fejezet*** követelményeinek megfelelő kapacitással kell rendelkeznie. Véges kapacitású eszköz esetén, amikor a naplózásra rendelkezésre álló memória már betelt, a további események a legrégebbiek törlését kell, hogy eredményezzék.

A 2-es, 3-as és 4-es biztonsági fokozatú behatolás- és támadásjelző rendszerek az eseményen kívül az esemény megtörténésének időpontját és dátumát is naplózniuk kell.

Az órának évente +/- 10 percen belül pontosnak kell lennie 20 C° névleges hőmérsékleten. Az eseménynaplózó eszköz a behatolás- és támadásjelző rendszer egységeiben vagy egy riasztásfelügyeleti központban lehet elhelyezve.

MEGJEGYZÉS: Ha az eseménynaplózás a riasztásfelügyeleti központban történik, a jelentő eszközről szükségképpen az behatolás- és támadásjelző rendszernek kell gondoskodni. A riasztásfelügyeleti központban elhelyezett eseménynaplózó eszköznek ki kell elégítenie ezen szakasz követelményeit.

A 3-as és 4-es biztonsági fokozatnál gondoskodni kell a naplózott események folyamatos feljegyzéséről. Ebbe nem kell beletartoznia a folyamatosan feljegyzést előállító eszközöknek. Valamely egyedi forrástól jövő naplózott események számát háromra kell korlátozni bármely élesített időszakban.

6.1.28. Tápegység

6.1.28.1. Tápegység típusok

A típus: Egy elsődleges és egy, a behatolás- és támadásjelző rendszer által utántöltött másodlagos tápáramforrás.

***1. PÉLDA*:** újratölthető akkumulátortelep, amelyet a behatolásjelző rendszer automatikusan újratölt.

B típus: Egy elsődleges és egy, nem az behatolás- és támadásjelző rendszer által töltött másodlagos tápáramforrás.

***2. PÉLDA*:** egy akkumulátortelep, amelyet nem a behatolás- és támadásjelző rendszer tölt automatikusan.

C típus: Egy elsődleges tápáramforrás, aminek véges a kapacitása.

***3. PÉLDA*:** egy (galván) elem.

6.1.28.2. Követelmények

A tápegység legyen képes a behatolás- és támadásjelző rendszer tápellátására annak minden állapotában, beleértve az energiatároló eszközöknek az előírt időszakokban való újratöltését is. A tápegységet a behatolás- és támadásjelző rendszer egy vagy több egységében lehet elhelyezni, vagy külön házban.

Az elsődleges és a másodlagos tápegység közötti átváltás, majd visszaváltás nem idézhet elő riasztási állapotot, és másképpen sem befolyásolhatja a behatolás- és támadásjelző rendszer állapotát.

Minden biztonsági fokozatban, az olyan behatolás- és támadásjelző rendszer, amelynek **C típusú** tápegysége van, mint elsődleges tápegység, az elsődleges tápegység legkisebb használhatósági ideje elegendő legyen a behatolás- és támadásjelző rendszer energiával való ellátására egy évig a behatolás- és támadásjelző rendszer valamennyi használati körülménye között.

Valamennyi behatolás- és támadásjelző rendszerben az elsődleges tápegység hibája esetén a másodlagos tápegység legyen képes a behatolás- és támadásjelző rendszer energiával való ellátására a ***6. fejezetben*** meghatározott időtartamokra.

A 3-as és 4-es biztonsági fokozatú behatolás- és támadásjelző rendszereknél az olyan behatolás- és támadásjelző rendszerek, amelyek tartalmaznak tápegységet és a tápegység állapotát továbbítják egy riasztásfogadó központba vagy más távfelügyeleti központba, az az időtartam, amíg az alternatív tápegységnek biztosítani kell a behatolás- és támadásjelző rendszer energiával való ellátását, a ***6. fejezetben*** megadott időtartamok fele lehet.

Ha a 2-es, 3-as és 4-es biztonsági fokozatú behatolás- és támadásjelző rendszerben kiegészítő elsődleges tápegységről gondoskodnak, automatikus átváltással az elsődleges tápegység és a kiegészítő elsődleges tápegység között, az az időtartam, ameddig az alternatív tápegységnek biztosítani kell a behatolás- és támadásjelző rendszer táplálását, 4 órára csökkenthető.

Minden behatolás- és támadásjelző rendszerben gondoskodni kell olyan jelzésről, amely mutatja, ha a másodlagos tápegységről levehető feszültség a behatolás- és támadásjelző rendszer helyes működéséhez szükséges feszültségszint alá csökken.

MEGJEGYZÉS: A tényleges feszültség, amelynél a jelzés történik, nincs közvetlen kapcsolatban azzal az időtartammal, ameddig az alternatív tápegység képes a behatolás- és támadásjelző rendszer tápellátására.

Minden **A típusú** tápegységet tartalmazó behatolás- és támadásjelző rendszer esetén az alternatív tápegységet után kell tölteni, hogy legnagyobb kapacitásának 80 %-át szolgáltassa a ***6. fejezetben*** meghatározott időtartamon belül.

6.1.29. Működési megbízhatóság

Gondoskodni kell olyan eszközökről, amelyek biztosítják, hogy a behatolás- és támadásjelző rendszer rendeltetésszerű működését esetleg hátrányosan befolyásoló kezelői hibák vagy ne fordulhassanak elő, vagy pedig jelezzék azokat.

B.1. 06. sz. táblázat: Eseménynaplózás: általános funkciók

Általános funkciók	1. biztonsági fokozat	2. biztonsági fokozat	3. biztonsági fokozat	4. biztonsági fokozat
Felhasználó-azonosítás élesítéskor/hatástalanításkor	Op	Op	K	K
I&HAS élesített	Op	K	K	K
I&HAS hatástalanított	Op	K	K	K
Általános hiba	Op	K	K	K
Behatolásjelzés	Op	K	K	K
Első riasztott zóna	Op	K	K	K
Riasztás forrása	Op	K	K	K
Szabotázsriasztás	Op	K	K	K
Elsődleges táplálás hibája	Op	Op	K	K
*Elemcsere szükséges	Op	Op	K	K
Kizárás be	Op	K	K	K
Kizárás ki	Op	K	K	K
Tiltás be	Op	K	K	K
Felülbírálás	Op	K	K	K
**ATS hiba	Op	K	K	K
Időpont és dátum változtatásai	Op	Op	K	K
Konfigurációs adatok változtatásai	Op	Op	K	K
A periodikus kommunikáció hibája	Op	K	K	K
Egységek helyettesítése	Op	Op	Op	K
Jelzések vagy üzenetek helyettesítése	Op	Op	Op	K
A kommunikációs eszközök rendelkezésre állása	Op	Op	Op	K
MEGJEGYZÉS: A megadott események naplózási követelményeinek alkalmazása nem jelenti a kapcsolódó funkcióról való gondoskodás követelményét. Ha azonban a naplózandó eseményekkel kapcsolatos funkciókról gondoskodnak, a felmerülő eseményeket naplózni kell . ***Jelmagyarázat:*** Op = Választható; K = Kötelező;* = Csak az elemekre alkalmazható, ** = Ha alkalmazható				

6.1.29.1. A behatolásjelző rendszer alkotórészei

A behatolás- és támadásjelző rendszer működése során használt egységeket világosan és egyértelműen meg kell jelölni, és úgy kell logikailag elrendezni, hogy a helytelen működés lehetősége a legkisebb legyen. Csakis a felhasználói szintű funkciókat szabad a felhasználó számára hozzáférhetővé tenni.

6.1.30. Funkcionális megbízhatóság

A behatolás- és támadásjelző rendszer feleljen meg a rá vonatkozó szabványoknak. A behatolás- és támadásjelző rendszer kivitelezése és felépítése biztosítsa a behatolás- és támadásjelző rendszernek a jelen ajánlás követelményei szerinti működését. Ezt a következőkkel kell elérni:

- egyértelmű szabályokkal a kivitelezésre és a telepítésre;
- egyértelmű szabályokkal a beüzemelésre és a karbantartásra;
- pontos telepítéssel;
- rendszeres karbantartással;
- nagy jel/zaj viszonyt biztosító kivitelezéssel;
- jól megtervezett szoftverrel;
- a tervezési határokon belül működő elemekkel (feszültség, hőmérséklet);
- a funkciók tesztelhetőségével (a felhasználó és a telepítő által);
- a funkciók megfigyelésével
  Példa: felügyelő - ″watchdog″ - áramkör.

6.1.31. Környezeti követelmények

A behatolás- és támadásjelző rendszer környezeti stabilitásának azonos szintűnek kell lennie minden biztonsági osztályban.

A behatolás- és támadásjelző rendszer működését nem szabad befolyásolnia annak, ha a behatolás- és támadásjelző rendszert a környezeti osztályának megfelelő környezeti feltételeknek teszik ki. A behatolás- és támadásjelző rendszer nem változtathatja meg állapotát, egységei nem sérülhetnek meg, és nem változtathatják meg lényegesen működőképességüket.

Az ***MSZ EN 50130-5*** szabvány írja le a környezeti vizsgálati módszereket, amelyeket a behatolás- és támadásjelző rendszer egységeire alkalmazni kell, és meghatározza az alkalmazandó megfelelt/nem felelt meg követelményeket.

6.1.32. Elektromágneses összeférhetőség

A behatolás- és támadásjelző rendszer egységeire nézve az elektromágneses összeférhetőségi tulajdonságokra vonatkozó követelményeket az: ***MSZ EN 61000-6-3*** és az ***MSZ EN 50130-4:*** szabványok tartalmazzák.

6.1.33. Villamos biztonság

A behatolás- és támadásjelző rendszernek az áramütéssel és az ennek következtében előálló kockázatokkal szembeni biztonságról azáltal kell gondoskodniuk, hogy megfelelnek az ***MSZ 2364 szabványsorozat***, az ***MSZ EN 60950-1,*** és az ***MSZEN 60065*** követelményeinek.

6.1.34. Jelölések

A behatolás- és támadásjelző rendszer valamennyi egységét meg kell jelölni a következőkkel:
- a gyártó vagy a szállító neve;
- típus;
- gyártási dátum, vagy tételszám, vagy sorozatszám;
- biztonsági fokozat;
- környezeti osztály.

A jelölésnek olvashatónak, tartósnak és egyértelműnek kell lennie.

Ha a behatolás- és támadásjelző rendszer egy egységén a jelölésre szánt hely korlátozott, kódok alkalmazhatók, feltéve, hogy ezeket a kapcsolódó egység-dokumentáció leírja. Ha a kódok számára sincs elég hely, az egységnek olyan azonosítót kell tartalmaznia, amely lehetővé tesz hivatkozást arra a dokumentációra, amely a kívánt információt tartalmazza.

6.2. Egyéb részegségek

Más rendszerek részegységei beépíthetőek a behatolás- és támadásjelző rendszer, ha a behatolás- és támadásjelző rendszer teljesítménye ezáltal nem csökken.

6.3. Biztonság

A biztonságra országos és európai követelmények létezhetnek. Ez az ajánlás ezeket a követelmények nem tartalmazza, ezekre az előírásokra az érintetteknek hivatkoznia kell.

Példa: Elektronikus biztonság

6.4. Téves riasztás

A rendszer tervezői, telepítő cégek és vagyonvédelmi cégek és felhasználók felé ajánlott, hogy különös tekintettel kerüljék a téves riasztásokat.

6.5. Felelősség

A behatolás- és támadásjelző rendszer létesítésének minden egyedi lépésénél - mint a tervezés, telepítés, üzembe helyezés és átadás - a felek közti felelősséget egyértelműen meg kell határozni.

6.6. Képesítés

Azok a személyek, akik felelősek a kockázat meghatározásáért és a tervezés, telepítés, karbantartás és javítási tevékenységet végeznek, a megfelelő képesítéssel kell, hogy rendelkezzenek.
***Megjegyzés*:** ezek a képesítések országonként változhatnak.

6.7. Bizalmas adatok kezelése

A behatolás- és támadásjelző rendszer tervezése, telepítése, működtetése, karbantartása során keletkezett információkat bizalmas adatként kell kezelni.

6.8. Egyeztetések

A rendszer kialakítását az ügyféllel történő, a behatolás- és támadásjelző rendszer szakértővel, vagy bármely érdekelt féllel tartott egyeztetéssel kell meghatározni.
***Példa*:** biztosítók, vagy rendőrség

Szükség esetén szakértői véleményt kell kérni.

6.9. Kompatibilitás

Az alkotó elemek kiválasztásánál biztosítani kell, hogy a rendszer összes alkatrésze kompatibilis legyen. Bizonytalanság esetén konzultálni kell az érintettekkel.
***Példa*:** gyártó, forgalmazó, vizsgáló szervezet vagy harmadik fél.

7. A rendszer tervezése

A rendszer tervezés célja a behatolás- és támadásjelző rendszer és részegységeinek kiválasztása a környezeti követelmények figyelembe vételével.
***Példa*:** Az érzékelők száma és típusa, elhelyezésük.

7.1. Helyszíni bejárás — kockázat

A behatolás- és támadásjelző rendszer biztonsági osztálynak meghatározására a helyszínt be kell járni.

7.1.1. Tárgyak, berendezések

A behatolás- és támadásjelző rendszer tervezésnél a felügyelt helyiségben található tárgyakat is figyelembe kell venni. A ***B.1. A függelék*** mutatja be a figyelembe veendő tényezőket. A lista nem teljes, miután több más tényező is felmerülhet.

7.1.2. Épület

A behatolás- és támadásjelző rendszer tervezésénél több más tényező mellett meg kell vizsgálni a felügyelt terület építési módját, elhelyezkedését, a felhasználás típusát és a bűnügyi előzményeket (kriminalitás). A ***B.1. B függelék*** mutatja be a figyelembe veendő tényezőket. A lista nem teljes, miután több más tényező is felmerülhet.

7.1.3. Minimális felügyeleti szintek

A ***B.1. A és B.1. B függelék*** által kerül sor a minimális felügyeleti szintek meghatározására. Ezen megállapítások alapján a szakértő megállapítja a behatolás várható módszerét, mely a terület különböző pontjain történhet meg, és ennek alapján meghatározza a behatolás- és támadásjelző rendszer **biztonsági fokozatát és kockázati osztályát** és a behatolás- és támadásjelző rendszer felépítését. A **B.1.** ***E függelék*** a behatolás módszereinek példáját mutatja be, melyek ellen valószínűleg védekezni kell.

7.2. A helyszíni bejárás — egyéb befolyásoló tényezők

A behatolás- és támadásjelző rendszert a felügyelt terület helyszíni felmérése alapján a meglévő és/vagy potenciálisan kialakuló körülmények szem előtt tartásával kell megtervezni. A behatolás- és támadásjelző rendszer működését befolyásoló körülmények két csoportba oszthatók:

- A felügyelt terület olyan feltételei, melyekre a behatolás- és támadásjelző rendszer felhasználójának várhatóan ráhatása van. A ***B.1. C függelék*** felsorolja ezeket a tényezőket. A lista nem teljes, miután több más tényező is felmerülhet.
- Azok a feltétek, melyek a felügyelt területen kívül állnak fenn, amely felett a behatolás- és támadásjelző rendszer felhasználójának várhatóan nincs ráhatása, a ***B.1. D függelék*** sorolja fel. A lista nem teljes, miután több más tényező is felmerülhet.

Megjegyzés: A helyszíni felmérés célja a rendszer (terv) ajánlat készítése során kell beazonosítani azokat a tényezőket, melyek befolyásolhatják a rendszer részegségeinek az elhelyezését. – különösen az érzékelők tekintetében.

7.3. A rendszer terv ajánlat (árajánlat)

A rendszer ajánlatot vagy az ügyfélnek, vagy az ügyfél által meghatalmazott képviselőnek kell benyújtani. Ez az ajánlat a ***B.1. F függelék*** információit kell, hogy tartalmazza.

A rendszer ajánlat módosítható a kivitelezés során.
Példa: A kiviteli terv és megvalósulási terv szakaszaiban.

Ezeket a módosításokat mindkét félnek jóvá kell hagynia, és a dokumentációt ennek megfelelően módosítani kell.

7.3.1. A rendszer elemeink kiválasztása

Csak olyan részegységeket szabad kiválasztani, melyek megfelelnek a biztonsági fokozatnak, védelmi osztálynak és a környezeti osztálynak.

Különös figyelemmel kell lenni a téves riasztások számának minimalizálására.

7.3.2. A készülékek telepítése:

7.3.2.1 A vezérlő- és kijelző berendezés telepítése

A vezérlő- és kijelző berendezést a felügyelt területen belülre kell telepíteni. Ahol a behatolás- és támadásjelző rendszer alrendszerekre van felosztva – melyeknek különféle biztonsági fokozatai vannak – a vezérlő- és kijelző berendezésnek a legmagasabb biztonsági fokozatú alrendszer területén kell elhelyezkednie. A vezérlő- és kijelző berendezést a 3. és 4. biztonsági fokozatú behatolás- és támadásjelző rendszer telepítésénél az alrendszerek felügyeleti területén kell elhelyezni.
A vezérlő- és kijelző berendezés és a kiegészítő kijelző berendezés telepítésére a ***B.1. G. függelék 20.*** . és ***21. pontjaiban*** mutatunk be példákat.
Ha a hatástalanítás a felügyelt területen kívül kezdődik, és a felügyelt területen belűl fejeződik be, akkor a vezérlő- és kijelző berendezés és kiegészítő kijelző berendezés telepítését úgy kell végrehajtani, hogy a felügyelt terület végső kilépési pontjánál legyen.

A vezérlő- és kijelző berendezés és a kiegészítő kijelző berendezés telepítésénél figyelembe kell venni, hogy ezeknek a működtetését illetéktelen személyek ne figyelhessék meg.

7.3.2.2 A riasztásátviteli berendezés telepítése:

A riasztásátviteli berendezést a felügyelt területen belűl kell telepíteni. Ahol a behatolás- és támadásjelző rendszer alrendszerekre van felosztva – melyeknek különféle biztonsági fokozatai vannak – a riasztásátviteli berendezésnek a legmagasabb biztonsági fokozatú alrendszer területén kell elhelyezkednie. A riasztásátviteli berendezés telepítési példáit a ***B.1. G. függelék 23.pontjában*** mutatjuk be.

7.3.2.3 Az érzékelők telepítése:

Az érzékelőket a gyártó cég ajánlásainak megfelelően kell telepíteni, biztosítva a a hatósugarát, figyelembe véve a kitakarásokat, melyet a behatolás- és támadásjelző rendszer tervezési fázisában megállapítottak. Az érzékelők telepítésének példáit a ***B1 G. függelékben*** mutatjuk be.

7.3.2.4 Figyelmeztető eszközök telepítése:

A figyelmeztető eszközöket olyan pozíciókba kell telepíteni, melyek nehezen elérhetőek, hogy minimalizálják a szándékos vagy a vétlen rongálás valószínűségét. Ugyanakkor a karbantartására, javítására megfelelő hozzáférési lehetőséget kell biztosítani számukra, és olyan helyre kell telepíteni, ahonnan hatékony riasztó jelzést tudnak kibocsátani.

A figyelmeztető eszközt úgy kell felszerelni, hogy minimalizáljuk annak esélyét, hogy az eltávolítása ne eredményezzen riasztást.

Azokat a külső szerelésű figyelmeztető eszközöket, amelyek a felügyelt területen kívülről hozzáférhetőek, szabotázsvédelemmel kell ellátni.
***Példa*:** A vezetékeket fém csőbe kell vezetni.

7.3.2. Összeköttetés:

Olyan összeköttetéseket kell alkalmazni, melyeket a rendszer megkövetel és a környezeti feltételeket is kielégíti.

Ha a vezetékes összeköttetést használnak, a vonatkozó villamos szabványoknak megfelelően kell azokat kivitelezni, beleértve a gyártó cég előírásait.

7.3.2.1. Speciális vezetékes összeköttetés előírásai:

Amikor vezetékes összeköttetés létesül, a vezetékeket a felügyelt területen belűl kell elhelyezni. Ha az összeköttetéseket nem praktikus a felügyelt területen belűl kialakítani, ezeket szabotázsvédelemmel kell ellátni.
***Példa*:** A vezetékeket fém csőbe kell vezetni.

Az összeköttetésre használt vezetékek méretezése és anyaga, valamint szigetelése olyan legyen, hogy a feszültség, amit továbbít a rendszer bármilyen részegységének, ne legyen kevesebb, mint a minimálisan meghatározott működtetési feszültség, melyet a maximális terhelési állapotban mérnek a megadott minimális tápfeszültség megléte mellett.

Az összes, összeköttetésre használt vezetéket megfelelő módon kell rögzíteni, és a szerelésnek meg kell felelni az általánosan elfogadott szereléstechnológiának.

Azok a vezetékeknek, melyek ki lehetnek téve vétlen rongálásnak, járulékos mechanikai védelemmel kell ellátni.
***Példa*:** A padlószinttől 2 méterig.

A vezetékeket olyan módon kell telepíteni, hogy a fizikai károsodás kockázata a legkisebb legyen. Amennyiben ez a fizika kockázat fennáll, a vezetékek járulékos mechanikai védelmét süllyesztett, eltakart szereléssel, vagy védőcsőben/csatornában fektetve kell megoldani.

Ha járulékos mechanikai védelmet fémes anyaggal oldják meg, gondoskodni kell ezek megfelelő leföldeléséről, nullázásáról (érintésvédelméről).

Elektromos behatások (interferencia) téves riasztásokat okozhatnak. Ez általában elkerülhető a behatolás- és támadásjelző rendszer fő betáplálásának szűrésével, az összekötő vezetékek elválasztásával az erősáramú vezetékektől, ill. árnyékolással.

Az összekötő vezetékeket nem szabad a magasfeszültségű vezetékekkel közös védőcsőben vagy csatornában vezetni.

Az összes vezetékkötésének mechanikus és villamos szempontból megbízhatónak kell lennie.

Az összekötő vezetékek hibáinak gyors felderítését megkönnyítendő, az összes vezetékvéget meg kell jelölni. A csatlakozó dobozokban megfelelő mérőpontokat kell kialakítani a hatékony hibafelderítés érdekében.
***Példa*:** Színkódolt szigetelés vagy feliratozás.
A vezetékek nyomvonalának, rögzítésének, méretének és típusának kiválasztásánál körültekintően kell eljárni – erre a ***B.1. G. függelék 1.1. pontjában*** találunk példákat.

7.3.2.2. A nem speciális vezetékes összeköttetés előírásai

Ha ezt a vezetékezést választjuk, a **7.3.3.1.** pont követelményein felül figyelembe kell venni a más rendszerek hatását a behatolás- és támadásjelző rendszerre. Ez a téma különösen jelentős lehet, ha a többi rendszerek meghibásodnak – erre az esetre a ***B.1. G. függelék 1.2. pontjában*** találhatóak példákat.

7.3.2.3. Vezeték nélküli összeköttetések

A vezeték nélküli összeköttetés kiválasztásánál komoly megfontolás tárgyává kell tenni a szándékos, vagy vétlen zavarás befolyását, melyek a behatolás- és támadásjelző rendszer által használttal megegyező frekvenciát és/vagy jel-modulációt használják. Ilyen jelátvitel a behatolás- és támadásjelző rendszerben szabotázs vagy hibajelet válthat ki, vagy meggátolja a kapcsolatrendszer helyes működését – erre az esetre a ***B.1. G. függelék 1. - 3. pontjában*** találhatóak példák.

7.3.4. Élesítés és hatástalanítás

Különösen körültekintően kell eljárni az élesítés és hatástalanítás módszereinek kiválasztása során. Amikor csak lehetséges, az élesítés és a hatástalanítás befejezése a felhasználó szándékos beavatkozását követelje meg.

Az élesítés és hatástalanítás eljárását hallható, vagy látható jelzésnek kell kísérnie, mutatva, hogy az eljárás folyamatban van, vagy befejeződött.

7.3.4.1. Élesítés

Az élesítést vagy a felügyelt területen belűl lehet kezdeni, és ezt a felügyelt területen kívül befejezni, vagy az egész élesítési eljárást a felügyelet területeken kívül is el lehet végezni akkor, ha a megfelelő kiegészítő vezérlő berendezést használjuk.

A behatolás- és támadásjelző rendszert nem szabad addig élesíteni, amíg a behatolás- és támadásjelző rendszer nincs normál üzemmódban. A behatolás- és támadásjelző rendszer néhány korlátozó feltétel mellett élesíthető - megelőzendő, hogy az élesítést kihagyják.
Megjegyzés*:** Az ***MSZ EN 50131-1 szabvány *8.3.3.1 pontja* tartalmazza azokat a feltételeket, melyek betartásával az élesítés ilyen esetben is végrehajtható.

Amikor az élesítést a felügyelt területen belül kezdik meg, és ezt a felügyelt területeken kívül fejezik be, maximalizált időintervallumot kell adni arra, hogy az élesítési eljárást befejezzék. Ennek a maximális élesítési periódusidőnek a leteltekor jelzésnek kell kiváltani.

Amikor az élesítés a felügyelt területeken belűl kezdődik, és a felügyelt területeken kívül fejeződik be, az élesítés kezdetét és befejezését jelzésnek kell kísérnie. Ez a jelzés időben korlátozott legyen.

Amikor a behatolás- és támadásjelző rendszer élesítését teljes mértékben a felügyelt területeken kívül folytatjuk le, az élesítési folyamat befejezését jelzésnek kell kísérnie. Ez a jelzés időben korlátozott legyen.

7.3.4.2. Hatástalanítás

A hatástalanítás vagy a felügyelt területeken belűl kezdődik és fejeződik be, vagy teljes mértékben a felügyelt területeken kívül történik a megfelelő kiegészítő vezérlő berendezést használatával.

Különösen fontos, hogy megelőzzük a felügyelt területekhez történő fizikai hozzáférését megakadályozzuk a végső kilépési pontnál addig, ameddig vagy a belépési eljárás elkezdődik, vagy amíg a behatolás- és támadásjelző rendszer hatástalanított állapotba nem kerül.

Amikor a hatástalanítás a felügyelt területeken kívül kezdőik, és a felügyelet területeken belűl fejeződik be, jelzés kell biztosítani a hatástalanítási eljárás kezdetekor és befejezésekor.

Amikor a behatolás- és támadásjelző rendszer hatástalanítása teljes mértékben a felügyelt területeken kívül történik, jelzést kell biztosítani a behatolás- és támadásjelző rendszer hatástalanított állapotba kerülésekor. Ez a jelzés időben korlátozott legyen.

A hatálytalanítási eljárás időtartamára maximalizált időintervallumot kell adni arra, hogy az hatástalanítási eljárást befejezzék. Ennek a maximális hatástalanítási periódusidőnek a leteltekor jelzésnek kell kiváltani.

7.3.5. A belépési és távozási útvonalak

Ha a behatolás- és támadásjelző rendszer élesítése, vagy hatástalanítás két lépésben történik, az útvonalaz ezen két pont között jól át kell gondolni, és ennek a lehető legrövidebbnek kell lennie.
Példa: Az élesítés a vezérlő- és kijelző berendezésnél vagy az kiegészítő vezérlő berendezésnél kezdődik, és a végső kilépési pontnál fejeződik be.

Az élesítési és hatástalanítási eljárások közben ki kell jelezni, hogy az élesítés és hatástalanítás két lépésben fog történni, és ennek a kijelzésnek érzékelhetőnek kell lennie a teljes belépési és kilépési folyamat alatt és a végső kimeneti pontnál is.

A vezérlő és kijelző berendezést úgy kell kialakítani, hogy a belépési és/vagy távozási útvonal érzékelőitől jövő jelek vagy üzenetek úgy legyenek feldolgozva az élesítési vagy hatástalanítási eljárás alatt, hogy ezek ne minősüljenek behatolási jelnek vagy üzenetnek. Azok az érzékelőknek, melyek a belépési vagy távozási útvonalon helyezkednek el, felügyeltnek kell lennie, valamint a behatolás- és támadásjelző rendszer ne legyen bekapcsolható addig, ameddig normál üzemmódban nem működik.

7.3.5.1 A belépési útvonalak

Ha a hatástalanítási eljárás alatt egy olyan érzékelőt aktiválnak, mely nem része a távozási útvonalnak, ezt riasztási feltételnek számít.

7.3.5.2. A távozási útvonalak

Ha az élesítési eljárás alatt olyan érzékelőt aktiválnak, mely nem része a távozási útvonalnak, ez ki kell jelezni és ennek a jelzésnek meg kell gátolni az élesítési eljárás befejezését.

7.3.6. Kijelzés

A kijelzés követelményeit az ***MSZ EN 50131-1*** szabvány tartalmazza.

Ez a szabvány megköveteli, hogy az összes típusú, kötelezően alkalmazandó kijelző egy adott helyen együtt legyen telepítve. A jelzéseket teljesen, vagy részben meg lehet ismételni más helyeken is.

Egyedi kijelzéseket kell biztosítani minden aktivizált érzékelő riasztási állapotának kijelzésére.
***1. példa*:** Mozgás, rezgés, akusztikus, vagy infravörös sugarak érzékelői. Nem szabad több mint 10 passzív érzékelőt egy kijelzésre csatlakoztatni.
2. példa: mágneses, vagy mechanikus kontaktusok.

7.3.7. Az érzékelők csoportba foglalása

Az egyes érzékelőket csoportba lehet foglalni vezérlés vagy egyéb célból.
Példa: Részleges élesítés és/vagy hatástalanítás körülményeinek biztosítása érdekében, vagy több érzékelő elkülönítése egy önálló parancs, vagy működtetés céljából, vagy a riasztási feltételek eredetének azonosításának egyszerűsítése érdekében.

7.3.8. Átjelzés

Az átjelzés minimális feltételeit az ***MSZ EN 50131-1*** szabvány tartalmazza, a behatolás- és támadásjelző rendszer biztonsági fokozatától függően az átjelzés figyelmeztető eszköz vagy riasztásátviteli rendszer felhasználásával történhet, vagy e kettő kombinációjával.

7.3.9 Figyelmeztető eszközök

Ha a kijelzés két figyelmeztető eszközzel történik, akkor a két figyelmeztető eszköz telepítésénél törekedni kell arra, hogy a lehető legmesszebb legyenek egymástól.

Ahol fennáll annak a lehetősége, hogy a behatolás- és támadásjelző rendszer figyelmeztető eszköz hangjelzését összetéveszthetjük más riasztó rendszerek figyelmeztető eszköz hangjelzésével, meg kell fontolni, hogy a behatolás- és támadásjelző rendszer figyelmeztető eszköz hangját meg tudjuk különböztetni a más riasztó rendszerek figyelmeztető eszközétől.

Abban az esetben, ha a figyelmeztető eszköz egy riasztásátviteli rendszer kiegészítésül szolgál, a figyelmeztető eszköz üzemeltetése késleltethető – nem több, int 10 percre – vagy teljesen elnyomható, amennyiben a riasztásfogadó központ visszaigazolja az riasztásátviteli rendszerből érkező riasztási jel vételét.

7.3.10 Riasztásátviteli eszközök

Több kommunikációs mód létezik az riasztásátviteli berendezés és a riasztásfogadó berendezés között az üzenetek átvitelére. Ebben az esetben figyelemmel kell lenni arra, hogy az riasztásfogadó berendezés képes-e az riasztásátviteli berendezés jeleinek fogadására.

7.3.11 Tápellátás.

Figyelembe kell venni, hogy a behatolás- és támadásjelző rendszerben használt tápellátás megfelelő kapacitású legyen normál és riasztási üzemmódban is.

Ha a tápellátás fő tápegységből történik alternatív helyettesítő tápellátással, biztosítani kell, hogy az alternatív tápegység kapacitása képes legyen a behatolás- és támadásjelző rendszer táplálására - bele értve a figyelmeztető eszközt - arra az időszakra, ameddig működnie kell.

7.3.12. A behatolás- és támadásjelző rendszer reagálása

A behatolás- és támadásjelző rendszer aktiválását követően a behatolás- és támadásjelző rendszer reagálásának egyértelműen meghatározottnak kell lennie.

7.3.13. Tervezői jogosultság:

Tervezői jogosultsága annak a magánszemélynek és/vagy vállalkozásnak van, aki tagja az **SzVMSzK-**nak, a **Magyar Mérnöki Kamarának**, vagyonvédelmi rendszertervező jogosultsággal és rendőrhatósági igazolvánnyal rendelkezik.

8. A telepítés tervezése

A telepítés megkezdése előtt a következőket kell figyelembe venni:

8.1. A gyártó cég ajánlásai

A rendszer összes összetevőjét a gyártó cég ajánlásainak kell telepíteni. Abban az esetben, ha az eszközt nem lehet a gyártó ajánlásai szerint telepíteni, ki kell kérni a gyártó, vagy forgalmazó véleményét.

8.2. Környezeti hatások

A rendszer részegységeinek meg kell felelnie az alkalmazás a környezeti feltételeinek.

8.3. Helyszíni bejárás

Annak érdekében, hogy a behatolás- és támadásjelző rendszer teljesítménye megfeleljen a rendszer terv javaslatban meghatározott részleteknek, a helyszínt be kell járni.

Ennek a bejárásnak a célja az, hogy amennyire csak lehetséges, biztosítsa, hogy a behatolás- és támadásjelző rendszer el tudja látni azt a feladatot, amire a rendszer terv javaslat tartalmaz. Azoknak a felvetéseknek a sora, melyet a bejárás alatt meg kell fontolni, a ***G. függelékben*** található.

Megjegyzés: A tervezett behatolás- és támadásjelző rendszer méretétől és bonyolultságától függően ez a helyszíni bejárás elvégezhető az előzetes bejárás idején, vagy végrehajtható a telepítő által a behatolás- és támadásjelző rendszer telepítésének megkezdése előtt, vagy elvégezhető külön eljárásban.

8.4. Az behatolás- és támadásjelző rendszer működtetése

A helyszíni bejárásnak figyelembe kell venni a rendszer üzemeltetési körülményeit, különösen az élesítés és hatástalanítási eljárások tekintetében, annak érdekében, hogy a behatolás- és támadásjelző rendszer a lehető legegyszerűbben legyen üzemeltethető.

8.5. Az alkotó elemek kiválasztása

A helyszíni bejárás megerősíti azoknak az alkotó elemek kiválasztását, melyeket a rendszer terv javaslat tartalmaz, továbbá megerősíti azok javasolt elhelyezését – az optimális teljesítmény és a gyártó ajánlásainak megfelelően.

Azoknak az alkotó elemek elhelyezését – melyet a felhasználó fog működteti – ellenőrizni kell annak érdekében, hogy a működtetés minél könnyebb legyen.

8.6. Összeköttetések

Az összeköttetési követelményeket szintén szem előtt kell tartani, valamit a rendszert terv javaslat által meghatározott módszereket is figyelembe kell venni.

8.7. A rendszer terv javaslat (árajánlat) módosítása

A telepítés előtti bejárás feltárhat olyan problémákat, melyek a rendszer terv javaslat (árajánlat) módosítását igénylik. Bármilyen ilyen változtatást egyeztetni kell az ügyféllel, és megfelelően dokumentálni kell.

8.8. A kiviteli terv és az eszközök listája

A tervezett behatolás- és támadásjelző rendszer méretét és bonyolultságát a kiviteli terv elkészítésénél figyelemmel kell venni. A kiviteli tervet a rendszer terv javaslat alapkán kell elkészíteni, és figyelemmel kell venni a telepítés előtti bejáráson tapasztaltakat.

A telepítési tervben határozzák meg a rendszer minden egyes komponensének telepítési helyét és helyzetét.
***1. példa*:** padlószinttől mért magasság

Az összeköttetések részleteit - ha ez vezetékes, akkor a vezetékek típusát és nyomvonalát – meg kell határozni.

A rendszer konfigurációjában meg kell állapodni, és véglegesíteni kell.
2. példa: Élesítés év/vagy hatástalanítás eljárásai, áramkörök programozása, figyelmeztető eszközök késleltetése és megszólalási időtartama (ha van ilyen).

A kiviteli tervnek részleteznie kell az összes telepítendő eszköz/berendezés listáját, bele értve az elektromos vezetékek listáját is (ha van ilyen).

9. A rendszer telepítése

9.1. Képzettségi, jogosultsági követelmények

A telepítést olyan telepítők, vagy telepítő vállalkozások végezhetik el, melyek a szükséges képesítése, jogosultsága és gyakorlata van, rendelkeznek vagyonvédelmi rendszer szerelői rendőrhatósági engedéllyel és tagjai az **SzVMSzK**-nak.

A telepítőknek a behatolás- és támadásjelző rendszer telepítéséhez szükséges szerszámoknak és teszt készülékkel rendelkezni kell.

9.2. A telepítési eljárás

A rendszer a rendszer terv javaslatnak (és/vagy kivitelezési tervnek) megfelelően kell telepíteni, és összeállítani. Minden ettől eltérő megoldást az ügyféllel írásban kell egyeztetni.

10. Vizsgálat, működési teszt, üzembe helyezés és átadás

10.1. Vizsgálat

A telepítés befejezésekor a rendszer vizsgálatát el kell végezni, megerősítendő, hogy a behatolás- és támadásjelző rendszer telepítése a rendszer terv javaslatnak (ajánlat) és a kiviteli tervdokumentációnak (ha készült ilyen) megfelelően történt. Ezektől bármilyen eltérést fel kell jegyezni, és a megvalósulási dokumentációba fel kell tüntetni.

10.2. Működési teszt

Minden egyes érzékelő teljesítményét vizsgálni kell, és össze kell hasonlítani a rendszer terv javaslat és a kiviteli tervdokumentáció (ha készült ilyen) követelményeivel. Különleges figyelmet kell fordítani a mozgás- és rezgésérzékelőkre, amelyek érzékenységét változtatni lehet. Más típusú érzékelők is megkövetelhetnek üzembe helyezés előtti végső beállítást.

Az elhelyezkedéstől függő adatok beállítását ellenőrizni kell, megerősítve a kijelzéseknek és átjelzéseknek a rendszer terv javaslatnak való megfelelését.

Az eljárás végén teljes működtetés tesz végrehajtása szükséges, beleértve az összes figyelmeztető eszköz és riasztásátviteli berendezés működtetését is. Ahol riasztásátviteli berendezés van telepítve, ellenőrizni kell a riasztásfogadó központtal, vagy más fogadó központtal való kapcsolatot meggyőződve arról, hogy a teszt jeleket megfelelően fogadták-e.

10.3. Üzembe helyezés

Az összes vizsgálat befejezését követően a behatolás- és támadásjelző rendszer üzembe lehet helyezni.

10.4. Átadás

A behatolás- és támadásjelző rendszert az üzemeltető felé történő átadását olyan személynek kell elvégezni, aki rendelkezik a megfelelő képesítéssel és gyakorlattal.

A behatolás- és támadásjelző rendszer teljes – működés közbeni – bemutatása követelmény, beleértve az érzékelők vizsgálatát és működtetését.

A vezérlő- és kijelző berendezés, a riasztástovábbító berendezés és a riasztásátviteli rendszer funkcióit ismertetni kell. A riasztásfogadó központtal való kommunikációs eljárásokat is ismertetni kell (ha van ilyen).

Pontos és precíz kezelési utasításokat kell biztosítani, melyeknek tartalmaznia kell a vezérlő- és kijelző berendezés működését, és a behatolás- és támadásjelző rendszerben alkalmazott egyedi élesítési és hatástalanítási eljárásokat. Ezeket az utasításokat a behatolás- és támadásjelző rendszer működtetéséért felelős összes felhasználónak át kell adni.

A behatolás- és támadásjelző rendszer bonyolultságától függően a behatolás- és támadásjelző rendszer működtetésével kapcsolatban a felhasználóknak betanítási lehetőséget kell felajánlani. Ezen betanítás szintjének a behatolás- és támadásjelző rendszer bonyolultságának megfelelőnek kell lennie.

A betanításnak ki kell térnie arra, hogyan kell elkerülni a nem kívánt riasztásokat. Például a ablakok, ajtók megfelelő bezárása, és azoknak a készülékeknek a kikapcsolása, melyek károsan befolyásolhatják az érzékelőket.

10.5. Próbaüzem

Javaslott, hogy a behatolás- és támadásjelző rendszer átadását követően a behatolás- és támadásjelző rendszert próbaüzemeltessék az ügyféllel megállapodott időtartamig. Ez alatt az időszak alatt a behatolás- és támadásjelző rendszert normál üzemmódban kell működtetni.

Annak érdekében, hogy a próbaüzem alatti téves jelzések következményeit minimalizáljuk, a kijelzőket le kell tiltani.

Alternatívaként – mikor egy riasztásátviteli rendszert telepítünk – csak a figyelmeztető eszközök működtetését tiltjuk le, a riasztásátviteli rendszer működőképes marad. A riasztásfogadó központot riasztás esetére a telepítő cég, a riasztás fogadó cég és/vagy az ügyfél értesítésére kell beállítani

A próbaüzem alatt történt bármely riasztás okát a telepítő cégnek, a riasztás fogadó cégnek és/vagy az ügyfélnek ki kell vizsgálnia és a javításról intézkedni kell.

A próbaüzem megállapodott időszakát követően – mely alatt nem történtek téves jelzések – a behatolás- és támadásjelző rendszer teljes mértékben beüzemeltnek tekintjük.

10.6. Teljesítés igazolás

A próbaüzem sikeres befejezését követően az riasztásfogadó központot értesíteni kell, hogy a behatolás- és támadásjelző rendszer teljes mértékben működőképes. A reagáló szervezet (ha van ilyen) szintén kapjon értesítést, és ahol szükséges, ezeket a szervezeteket el kell látni a szükséges kulcsokkal és hozzáférési kódokkal.

Az ügyfél ezt követően átvételi dokumentumot ír alá, melyben kijelenti, hogy a behatolás- és támadásjelző rendszert a megvalósulási dokumentáció szerint telepítették, és ennek megfelelően működik; továbbá, hogy a behatolás- és támadásjelző rendszer megfelelő működését biztosító kezelési utasításokat átvette és annak helyes kezelésére az oktatás megtörtént.

10.7. A megvalósulási tervdokumentáció

A rendszer terv javaslat (ajánlat) alapján megvalósulási tervdokumentációt kell készíteni, melynek tartalmaznia kell azokat a változásokat, melyek a behatolás- és támadásjelző rendszer terveihez képest a telepítés során, melyek esetleg szükségessé váltak.

A megvalósulási tervdokumentációnak a telepített behatolás- és támadásjelző rendszer teljesen részletes történetét tartalmaznia kell, beleértve a berendezésre vonatkozó összes információt, telepítési helyét. Amennyiben a behatolás- és támadásjelző rendszer mérete és bonyolultsága megkívánja, a megvalósulási dokumentációnak tartalmaznia kell az elektromos vezetékek nyomvonalát és típusát is.

Ezt a megvalósulási tervdokumentációt a karbantartó és javító szervezetnek rendelkezésére kell bocsátani.

10.8. A megfelelőség bizonylatai

A telepítő cégnek megfelelőségi bizonylatokat kell, hogy átadjon az ügyfélnek, mely tartalmazza, hogy az behatolás- és támadásjelző rendszert a kiviteli terveknek, ill. a megvalósulási tervdokumentációnak megfelelően telepítették**.** ***(tervezői, és/vagy kivitelezői nyilatkozat)***.

A megfelelőségi bizonylatot kiállító vállalkozónak vagy vállalkozásnak rendelkeznie kell a 2005. évi CXXXIII. törvény (a személy- és vagyonvédelmi, valamint a magánnyomozói tevékenység szabályairól) szerinti valamennyi engedéllyel, tagjának kell lennie az SZVMSzK-nak.

Ha a behatolás- és támadásjelző rendszer, vagy valamely része megfelel valamely törvényi előírásnak, nemzeti, vagy európai szabványnak, ezeket a ***szabványosítási nyilatkozatnak*** – a szabványok és előírások **tételes felsorolásával** -tartalmaznia kell.

Hasonlóképpen tartalmaznia kell a ***szabványosítási nyilatkozatnak*** mindazon eltéréseket fenti szabványoktól, melyhez a Megrendelő (üzemeltető) előzetesen, írásban hozzájárult.

11. Dokumentumok és dokumentációk

11.1. Dokumentációk

Az ügyfélnek a következő dokumentációkat kell átadni:

- megvalósulási tervdokumentáció;
- kezelési utasítások (ezeket a dokumentációkat megfelelő részletezettséggel kell átadni, hogy minimalizáljuk a téves kezelés lehetőségét. Különös tekintettel kell lenni a következő két rész utasításaira:
  - Az élesítés és hatástalanítás folyamata;
  - A vezérlési funkciók korlátozásának módjai (pl. élesítés, hatástalanítás, újra élesítés, leválasztás vagy teszt).
  - A behatolás- és támadásjelző rendszer összes többi funkcióira vonatkozó részletes utasítások;
- Karbantartási és javítási utasítás: A behatolás- és támadásjelző rendszer karbantartásához és javításához szükséges utasítások és dokumentációk;
- A telepítő cég adatai: (név, cím , elérhetőségek);
- Karbantartó és javító cég adatai: (név, cím , elérhetőségek);
- Távfelügyeleti cég (a behatolás- és támadásjelző rendszer jelzéseire történő reagálás a feladata) adatai: (név, cím , elérhetőségek);
- Megerősítés: A riasztás valós okának megállapítására, megerősítésére vonatkozó eljárások részletes ismertetése;
- Beavatkozás: Azoknak a szervezeteknek az elérhetőségei, melyek megjelennek a felügyelt területen a riasztást követően;
- Teljesítés igazolás;
- A megfelelőség bizonylatai.

11.2. Dokumentumok

Annak a módszere, amivel biztosítani lehet a behatolás- és támadásjelző rendszer működésének minden lényeges eseményének rögzítését. Ennek a naplónak tartalmaznia kell a riasztások dátumát és időpontját, melyik érzékelő váltotta ki a riasztást. Téves riasztás esetén azoknak a tevékenységeknek a leírását, melyeket a további téves riasztások elkerülése érdekében megtettek. Ebben a naplóban kell rögzíteni a behatolás- és támadásjelző rendszeren elvégzett változtatásokat, módosításokat.

A behatolás- és támadásjelző rendszer üzemeltetési naplót bármilyen adathordozón lehet vezetni, akár a felügyelt objektumtól távol is, de a karbantartó személyzet által hozzáférhetőnek kell lennie.

A **B.1.** ***H. függelék*** tartalmazza azokat az adatokat, melyeket az üzemeltetési naplónak tartalmaznia kell, és ennek a naplónak vagy a helyszínen, vagy egyéb helyen fellelhetőnek kell lennie.

Az üzemeltetési naplót olyan formában kell megvalósítani, hogy az alkalmas legyen a bejegyzett adatok hosszú távú megőrzésére.

Abban az esetben, ha az üzemeltetési naplót a felügyelt területen tárolják, az ügyfélnek biztosítania kell, hogy ezekhez az adatokhoz a behatolás- és támadásjelző rendszer karbantartója hozzáférjen, továbbá azt is biztosítania kell, hogy ezeket az adatokat a napló bejegyzések időszakán kívül biztonságosan tárolják. Fel kell hívni az ügyfél figyelmét, hogy üzemeltetési naplót naprakészen kell tartani.

12. Az behatolás- és támadásjelző rendszer üzemeltetése

Az ügyfelet és/vagy a behatolás- és támadásjelző rendszer felhasználóját, valamint azokat, akik a behatolás- és támadásjelző rendszer karbantartásáért és javításáért felelősek a következőkről kell felvilágosítani:

- Biztosítani kell, hogy a I behatolás- és támadásjelző rendszert csak szakképzett személyek üzemeltethetik, valamint, hogy a behatolás- és támadásjelző rendszert a kezelési utasítások és az oktatáson elhangzottak szerint működtessék.
- Biztosítani kell, hogy a felügyelt helyiségeket olyan módon használják és tartsák karban, hogy ne okozzon téves riasztásokat.
- A behatolás- és támadásjelző rendszert rendszeresen tesztelni kell, annak érdekében, hogy a behatolás- és támadásjelző rendszer teljesítménye a megkívánt szinten maradjon.
- A behatolás- és támadásjelző rendszer bármilyen meghibásodását azonnal jelenteni kell a felelős vagyonvédelmi cégnek.
- Jelenteniük kell a helyiség használata ill. kialakításával kapcsolatos bármilyen változást, melyek károsan befolyásolhatják a behatolás- és támadásjelző rendszer teljesítményét.
- A dokumentumok és a dokumentációkat folyamatosan vezetni kell.

13. Az behatolás- és támadásjelző rendszer karbantartása és javítása

13.1. Általános

A behatolás- és támadásjelző rendszer megfelelő karbantartatása (felülvizsgálat és karbantartás) és javíttatása az ügyfél felelőssége – ahogy az szükséges. A behatolás- és támadásjelző rendszer karbantartására és javítására az ügyfél és egy kompetens szervezet között szerződést kell kötni. A szerződésben meg kell határozni a kapcsolattartás módszerét, mely a felügyelt területekre való bejutás teszi lehetővé. A karbantartó és javító szervezetnek és a vagyonvédelmi cégnek a nevét és telefonszámát látható módon kell elhelyezni a vezérlő- és kijelző berendezésen és a riasztásfogadó központon. Példát erre a ***B.1. I. függelékben*** találunk).

13.2. Felülvizsgálat és karbantartás

13.2.1. A karbantartási eljárás

Ahhoz, hogy a behatolás- és támadásjelző rendszer folyamatos és korrekt funkcióit biztosíthassuk, a behatolás- és támadásjelző rendszert időszakonként karban kell tartani (felülvizsgálat és karbantartás). A karbantartás gyakoriságát a telepítés befejezésekor meg kell határozni.

Az akkumulátorokat a gyártó által megadott időszakonként ki kell cserélni. Figyelembe kell venni, hogy az összes eszközt megfelelő módon újra be kell állítani a vizsgálatot követően.

A karbantartás és javítás alatt bekövetkezett minden beavatkozást – beleértve a tesztelést is – az üzemeltetési naplóba be kell jegyezni.

13.2.2. A téves riasztások megelőzése a rutin tesztelés alatt.

A behatolás- és támadásjelző rendszer karbantartásánál fontos biztosítani azt, hogy a karbantartás műveletei ne eredményezzenek nem kívánt (téves) riasztást.

Ha egy riasztásfogadó központ kapcsolat, vagy más kezelő által működtetett távfelügyelet működik a teszt időszakában, akkor alapvetően fontos a riasztásfogadó központot, vagy más távfelügyeleti központot értesíteni mielőtt a teszteket elkezdjük.

Ha a jelátvitel nem lehetséges a teszt alatt az riasztásfogadó központ, vagy más, kezelő által működtetett távfelügyelet felé, akkor ezt az állapotot vagy automatikusan, vagy kézi vezérléssel vizuálisan ki kell jelezni a vezérlő és kijelző berendezésen.

A felügyelt terület üzemeltetőit értesíteni kell minden olyan behatolás- és támadásjelző rendszer tesztről, mely a figyelmeztető eszköz működtetésével jár.

13.3. Javítás

A behatolás- és támadásjelző rendszer bármelyik részének meghibásodásának, vagy károsodásának jelzésénél az üzemeltetőnek haladéktalanul értesítenie kell az a szervezetet, vagy egyént, aki a behatolás- és támadásjelző rendszer javításáért és karbantartásáért felelős, hogy azok a szükséges javítást mielőbb elvégezhessék. A hibabejelentéstől a hibajavítás megkezdéséig eltelt időtartam megállapodás tárgyát képezi.

13.4. Tartalék alkatrészek

Ahol a behatolás- és támadásjelző rendszer nagy méretű, vagy nagy bonyolultságú, ajánlott, hogy tartalék alkatrészek álljanak rendelkezésre a felügyelt területen.

B.1. A. függelék (információ) **Rendszerterv - helyszíni bejárás - berendezések**

A behatolás- és támadásjelző rendszer tervezésénél figyelembe kell venni, hogy a rendszer arányos legyen a felügyelt terület elleni támadás kockázatával. A kockázat szinte – többek között a berendezések típusától függ. A következőkben példákat mutatunk be azokról a témákról, melyekkel foglalkozni szükséges.

A.1. Típus
Eladhatóság. A behatolót mennyire vonzza az érték.

A.2. Értékek
Az egyedi veszteség valószínű maximális értéke.
A járulékos vesztségek nagysága.
A személyes veszteség értéke.

A.3. Tömeg, vagy méret
A érték elvitelének, elszállításának nehézsége.
Az eladás és rétékesítés.
A felügyelt terüle5tre való bejutás nehézségi foka.

A.4. Előzmények
Lopási előzmények.
A korábbi lopások közben használt módszerek.

A.5. Veszély
A környezet felé.
A berendezések nem megfelelő használata.

A.6. Kár
A berendezések rongálása.
A berendezések felgyújtásának veszélye

B.1. B. függelék (információ) **- rendszer terv - helyszíni bejárás - épület**

A behatolás- és támadásjelző rendszer tervezésénél - a kockázat elemeit figyelembe véve - a felügyelt területek struktúrájának meghatározó szerepe van. Azokat a témákat, amiket szem előtt kell tartani a következőkben mutatjuk be.

B.1. Építési mód
A falak, tető, padló és a pince (ha van) építési módja.

B.2. Nyílászárók
Ablakok, ajtók, felülvilágítók, szellőző csatornák vagy bármilyen nyílások az épület héjazatában, melyek megkönnyíthetik az illetéktelen behatolást.

B.3. Lakottság
- A felügyelt területek hosszabb időszakokon ált üresek,
- Biztonsági őrök jelenléte,
- Közönség által látogatott terület e.

B.4. Kulcskezelés

A behatolás- és támadásjelző rendszer jelzéseire reagálóknak a kulcstárolókhoz való hozzáférhetősége.

B.5. Elhelyezés
- A felügyelt területek olyan területen helyezkednek el, melyeket maga bűnözési kockázatot jelentenek
- Olyan csatlakozó épületek, vagy struktúrák jelenléte, melyek a behatolót segíthetik
- A behatolás- és támadásjelző rendszer jelzésére történő reagálás sebessége és minősége
- Lakott területek közelsége, vagy más módon történő csatlakozása

B.6. Meglévő biztonság
- A meglévő mechanikai biztonsági berendezések minősége és hatásfoka
- A meglévő I&HAS (ha van) minősége és hatásfoka

B.7. Kriminalisztikai előzmények
- A felügyelt területeken történt előző lopások száma
- A támadás, vagy behatolás módszerei, melyeket az előző behatolásokkor használtak

B.8. Helyi törvényi szabályozások, rendelkezések
- A behatolás- és támadásjelző rendszer tervezését befolyásolható biztonsági követelmények
- A behatolás- és támadásjelző rendszer tervezését befolyásolható tűzvédelmi előírások
- A behatolás- és támadásjelző rendszer tervezését befolyásolható épületszerkezetek

B.9. Biztonsági környezet
- Az épület városi környezetben helyezkedik el
- Az épület külterületen helyezkedik el

B.1. C. függelék (információ) **Helyszíni bejárás –A behatolás- és támadásjelző rendszer működését befolyásoló tényezők a felügyelt területen belűl.**

A felügyelt területen belől több tényező van, melyek befolyásolhatják a behatolás- és támadásjelző rendszer teljesítményét. Ezeket a tényezőket figyelembe kell venni a berendezés típusának - különösen az érzékelők esetében – és elhelyezésének kiválasztásánál.

C.1. Vízvezetékek

Ha mikrohullámú mozgásérzékelőket használunk, figyelembe kell venni a műanyag csövekben mozgó víz hatását.

C.2. Fűtés, ventilláció, szellőzés és légkondicionáló rendszerek

Ha ezeket a fűtési, ventillációs, szellőző- és légkondicionáló rendszereket telepítenek, figyelembe kell venni ezeknek a rendszereknek a hatását az érzékelőkre, melyekre a légmozgásoknak hatása lehet

Példa: Ultrahangos érzékelők

C.3. Felfüggesztett táblák, vagy más tarágyak

A mozgásérzékelők érzékelési terében lévő felfüggesztett tárgyak vagy bármilyen más tárgy hatását figyelembe kell venni.

Példa: Függönyök, vagy növények

C.4. Felvonók

A felvonók, vagy bármely más gépészeti szerkezetek rezgést keltő hatásait figyelembe kell venni

C.5. Világítás

A fénycsövek – különösen a fluoreszcens fénycsövek – hatását figyelembe kell venni, melyek interferálhatnak a mikrohullámú érzékelőkkel; kompakt, magas fényintenzitású fénysugárzók, melyek maga szintű elektromágneses interferenciát okozhatnak; valamint a irányfényszórók, melyek a passzív infravörös érzékelők lencséjére irányulva és téves jelzés okozhatnak. A passzív infravörös érzékelők elhelyezésénél a gépjárművek fényszóróinak hatását is figyelembe kell venni.

C.6. Elektromágneses interferencia

Minden elektromos eszköz képes szándékoltan, vagy nem szándékoltan elektromágneses interferenciát okozni, mely befolyásolhatja a behatolás- és támadásjelző rendszer berendezés működését. Ezt az interferencia a berendezésbe a tápellátás vagy jelzővezetékeken keresztül juthat be, továbbá a vezetékek antennaként viselkednek a sugárzott interferencia szempontjából. A bejuttatott és kisugárzott interferencián túl figyelembe kell venni az elektrosztatikus kisülés hatását is, amikor elektronikus részegységet kezelünk. Fenti interferenciát okozható általánosan alkalmazott berendezésekre példák a következőek:

Példa: Elektromos hegesztő berendezések, *g*ázfejlesztő készülékek, elektromos generátorok, vagy motorok, motor által meghajtott háztartási gépek stb.

C.7. Külső zajok

Ott, ahol olyan ultrahangos technikát alkalmazó érzékelőket használunk , melyek ugyanabban a frekvencia tartományban működnek, mint az energia kibocsátó, ezeknek a készülékre való hatását figyelembe kell venni.

Példa: telefon csengések, levegő vezetékek (különösen, ha lyukasak), kompresszorok

C.8. Állatok

Ott, ahol mozgásérzékelőket alkalmazunk, figyelembe kell venni az állítok jelenlétének hatását. Más típusú érzékelők is érzékenyek lehetnek erre.

C.9. Huzat

Légmozgások befolyásolhatják a mozgásérzékelők teljesítményét, ezért az érzékelők elhelyezésekor figyelembe kell venni a huzat hatását. Az ultrahangos és a passzív infravörös érzékelők a legérzékenyebbek a huzatra. Az ultrahangos érzékelők a levegő energiaátadó képességét használják fel az érzékelés során az ultrahangos energia átvitelére (Dopper elv), melyet a légmozgások befolyásolnak. A passzív infra mozgásérzékelők reagálhatnak a huzatra, ha a huzat gyors hőmérsékleti változást okoz az érzékelő érzékenységi területén. Ez a gyors hőmérséklet-változás az érzékelőhöz közel hő-sokkot okozhat és aktiválhatja a készüléket. A huzatot a rosszul illesztett ajtók és ablakok okozhatják. A mozgásérzékelőket is – nem közvetlenül – befolyásolhatják a lazán elhelyezett tárgyak, melyek a huzatban mozognak, példa: felfüggesztett táblák, függönyök vagy növények.

C.10. Kitakarás

A mozgásérzékelők elhelyezésénél figyelembe kell venni annak a lehetőségét, hogy a berendezést (árukészletet) átrendezik, ezzel az érzékelő látóterét kitakarják. Annak a lehetőségét is figyelembe kell venni, hogy a berendezés (árukészlet) ledől, mely azonnali riasztás okozhat.

C.11. A felügyelt területek építészeti kialakítása

A felügyelt terület építészeti kialakítását figyelembe kell venni. Különös figyelmet kell szentelni a tető kialítására, továbbá a falazatokra, padozatra és a pincékre. Amikor a könnyűszerkezetű építési anyagokat használnak, különös figyelmet kell szentelni a mozgásérzékelők felszerelésére, melyet a rezgések befolyásolhatnak. Az érzékelők kiválasztásánál és elhelyezésénél figyelembe kell venni az ajtók és ablakok állapotát és illesztését, valamint a gyors hőmérsékletváltozások hatását.

C.12. Különleges megfontolások

Ahol a felügyelt területek gyúlékony, vagy robbanásveszélyes anyagokat raktároznak, vagy dolgoznak fel, különös figyelmet kell szentelni azoknak a berendezéseknek a megfelelőségére, melyeket ilyen feltételek mellett használnak, és javasolt, hogy ilyen esetben szakértő tanácsát kérjék ki. Hasonlóképpen, ha korrozív, vagy poros környezet kialakulása várható (a por kiválthatja a robbanást, ugyanolyan módon, mint a gyúlékony gőzök) megfelelő berendezések alkalmazását kell megfontolni, melyek úgy vannak tervezve, hogy a jelenlegi, vagy a várható feltételek között működni fognak.

***1. Példa**:* Olyan berendezés, mely az MSZ EN 50014 követelményeinek megfelel.
Abban az esetben, ha az érzékelők a felügyelt terület olyan felületét felügyelik, melyek célja az ezen szerkezet elleni támadás érzékelése, akkor figyelembe kell venni, hogy milyen anyagból áll ez a szerkezet, és hogy ez a szerkezet állandó e. Amikor a szerkezetben használt anyagot megváltoztatják, az érzékelők érzékenységét esetleg meg kell változtatni.

***2. Példa:** Az* érzékenységet át kell állítani, vagy más típusú érzékelőket kell használni.

Ahol az érzékelőket fóliázott (üveg) felületre szereljük, figyelembe kell venni az üveg típusát.

***3. Példa**:* A üveglap vagy edzett, vagy rétegelt – az érzékelők elhelyezése ezen típusoknak megfelelően kell, hogy történjen.
Ha az érzékelőket telepítjük, megfontolandó, hogy az üveg milyen könnyen emelhető ki a keretéből.

A páralecsapódás szintén problémákat okozhat ott, ahol az érzékelők közvetlenül a fóliázott felületre vannak helyezve, mert magas hőmérsékletemelkedés bekövetkeztekor a belső és külső felület között páralecsapódás okozhat az üveg felületén.

B.1. D függelék (információ) **Helyszíni bejárás: A behatolás- és támadásjelző rendszer működését befolyásoló tényezők a felügyelt területen kívül.**

Több tényező hat a felügyelt területen kívül (beleértve a környezeti feltételeket, melyek befolyásolhatják a behatolás- és támadásjelző rendszer teljesítményét. Ezeket a tényezőket szem előtt kell tartani, amikor a berendezés típusát és elhelyezését kiválasztjuk, különösképpen az érzékelők esetében. A felügyelt területeken kívüli tényezők általában a felhasználó ellenőrzési területén kívül esnek. Ahol ilyen feltételek negatívan befolyásolják valamely berendezés, vagy az egész behatolás- és támadásjelző rendszer működését, ezeknek a feltételeknek a hatását meg kell kísérelni megszüntetni azzal, hogy a berendezés kiválasztását és elhelyezését körültekintően végezzük. Azon feltételeket, melyek negatívan befolyásolják a behatolás- és támadásjelző rendszer működését a következőkben mutatjuk be:

D.1. Hosszú távú tényezők

A hosszú lejáratú tényezők azok, melyek várhatóan nem változnak egy jelentős időszakon belül (pl. több év alatt). Ezek a tényezők magukba foglalják pl. út, vasút, földalatti közlekedési rendszerek, légi közlekedés és gépjármű parkolás földfelszín felett és alatt. Bizonyos országokban a kisebb földrengések és rezgések lehetőségét is számba kell venni, továbbá a földsüllyedésnek/földcsuszamlás lehetőségét is.

D.2. Rövid távú tényezők

A rövid távú tényezőket is szem előtt kell tartani, különösen a felügyelt területhez kapcsolódó építkezés hatásait.

D.3. Időjárási feltételek

Szem előtt kell tartani a meglévő és potenciális időjárási feltételeket, melyek befolyásolhatják a felügyelt területet, különösen akkor, ha a terület exponált területen helyezkedik el, vagy egy tengerparti helyen, amely erős szeleknek és nagyon erős esőzésnek van kitéve. Bizonyos helyeken a terület a normálisnál több villámcsapásnak is lehet kitéve. Ezekben a körülményekben különös megfontolást igényel a megfelelő berendezés kiválasztása, a megfelelő környezeti teljesítmények jellemzőivel.

D.4. Rádiófrekvencia és interferencia

Ahol a felügyelt területek úgy helyezkednek el, hogy közel esnek a nyilvános rádióállomáshoz. Vagy TV adóantennához, polgári vagy katonai radar antennákhoz, mobil telefonrendszerek fejállomásaihoz, vészhívó szolgálatok adóantennáihoz, vagy amatőr rádió antennákhoz különleges megfontolást kíván a telepítendő berendezés EMC megfelelősége. Ha a behatolás- és támadásjelző rendszer vezeték nélküli összeköttetést használ, alaposan meg kell fontolni egy másik, a behatolás- és támadásjelző rendszer környezetében működő, feltehetően erősebb adó hatását.

D.5. Környező területek

Amikor kapcsolódó területek vannak a felügyelt terület környékén, különös megfontolás tárgyát képezi az aktivitás és eljárások, és a berendezések tekintetében, melyeket behoznak, működtetnek ezen a kapcsolódó területen. Különös gondossággal kell eljárni, ha nehéz munkagépek működnek ezeken a területeken, melyek rezgéseket okozhatnak, vagy olyan berendezések esetében, melyek magas elektromágneses interferenciát eredményezhetnek.

Példa: Hegesztő berendezés

D.6. Környezeti feltételek

Olyan berendezések alkalmazandóak, melyek alkalmasak a meglevő, vagy potenciális környezeti feltételeknek.

Példa: A hőmérséklet ingadozás (maximum/minimum), vagy levegő páratartalom

D.7. Egyéb feltételek

Abban az esetben, ha a szerkezet külső részei hozzáférhetőek a közönség számára, akkor meg kell fontolni azokat a tevékenységeket, melyek várhatóan bekövetkeznek.

Példa: Játszó gyermekek

Hasonlóképpen, ha felügyelt területek részei egy nagyobb szerkezetnek, megfontolás tárgyává kell tenni azokat a tevékenységeket, melyek várhatóan bekövetkeznek az épület kapcsolódó részein belűl.

B.1. E. függelék (információ)**: A felülvizsgálat szintjei**

A ***B.1. E.1. táblázat*** az ügyfeleknek vagy a specialistának mutat irányt a behatolás típusaival kapcsolatban, melyek a felügyelt területek különböző pontjain várhatóak. A felhasználási irányelveket arra a kockázatra kell alapozni, melyet a helyszíni bejáráson állapítottak meg, továbbá a behatolások várható módjainak megállapítása által, melyet a különböző tudás/ismeretszintű behatoltok valószínűleg használni fognak

A felügyeleti intézkedéseket az **ajánlás *A. fejezete*** – kockázati osztályba sorolás – részletesen tartalmazza.

A táblázatban bemutatott irányelv nem kimerítő listája az összes lehetséges behatolási módszernek, miután a feltételek helyszínről helyszínre változnak. Meg kell fontolni, hogy olyan behatolási módszerek elleni védelmet kell biztosítani, melyek nem szerepelnek ezen táblázatban. Hasonlóan lehetnek olyan körülmények, ahol a specialista úgy érezheti, hogy bizonyos behatolási módszerek nem vonatkoznak egészére, vagy részére a felügyelt területnek, annak ellenére, hogy ezeket az I&HAS osztályba sorolása tartalmazza, és szükségesnek minősíti.

A táblázat nem kísérli meg azt, hogy kijelölve a szakemberek számára, ahogyan tervezzék az összes behatolás- és támadásjelző rendszert egy adott biztonsági fokozaton belül, és nem is szabad ezt így tekinteni. Sok esetben a szakember el tudja érni a kívánt védelmi szintet egy adott védelmi területre úgy, hogy különböző osztályú behatolás- és támadásjelző rendszer alkotórészeket használ, így biztosítva a védelmet a különböző behatolási módszerek ellen.

B1 E.1. táblázat: a felügyelet módozatai

Megfontolások	**1. biztonsági fokozat**	**2. biztonsági fokozat**	**3. biztonsági fokozat**	**4. biztonsági fokozat**
Külső térbe nyíló ajtók	O	O	OP	OP
Ablakok		O	OP	OP
Egyéb nyílászárók		O	OP	OP
Falak				P
Mennyezetek és padozatok				P
Padlók				P
Terek	T	T	T	T
Tárgyak (magas kockázat				S
Jelmagyarázat: O = nyitásra, P = T 7 S 7 a tárgy különleges felügyeletet igényel				

B.1. F. függelék (információ) Információ a rendszer terv ajánlat (árajánlat) tartalmához

A rendszer terv ajánlatot az ügyfél vagy a behatolás- és támadásjelző rendszer specialista részére kell elkészíteni. A javaslatnak az összes információt tartalmaznia, amely ahhoz szükséges, hogy az ügyfelet, vagy a specialistát biztosítsa arról, hogy a behatolás- és támadásjelző rendszer alkalmas a felhasználásra.

A behatolás- és támadásjelző rendszer egységeire vonatkozó dokumentációnak tömörnek, teljes körűnek és egyértelműnek kell lennie.

A dokumentációnak megfelelő információt kell szolgáltatnia a telepítéshez, az üzembe helyezéshez és a behatolás- és támadásjelző rendszer egységeinek karbantartásához. Elegendő információról kell gondoskodni a behatolás- és támadásjelző rendszer részegységeinek a behatolás- és támadásjelző rendszer más egységeivel való integrálásának biztosításához.

Az átadott információknak a következőket kell tartalmaznia:

F.1. Ügyfél adatai

Név, cím, cégszerű megnevezés (amennyiben ez különbözik az ügyfélétől), illetve bármely más információ, mely biztosítja az ügyfél azonosíthatóságát.

F.2. Felügyelt területek részletezése

A felügyelt területek neve és címe

A felügyelt területek leírása

***1. Példa**:* Építmény típusa, földszintes, több emeletes

A terület hasznosítása

***2. Példa**:* Üzlet, gyár, lakás

F.3. Biztonsági fokozat

Az ajánlott behatolás- és támadásjelző rendszer biztonsági fokozata.

Az alrendszerek biztonsági fokozatai

F.4. Környezeti osztály

A minden rendszerkomponens környezeti osztálya.

F.5. Az alkalmazott eszközök listája

Az összes berendezés felsorolása, megmutatva a típust és az elhelyezést (szavakban, vagy rajzon) és nyilatkozni kell a mozgásérzékelők által várhatóan lefedett területről.

F.6. A rendszer konfiguráció

A rendszer konfigurációjának részletei.

***Példa**:* A helyszín-specifikus adatok programozása

F.7. Jelzések

A javasolt jelzőberendezések: figyelmeztető eszközök és riasztásátviteli berendezés típusa, elhelyezése, az riasztástovábbító rendszer megnevezése, vagy más távjelző központ neve, ahova a jelek átvitelre kerülnek.

F.8. Jóváhagyások

A rendszer, vagy a behatolás- és támadásjelző rendszer komponenseinek megfelelőségi tanúsítványa a helyi és nemzeti jogi előírásoknak megfelelően.

Példa: A zaj határértékre vonatkozó törvényi előírások

F.9. Szabványosítás

A rendszer, vagy a behatolás- és támadásjelző rendszer komponenseinek megfelelőségi tanúsítványa a nemzeti vagy EU szabvány előírásoknak megfelelően.

F.10. Egyéb rendelkezések

A rendszer, vagy a behatolás- és támadásjelző rendszer komponenseinek megfelelőségi tanúsítványa más előírásoknak megfelelően.

***Példa**:* Irányelvek, vagy szakmai kódok, melyeket a biztosítók , vagy a felügyeleti szervek adnak ki.

F.11. Tanúsítvány

A részegységek és a behatolás- és támadásjelző rendszer tanúsítványainak részletei.

F.12. Beavatkozás

A riasztás és hibajelekre tervezett reakció terve.

***Példa**:* Rendőrség, szolgáltató cég kulcsőrzési, beavatkozási szolgáltatása

F.13. Karbantartás

Javaslatok a behatolás- és támadásjelző rendszer vagy bizonyos rendszer-elemeinek tervszerű karbantartására. Ennek tartalmaznia kell a karbantartás gyakoriságát, és az elvégzendő munkák listáját is tartalmaznia kell karbantartásonkénti bontásban. A karbantartás alatt a behatolás- és támadásjelző rendszert le kell ellenőrizni, tesztelni és be kell állítani, hogy biztosítsuk a megfelelő működést. A behatolás- és támadásjelző rendszer karbantartása során figyelembe kell venni a ***B1 I. függelékben*** foglaltakat.

F.14. Javítás

A javasolt javítási szolgáltatások részleteit meg kall határozni, beleértve a kapcsolattartók neveit, napközbeni és 24 órás telefonszámaikat.

B.1. G. függelék (információ) **Helyszíni bejárás**

A helyszíni bejárást úgy kell végrehajtani, hogy a rendszer tervezési javaslat (árajánlat) követelményeinek meg tudjunk felelni, valamint meg tudjuk határozni a rendszer össze összetevőjének pontos elhelyezését – beleértve a vezetéke összeköttetések nyomvonalát is (ahol ezek az összeköttetőseket használjuk). A helyszíni bejáráson határozzuk meg a behatolás- és támadásjelző rendszer biztonságos működését befolyásoló tényezőit. Ezen szempontokra példákat a következőkben adunk meg:

G.1. Összeköttetések

Ezek (speciális vagy nem speciális) vezetékes, vagy vezeték nélküli technikákat alkalmazó összeköttetések lehetnek.

G.1.1. Speciális vezetékes összeköttetések

Amikor speciális vezetékes összeköttetés alkalmazunk, a következő tényezőket kell figyelembe venni.

- a kábel típusa és mérete;
- rejtetten kell-e a vezetéket szerelni;
- feszültségesés hatásai;
- a behatolás- és támadásjelző rendszer vezetékeinek elkülönítése a többi, magas feszültségű vezetéktől.
  Példa: A fővezeték, vagy azok, amelyek nagyfeszültségű jeleket továbbítanak;
- a vezetékek mechanikai védelméről gondoskodni kell;
- a szabotázs lehetőségének csökkentése érdekében a vezetékeket lehetőleg nehezen hozzáférhető módon kell vezetni;
- a vezetékeket mechanikai károsodás ellen védeni kell.
  ***Példa*:** a padlószinttől számított 2 m-en belűl;
- a nemzeti szabványokat a vezetékszerelésnél be kell tartani;
- megfelelő kötési módszereket kell alkalmazni, például csatlakozó dobozban (forrasztott vagy csavart kötést csak akkor szabad használni, ha a csatlakozó doboz alkalmazása nem praktikus);
- a csatlakozó dobozok szabotázsvédelméről gondoskodni kell (a behatolás- és támadásjelző rendszer biztonsági fokozatától függően);
- speciális vezetékek használata – ahogy azt a berendezés gyártója javasolja;
- ahol szükséges, használjunk hajlékony kábelátvezetéseket;
- a vezetékeket – ahol csak lehetséges -a felügyelt területeken belűl kell vezetni;
- ha a vezetékeket a felügyelt területen kívül kell vezetni, a vezeték megfelelő szabotázsvédelméről gondoskodni kell.

G.1.2. Nem speciális vezetékes összeköttetések

Ha nem speciális vezetékes összeköttetéseket alkalmazunk, a ***B.1. G. függelék 1.1.*** pontban felsorolt követelményeken felül a következő szempontokat kell figyelembe venni:

- bármely más jel hatását figyelembe kell venni, mely a közönséges vezetékezés miatt a behatolás- és támadásjelző rendszer működésére hatással van
- a behatolás- és támadásjelző rendszer vezetékezésével közös nyomvonalon lévő más rendszerekből eredő hibajelzés hatását figyelembe kell venni;
- a behatolás- és támadásjelző rendszer vezetékezésével közös nyomvonalon lévő más rendszerek módosításából eredő hatásokat figyelembe kell venni;

G.1.3. Vezeték nélküli összeköttetések

Amikor vezeték nélküli összeköttetéseket alkalmazunk, az alábbi tényezőket kell figyelembe venni:

- az antennák telepítését úgy kell végezni, hogy biztosítsuk a rendszer többi összetevőjével való megbízható kommunikációt;
- a behatolás- és támadásjelző rendszer ily módon összekapcsolt berendezéseinek bármilyen más RF berendezés interferencia hatását el kell kerülni;
- a berendezés antennájához közeli a kiterjedt fémtárgyak hatását figyelembe kell venni;

G.2. Érzékelőkkel kapcsolatos általános megfontolások

Függetlenül attól, hogy milyen típusú érzékelőket használunk, vannak olyan szempontok, melyeket figyelembe kell venni a helyszíni bejárás során. Ezen szempontokra példákat a következőkben adunk meg:

- az érzékelő érzékelési területén belűl lévő mozgó tárgyak;
- a behatolás- és támadásjelző rendszer élesítésekor nem lehetnek állatok az érzékelők érzékelési területén;
- az érzékelőknek a környezeti hatásoknak megfelelő kiválasztása;
- a telepítést a gyártó előírási szerint kell elvégezni;
- az érzékelőket úgy kell kiválasztani, hogy lehetőséget teremtsünk aktivizálásukkor az egyedi azonosításukra
- az érzékelők működésének ellenőrzésére teszt berendezést kell biztosítani;
- az érzékelőket úgy kell elhelyezni, hogy elmozdításukat, rongálásukat, vagy szabotázsukat nehezen lehessen végrehajtani.

G.3. A mozgásérzékelőkkel kapcsolatos általános megfontolások

Mozgásérzékelők alkalmazásakor figyelembe kell venni azokat a szempontokat melyek behatással vannak bármelyik típusú mozgásérzékelő működésére.:

- meg kell keresni az érzékelő eltakarásának megakadályozásának lehetőségének elkerülési módját;
- meg kell keresni a hatósugár területének jelentős csökkenését eredményező esetek elkerülési módját;
- olyan tartós felületre kell elhelyezni ezeket az érzékelőket, ahol a látóterület csökkentése a lehető legvalószínűtlenebb;
- ha az érzékelők nyilvános helyre vannak telepítve, biztosítani kell, hogy az érzékelő hatósugara ne terjedjen ki a felügyelt területeken kívülre;
- a biztonsági osztálynak megfelelően a járóteszt csak a teszt eljárások alatt eredményezzen kijelzést az érzékelőn

G.4. Ultrahangos mozgásérzékelők

Olyan érzékelők, melyek ultrahangos technikákat alkalmaznak, érzékenyek különleges befolyásokra, melyek példáit a következőkben mutatjuk be:

- külső (ultrahangos) zajforrások – Példa: telefon csöngés, kompresszorok, hűtőszekrények, stb.
- a szokásosnál nagyobb huzat, vagy bármilyen más légmozgás – pl. fűtő- és hűtő berendezések
- a relatív páratartalom változásai
- más ultrahangos érzékelőkkel való interferencia;
- az érzékelők felszerelési magassága, mely befolyásolhatja a működési képességeket

G.5. Mikrohullámú érzékelők

Olyan érzékelők, melyek mikrohullámú technikákat alkalmaznak, érzékenyek különleges befolyásokra, melyek példáit a következőkben mutatjuk be:

- biztosítani kell, hogy az érzékelő érzékelési területe csak a felügyelt területekre terjedjen ki;
- példa: Az épület anyaga a mikrohullámú energiát ne engedje át;
- folyadékok műanyagcsőben történő áramlása;
- más, mikrohullámú érzékelőkkel való interferencia;
- fénycsövekből eredő interferencia;
- eltorzított jelek, melyeket fém, vagy más reflektiv felületek okoznak
- mozgás, vagy rezgés
    a.) fém tárgyak az érzékelő érzékelési területén belűl – pl. fém csövek
    b.) nagy méretű fémtárgyak az érzékelési területen kívül

G.6. Passzív infra mozgásérzékelő

Olyan érzékelők, melyek passzív infra technikákat alkalmaznak, érzékenyek különleges befolyásokra, melyek példáit a következőkben mutatjuk be:

- az érzékelt területen elhelyezkedő gyors hőmérsékletváltoztatást eredményező tárgyak – pl. fűtőtestek, fűtő szerkezetek;
- huzat az érzékelő környezetében;
- közvetlen napsugárzás az érzékelő látóterében;
- hideg, vagy meleg légmozgás;
- padlófűtés;
- közvetlen fény az érzékelőre – pl. autó fényszóró, vaku;
- kombinált érzékelő elhelyezése ott, ahol referencia szint az érzékelő érzékelési zónáiban ugyanolyan hőmérsékletváltozásnak van kitéve – pl. szőnyegek és bútorok;
- rovarok, bogarak bemászásának lehetősége az érzékelőbe -pl. olyan érzékelőket használni, melyek megfelelő borítással vannak ellátva.

G.7. Kombinált érzékelők

Olyan érzékelők, melyek kettő, vagy több érzékelési technikát alkalmaznak, érzékenyek különleges befolyásokra, melyek példáit a következőkben mutatjuk be: Példa: passzív infravörös és mikrohullámú érzékelő.

Miután mindegyik érzékelési elv különböző hatásokra érzékeny, figyelembe kell venni mindent, ami az érzékelő teljesítményét befolyásolja, melyek példáit a következőkben mutatjuk be:
- minden egyes egyedi technológiára vonatkozó összes tényező;
- minden egyes technológiára legyen önálló teszt lehetőség;
- mindkét, vagy összes technológiához kapcsolódó érzékelési módszert figyelembe kell venni az együttes érzékelés megtörténtéhez.

G.8. Rezgés és testhang érzékelők

Azok a szempontok, melyeket figyelembe kell venni, a következők:
- a meglévő, állandó rezgési szint;
- az érzékelőket sima, stabil felületre kell rögzíteni;
- az anyagban létrejövő változás, vagy repedések az anyagstruktúrában, melyek a megfigyelés jellemzőit megváltoztatja;
- különböző építőanyagok használata különböző rezgési jellemzőkkel;
- olyan érzékelők kiválasztása, melyek jellemzői alkalmazhatóak az épület anyagának jellemzőihez
- a hőmérsékletváltozások hatásai – pl. az épület vagy szerkezet tágulása vagy összehúzódása, mely rezgéseket kelt a szerkezetben;
- nevesség, vagy víz bejutásának megakadályozása az érzékelőbe, valamint az üvegfelületen páralecsapódás keletkezzen;
- az érzékelő tesztelhetősége.

G.9. Üvegtörés-jelző (aktív és passzív)

Az üvegtörés-jelzők teljesítményét jelentősen befolyásolja az üveg és a ragasztó anyaga típusa. Ezekre és más tényezőkre vonatkozó példákat a következőkben ismertetünk:
- az üvegtörés-jelző csak üvegfelületre ragasztható – pl. nem polikarbonát fóliára;
- a teljesítmény csökken, ha rétegelt vagy fóliázott üvegre szerelik az érzékelőt;
- nem szabad repedt, törött vagy nem kellően rögzített üvegre telepíteni;
- bevonatos üvegre alkalmas módon kell telepíteni, különösen figyelni kell a kazettás üveg esetében
- a ragasztó anyagát a gyártó által meghatározottak szerint kell megválasztani;
- lehetőséget kell teremteni arra, hogy az üveget az érzékelő aktiválása nélkül ki lehessen venni

G.10. Akusztikus üvegtörés-jelző

A következőket kell figyelembe venni
- be kell tartani a gyártó utasításait:
  a.) fóliázás
  b.) régezett üveg
  c.) dóruveg
- az érzékelő és a felügyelet alatt álló üveg között üres térnek kell lenni – pl. az akusztikusan tompító borítások az érzékenységet csökkentik
- a nem kívánt riasztások számának csökkentése, melyeket az üvegtöréshez hasonló karakterisztikájú zajtól származnak – pl. csörgő tárgyak (kulcsok) vagy csengő
- a fel és a padló borításának hatása – pl. hangvisszaverő, kemény burkolatok, melyek hajlamosak a megfigyelt terület növelésére

G.11. Infra sorompó

A következőket kell figyelembe venni:

- ha szükséges: mechanikus behatás elleni védelem;
- csak az érzékelővel együtt szállított tükröket szabad alkalmazni;
- a több sugaras visszaverődét el kell kerülni, ha ez nem része az alkalmazásnak;
- el kell kerülni a járművek, vagy a közvetlen napsütés fényét a vevőkészülékekben;
- a fűtőkészülékek hatása a sugár útvonalára;
- elkerülendő az sugár áthatolása üvegen, vagy más áttetsző anyagon

G.12. A vezetékek folyamatosságának biztosítása

A következőket kell figyelembe venni
- a várható támadás módszerét figyelembe vevő vezetékezés kialakítása – pl. benyúlás vagy teljes hozzáférés;
- biztonságos rögzítést tervezni – megelőzendő a vezeték riasztás mentes eltávolítását, pl. csavarozás, kötegelés;
- csak olyan felületre szabad telepíteni, mely nem okoz kárt a vezetékben;
- a vezetékek elhelyezése csak a felügyelt területen belül engedélyezett;
- a környezeti feltételeket figyelembe kell venni, pl. – ne telepítsük nedves területen, felületre;
- a vétlen károkozás ellen védelmet kell biztosítani – pl. a vezetékeket védeni kell a mechanikai sérülés ellen
- olyan konfigurációt kell kialakítani, hogy észlelni lehessen a szakadást, törést, vagy rövidzárlatot;
- folyamatos felügyelet szükséges a hibák korai felderítése érdekében;
- a vezetékeket úgy kell felszerelni, hogy közben ne feszüljön meg a vezeték.

G.13. Akusztikus érzékelők

A következőket kell figyelembe venni
- el kell kerülni a zajos környezetet;
- előtérbe kell helyezni az akusztikusan „kemény” környezetet;
- használjunk kisebb területeket, ahol jobb teljesítmény várható;
- az időszakosan fellépő zajokat figyelembe kell venni – pl. telefon csengés.

G.14. A vezető fólia – általános megfontolások

A következőket kell figyelembe venni
- a fóliát olyan konfigurációba kell felhelyezni, mely a várható behatolás észlelését lehetővé teszi – pl. teljes hozzáférés, vagy kézzel történő hozzáférés
- a fóliát csak a felügyelt területen belűl szabad telepíteni;
- a hiba korai kijelzése érdekében a fólia folyamatos felügyelete szükséges;
- javítás kerülendő – vagyis ha megszakad a fólia, a teles fóliát ki kell cserélni;
- a véletlen károkozás lehetőségét figyelembe kell venni – pl. ablaktisztítás, gyermekek – ha üzletről van szó;
- a fóliahordozó anyag használhatóságát és a felhelyezés módját figyelembe kell venni;
- a várható behatolás módszerének észlelésében biztosnak kell lenni.

G.15. A vezető fólia - üvegen

A következőket kell figyelembe venni:
- lehetőséget kell teremteni arra, hogy az üveget az érzékelő aktiválása nélkül ki lehessen venni
- olyan üveget kell használni, amelyik egyértelműen törik – pl. ne használjuk rétegzett, vagy fóliázott üvegre stb;
- az üvegtörés felszerelésénél a gyártó előírásait kell követni;
- ne szereljük az üvegtörés-jelzőt sérült, vagy hibás üvegfelületre – pl. reped üvegre;
- az üvegtörés-jelzőt úgy kell telepíteni, hogy a csatlakozásoknál a páralecsapódást elkerülhető legyen;
- megfelelően tervezett összeköttetést kell használni az ablakkeret és az üvegezés között.

G.16. Tárgyvédő kontaktusok

A következőket kell figyelembe venni:
- úgy kell elhelyezni, hogy az ajtók, ablakok vagy tárgyak elmozdítását észlelje;
- a felügyelt területeken belűl kell telepíteni;
- figyelembe kell venni a tárgyhoz való hozzáférési nyílás méretét az érzékelők elhelyezésénél – pl. személy behatolás, vagy benyúlás;
- úgy kell a kontaktusokat elhelyezni, hogy ne lépjenek működésbe a védett tárgy rendeltetésszerű mozgatása közben – pl. ajtó, ablak csapkodása (huzatban)
- meg kell fontolni a biztonságot, vagy a megbízhatóságot befolyásolhatják:
  a.) fémszerkezetre szerelt mágneskapcsolók – pl. használjunk nemfémes rögzítő elemeket;
  b.) olyan pozícióba kell telepíteni, ahol a kapcsolóhoz nem lehet könnyen hozzáférni – pl. vékony fémcsíkot használni, hogy a működtető elemet visszatartsuk
  c.) oda kell telepíteni, ahol a kapcsolót nem lehet szándékosan aktiválni – pl. a kiállított tárgy alatt;
  d.) biztosítani kell, hogy a kapcsoló fixen legyen rögzítve.
- A kontaktusok kiválasztásánál figyelembe kell venni a működés közbeni környezeti hatásokat – pl. vízhatlan kontaktusok a redőnyökön.

G.17. Kapacitív érzékelő

A következőket kell figyelembe venni
- stabil környezetbe kell telepíteni, pl. a kapacitív érzékelő a padozat és a védett tárgy között nem lehet kitéve gyors változásoknak;
- a közeli fémtárgyak hatását figyelembe kell venni;
- a megfigyelés területének a felügyelt tárgyra kell, hogy korlátozódjon.

G.18. Taposó kontaktus

A következőket kell figyelembe venni
- telepítésnél kerüljük el a nagy forgalmú területeket;
- a taposó kontaktusokat rejtetten kell telepíteni;
- megfontolandó: nyitott, vagy zárt felügyelet legyen-e
- megfontolandó a cserére való alkalmasság – pl. amikor padlószőnyeg alá vannak helyezve;
- a veszélyes környezeti feltételeket el kell kerülni – pl. párásodás, nedvesség kicsapódás;
- az összeköttetés módszerei – pl. a vezeték típusa diszkrét, de erős legyen.

G.19. Feszítő huzal

A következőket kell figyelembe venni
- a hőmérséklet és páratartalom változása;
- a felügyelt területen belűl kell telepíteni;
- olyan konfigurációba kell telepíteni, hogy a várható behatolás módszerét érzékelje.

G.20. Kezelő- és kijelző készülékek és áramellátásuk

A következőket kell figyelembe venni
- a nyilvánosság által hozzáfért területeket el kell kerülni;
- a felügyelt területen belüli telepítést úgy kell elvégezni, hogy könnyen legen karbantartható;
- telepítésükkor el kell kerülni azokat kültéri falakat- melyek nem kellően szilárdak;
- hiba és riasztás azonosítás céljaira megfelelő kijelzéseket kell tartalmaznia;
- a belépési és kilépési eljárásokat úgy kell megtervezni, hogy a nem kívánt riasztások számát minimalizáljuk;
- az eseménynapló kapacitásának meg kell felelnie a behatolás- és támadásjelző rendszer méretének és bonyolultságának,
  Megjegyzés: MSZ EN 50131-1 szabvány tartalmazza az eseménynaplózás követelményeit.
- megfelelő teszt feltételeket kell biztosítani a behatolás- és támadásjelző rendszer használói és karbantartóinak;
- a nagyméretű behatolás- és támadásjelző rendszer rendszereknél megfelelő teszt módszereket kell biztosítani – ahol sok érzékelő helyezkedik el egy nagy épületen belűl;
- biztosítani kell annak képességét, hogy megerősítse - az érzékelőteszt és a tesztet követő -, a megfelelő érzékelő működést;
- az áramellátást a felügyelt területen belülről a fő tápellátásról kell biztosítani;
- áramellátása kizárólag a behatolás- és támadásjelző rendszerből történhet;
- a behatolás- és támadásjelző rendszerhez az áramellátás csatlakoztatása a következőképp történjen:
- a fő tápegységbe történő bekötés egy külön biztosított pontról történjen (a 3. és 4. biztonsági fokozatú behatolás- és támadásjelző rendszernél);
- a fő tápegységre történő kapcsolódás közvetlenül történjen a behatolás- és támadásjelző rendszerhez (csak az 1. és 2. biztonsági fokozatú behatolás- és támadásjelző rendszernél)
- az áramellátó berendezést megfelelő szelőzéssel kell ellátni.

G.21. Kisegítő vezérlő berendezések

A következőket kell figyelembe venni
- olyan elhelyezést kell választani, ami a működtetést megkönnyíti;
- úgy kell elhelyezni, hogy a vezérlő berendezés kezelését idegen személyek ne tudják megfigyelni, hacsak az nincs letakarva.
- Ha külső falra szerelik, a környezeti feltételeket figyelembe kell venni

G.22. A nem szándékolt működtetés megelőzése

A következőket kell figyelembe venni
- előriasztó figyelmeztetést kell alkalmazni, ha a behatolás- és támadásjelző rendszert a belépési folyamat közben aktiválták;
- egyszemélyi felelősnek kell lennie – céges, vagy egyéni – a behatolás- és támadásjelző rendszer működtetésére, ha a behatolás- és támadásjelző rendszert olyan épületbe telepítették, ahol több felhasználó van;
- ha a behatolás- és támadásjelző rendszer részben élesítése történik, előriasztás figyelmeztetést kell kiváltania az élesítési vagy hatástalanítási folyamat alatti aktiválásnak.
- a vezérlő- és kijelző berendezés hozzáférhetőségét korlátozni kell olyan személyek számára, akik megfelelően ki vannak oktatva, és kompetensek annak kezelésére, mert ez befolyásolhatja a behatolás- és támadásjelző rendszer működését;
- a felügyelt terület nem szándékos hozzáférését meg kell akadályozni a rendszer élesített állapotában;
- *Példa*: a felügyelt területek összes ajtaját mechanikusan zárni kell, ha a behatolás- és támadásjelző rendszer élesítve van.
- A belépési és kilépési eljárás során a kijelölt ajtón való belépés megfontolás tárgyát képezi.

G.23. Riasztásátviteli rendszerek

A következőket kell figyelembe venni
- az átviteli vezetékezést a lehetőség szerint el kell rejteni;
- a riasztási jel átvitelét meggátolni képes tényezőket át kell gondolni – pl. a vállalati telefonközpont;
- felügyelni kell a helyi riasztásátviteli útvonalának rendelkezésre állását – pl. felügyelni a tárcsahangot;
- módszereket kell biztosítani a bejövő hívások által megakadályozott üzenet átviteleket, amikor a riasztásátviteli berendezés a postai vonalakhoz kapcsolódik. Javasolt külön telefonvonal biztosítása;
- az átviteli úton található dugaszolós csatlakozók véletlen kihúzását meg kell akadályozni – pl. egy telefon csatlakozó, mely reteszeléssel rendelkezik;
- ha az átviteli út légvezetéken keresztül vezet, a villámvédelemről gondoskodni kell;
- a riasztásátviteli berendezést a felügyelt területeken belűl, rejtetten kell telepíteni.

G.24. Külső jelzőberendezések

A következőket kell figyelembe venni
- feltűnő helyen kell felszerelni;
- a felhatalmazott személyzet részére működtethetőnek kell lennie a nélkül, hogy nyilvánosság előtt a hang- és fény hatását csökkentenénk;
- úgy kell elhelyezni, hogy a véletlen vagy szándékos károkozás valószínűségét minimalizáljuk;
- úgy kell elhelyezni, hogy a karbantartónak biztosítva legyen a megfelelő hozzáférés;
- a megfelelő szintű szabotázsvédelem érdekében a külső kábelezést el kell rejteni;
- ha két figyelmeztető eszköz kerül telepítésre és egyidejű támadás várható ellenük, a két figyelmeztető eszközt olyan messze kell egymástól telepíteni, amennyire csak lehetséges;
- az épületszerkezetre kell elhelyezni.

G.25. Belső jelzőberendezések

A következőket kell figyelembe venni
- a vezérlő- és kijelző berendezés vagy kiegészítő vezérlő- és kijelző berendezés való közelsége (a behatolás- és támadásjelző rendszer 3. és 4. biztonsági fokozatánál).
  Példa: a figyelmeztető eszközt nem szabad közvetlenül a vezérlő- és kijelző berendezés vagy kiegészítő vezérlő- és kijelző berendezés mellé telepíteni;
- olyan helyzetbe kell telepíteni a felügyelt területen belűl, mely nem teszi lehetővé a hallásának- és látásának csökkenését;

G. 26. Külső kulcsszéf

A következőket kell figyelembe venni
- felügyelet nyitás és a kulcs kivétele szempontjából
- a külső vezetékezést el kell rejteni, vagy biztosítani kell a megfelelő szabotázsvédelmi szintet.

B 1. H függelék (információ) **Eseménynapló**

A következőben egy példát mutatunk be, az eseménynapló formájára.

Például: A riasztási feltételek (akár valós, akár nem kívánt), hibák, tesztek, átmeneti lekapcsolások és javítási munkák bejegyzésére szolgál.

Bármilyen tevékenységgel kapcsolatban rövid megjegyzést kell tenni, mely elmagyarázza, hogy milyen munkát végeztek el, és milyen munkák vannak még hátra.

Alapadatok:

Név és Cím: ……..

……..

Felelős személy: …….. dátum …….

……...dátum …….

……...dátum …….

I&HAS telepítője ……...dátum …….

I&HAS karbantartója ……... dátum …….

…….

Ellenőr ……...dátum …….

…….

Hiba esetén értesítendő: ……... Tel: …….

Esemény adatai:

Dátum	Idő	Esemény	Kívánt intézkedés	Teljesítés időpontja	Aláírás

Cserélendő berendezésrészek
……..
……..
……..

A csere aktuális ideje
…….
……..
……...

B.1. I. függelék (információ) **Karbantartás**

I.1. Karbantartás – berendezés

A berendezés karbantartását a gyártó rendelkezései szerint kell végrehajtani.

I.2. Karbantartás – behatolás- és támadásjelző rendszer

A karbantartásnak (bevizsgálás és teszt) a következőket kell tartalmaznia:

- szabotázs érzékelés
- élesítés, hatástalanítás
- belépés és kilépési eljárások,
- tápellátás és áramkörök vizsgálata
- érzékelők működése
- a jelzőberendezések működése
- ATE működése

A berendezés visszaállítására a karbantartást követően kiemelt figyelmet kell fordítani.

B.1. J. függelék (információ) **Folyamatábra**

Az alábbi folyamatábra ezen **ajánlásban** leírtak fő eljárásait mutatja be. Ezen a folyamatábrán az eljárások egymás alatt vannak bemutatva, a gyakorlatban némelyik eljárások ugyanabban az időpontban zajlanak le. A folyamatábra azt a dokumentációt is leírja, melyet minden egyes eljárás eredményez