MAGYAR BIZTOSÍTÓK SZÖVETSÉGE

BIZTONSÁGTECHNIKAI ÚTMUTATÓ A BETÖRÉSES LOPÁS-RABLÁSBIZTOSÍTÁSI KOCKÁZATOK KEZELÉSÉRE

(AJÁNLÁS)

B.3. fejezet:

Távfelügyeleti rendszer követelmények

kiadás	A dokumentum megnevezése	kiadva	visszavonva
0	Távfelügyeleti rendszer követelmények	2007.01.19.	2007.09.30.
1	Távfelügyeleti rendszer követelmények	2007.10.01.	

Tartalomjegyzék

I. rész: Riasztásátviteli rendszerekkel szemben támasztott követelmények

1. Riasztásátviteli rendszerekkel és részegységeivel szemben támasztott követelmények

1.1. Bevezetés

Ez az **ajánlás** az épületekben és épületek közelében telepített riasztásátviteli rendszerekre és részegységeikre határoz meg követelményeket.

A riasztásátviteli rendszerek a védett létesítménybe telepített vagyonvédelmi (tűzjelző-, gázveszély-jelző- behatolásjelző-, támadásjelző-, segélyhívó-, beléptető- és videofelügyeleti stb.) rendszerek jelzéseinek felügyeleti helyre történő átvitelére szolgálnak.

Ez a fejezet a teljes átviteli út, valamint a jelzés fogadására, kezelésére és feldolgozására szolgáló felügyeleti központtal kapcsolatban fogalmaz meg követelményeket.

A riasztásátviteli rendszer valamely része (pl. automatikus híváskezdeményező egység interfésze) egy vagyonvédelmi technikai védelmi rendszer részét képezi, ennek a résznek az átvinni kívánt jelet adó rendszer(ek)re vonatkozó szabványok és ennek az **ajánlásnak** a követelményeit is ki kell elégítenie.

A riasztásátviteli rendszer követelményeit összefoglaló **ajánlás** az alábbiakat tartalmazza:

- biztonságtechnikai alkalmazásra szánt beléptetőrendszerek felépítését és általános követelmények;
- funkciókra vonatkozó követelmények;
- riasztásátviteli rendszer és részegységeinek az elektromágneses összeférhetőségi követelmények;
- riasztásátviteli rendszer más eszközökkel való kommunikációjára vonatkozó követelményeket (pl. riasztórendszerrel).
- az átviteli út berendezéseinek külső (légköri és egyéb eredetű) túlfeszültségek elleni védelem követelményei,

A megfelelőség követelményeit az **ajánlás** a **riasztásátviteli rendszerekre** és a **riasztásfogadó központokra** külön pontokban tárgyalja.

1.2. A riasztásátviteli rendszerekkel szemben támasztott követelmények

Ez az **ajánlás** a riasztásátviteli rendszerek működőképességére, megbízhatóságára és biztonsági jellemzőire vonatkozó általános követelményeket határozza meg.

Az **ajánlás** tartalmazza a riasztórendszer és a riasztásfogadó központ közötti jelzésátvitelt biztosító összeköttetésekre vonatkozó általános követelményeket.

Az **MSZ EN 50130**-as szabványsorozat a riasztó rendszerekkel szemben támasztott követelményei, illetve ennek **MSZ EN 50136** szabványsorozata valamennyi típusú riasztás átvitelére érvényes (tűzjelző, behatolásjelző, beléptető és segélyhívó riasztórendszerek stb.) riasztásaira. A különböző típusú riasztórendszerek a riasztási üzeneten kívül küldhetnek más típusú üzeneteket is, pl. hibaüzeneteket és állapotüzeneteket. Ezeket az üzeneteket is a riasztásátvitel részének tekintjük. Az **ajánlásban** a riasztás kifejezést ebben a széles értelemben használjuk.

A riasztásátviteli rendszerekre vonatkozó **EU direktívák** a következők:

73/23/EEC (LVD)	Electrical safety
89/336/EEC (EMC)	Emission Immunity
92/58/EEC	Safety and/or health signs at work

1.2.1. Szabványoknak való megfelelés

A riasztásátviteli rendszerek és részegségeik feleljenek meg az **MSZ EN 50133** szabványsorozat követelményeinek.

A riasztásátviteli rendszerekben alkalmazott eszközök, a belőlük kialakított rendszer (bele értve a kábelek telepítését is) feleljenek meg az alábbi szabványok követelményeinek:

Általános követelmények:

- MSZ 2364 szabványsorozat;
- MSZ EN 50131 szabványsorozat;
- MSZ EN 50164;
- MSZ EN 62305-4;
- MSZ IEC 1312-1;
- MSZ 274 szabványsorozat;
- MSZ EN 50130 szabvány sorozat;

Hivatkozott szabványok:

Kiadás	**Év**	**Cím**
EN 50082-1		Elektromágneses összeférhetőség. Általános zavartűrési szabvány. 1. rész: Lakóhelyi, kereskedelmi és kisipari környezet
EN 50131-1		Riasztórendszerek. Behatolásjelző rendszerek
EN 50136-1-1		Riasztórendszerek. Riasztásátviteli rendszerek és berendezések. 1-1. rész: Riasztásátviteli rendszerek általános követelményei
EN 50136-4		4. rész: Riasztásmegjelenítő berendezések
EN 55022		Informatikai berendezések. Rádiózavar-jellemzők. Határértékek és mérési módszerek (CISPR 22)
EN 60065	1993	Háztartási és hasonló általános célú hálózati elektronikus készülékek és velük összekapcsolt készülékek biztonsági előírásai (IEC 65:1985+A1:1987+A2:1989+A3:1992, módosítva)
EN 60950		Információtechnológiai berendezések biztonsága (IEC 60950 módosítva)
IEC 60068-1		Környezetállósági vizsgálatok. 1. rész: Általános előírások és irányelvek
IEC 60068-2-1 +IEC 60068-2-1A +A1	1974 1976 1983	2. rész: Vizsgálatok. A vizsgálat: Hideg
IEC 60068-2-2 +IEC 60068-2-2A	1974 1976	2. rész: Vizsgálatok. B vizsgálat: Száraz-meleg
IEC 60068-2-3	1969	2. rész: Vizsgálatok. Ca vizsgálat: Nedves meleg, állandósult állapot
IEC 60068-2-6	1982	2. rész: Vizsgálatok. Fc vizsgálat: Szinuszos rázás
IEC60068-2-27	1987	2. rész: Vizsgálatok. Ea vizsgálat és irányelvek: Ütés
IEC 60068-2-30 +A1	1980 1985	2. rész: Vizsgálatok. Db vizsgálat és irányelvek: Ciklikus nedves meleg (12 + 12 órás ciklus)
IEC 60068-2-42	1982	2. rész: Vizsgálatok. Kc vizsgálat: Érintkezők és csatlakozások kéndioxidos vizsgálata
IEC 60068-2-52	1984	2. rész: Vizsgálatok. Kb vizsgálat: Ciklikus sós köd (nátrium-klorid-oldat)
IEC 60068-2-56	1988	2. rész: Vizsgálatok. Cb vizsgálat: Nedves meleg, állandósult állapot, elsődlegesen berendezésekre
IEC 60068-2-63	1991	2. rész: Vizsgálati módszerek. Eg vizsgálat: Ütés rugós kalapáccsal
IEC 60364	sorozat	Épületek villamos berendezéseinek létesítése
IEC 60529		Burkolatok által nyújtott védettségi fokozatok (IP -kód)
IEC 60664	sorozat	Kisfeszültségű rendszerek villamos szerkezeteinek szigeteléskoordinációja
IEC 61000-4-2	1995	Elektromágneses összeférhetőség (EMC). 4. rész: Vizsgálati és mérési módszerek. 2. főfejezet: Elektrosztatikus kisüléssel szembeni zavartűrési vizsgálat
IEC 61000-*4-3*	1995	3. főfejezet: Sugárzott, rádiófrekvenciás elektromágneses térrel szembeni zavartűrési vizsgálat
IEC 61000-4-4	1995	4. főfejezet: Gyors villamos tranziens/burst jelenséggel szembeni zavartűrési vizsgálat
CCITT V24-es ajánlása		
CCITT V23-as ajánlása		
CCITT V31-es ajánlása		
CCITT X24-es ajánlása		

Ahol nyilvános hálózatokat használnak, ott az **ETSI** vonatkozó európai távközlési szabványait (ETS, European Telecommunication Standards) és a **CCITT, CCIR** és **CEPT** ajánlásait kell alkalmazni.

Ahol lehetséges, az **ISO** nyílt rendszerek összekapcsolására vonatkozó, (OSI, Open System Interconnection) rétegszerkezetű modelljére vonatkozó műszaki követelményeknek való megfelelésre vonatkozóan nyilatkozni kell.

Ahol lehetséges, a berendezések és rendszerek teljesítsék azokat a helyi, nemzeti és európai követelményeket, szabályokat, amelyek a nyilvános távbeszélő- és adathálózatokhoz való csatlakozásra (ideértve a PSTN-t), az ilyen hálózatokon keresztüli kapcsolatlétesítésre és annak befejezésére, valamint az átvitelre vonatkoznak, és/vagy azokat a szabályokat, amelyek a rádiórendszerek, az energiaelosztó-rendszerek vagy a kábeltelevíziós elosztórendszerek használatával megvalósuló átvitelre vonatkoznak.

Megjegyzés 1: Évszám nélküli hivatkozásoknál a hivatkozott kiadvány legutolsó kiadását kell alkalmazni (módosításokkal együtt)

Megjegyzés 2: A hatályos szabványok katalógusa az **ajánlás *A.1 függelékben*** találhatóak

Megjegyzés 3: A megfelelőséget a termék dokumentációhoz csatolt megfelelőségi tanúsítványokkal kell igazolni.

Megjegyzés 4: A megfelelőség-tanúsítványok hiánya esetén a vizsgálatoknak a nem tanúsított szabvány követelményeknek a gyártmánydokumentáció alapján végzett termékvizsgálatokkal is meg lehet az ajánlás követelményeinek felelni.

1.2.2. Rendszertechnikai követelmények

Az **ajánlás** riasztásátviteli rendszerekkel kapcsolatos megfelelőséget az **1.2.1. pont** alatti szabványok általános követelményeinek való megfelelés alapján állapítja meg.

A termék és rendszer kockázati osztályokba sorolása – ahol a vonatkozó szabványok az **ajánlás A. fejezete MSZ EN 50131 szabvány** szerinti **biztonsági fokozatba** sorolás szempontjából nem kellően részletes – döntően az **MSZ EN 50136 szabvány**sorozat műszaki követelményei és a kárstatisztikák, kriminalisztikai tapasztalatok alapján történik.

Az általános rendszertechnikai követelményeket az **MSZ EN 50136** szabványsorozat követelményeivel megegyezők.

A B.3. fejezet szerinti megfelelőségi vizsgálatok alapján **kockázati** osztályba sorolt riasztásátviteli rendszerekre és részegységeire a **MABISZ** csak abban az esetben ajánlja a tagbiztosítóinak, hogy az ily módon besorolt rendszer-elemekből összeállított **rendszert a kárkockázat** szempontjából kockázat csökkentő szempontként figyelembe venni, ha a rendszer maradéktalanul megfelel az **MSZ EN 50130**-as szabvány sorozat, de különösen az **MSZ EN 50136** Riasztórendszerek. Riasztásátviteli rendszerek és berendezések szabványsorozat rendszerekre vonatkozó megbízhatósági és működési követelményeinek.

1.2.3. Kockázati osztályba sorolás

A rendszertechnikai követelmények alapján a szerint sorolja az **ajánlás** az egyes riasztásátviteli termékeket kockázati osztályokba.

A riasztásátviteli rendszerek és részegységeinek kockázati osztályba sorolását a ***B.3. 01. táblázat*** tartalmazza.

Megjegyzés 1: A ***kockázati osztályok*** ill. a ***biztonsági fokozatok*** részletesen az **ajánlás „A" fejezetében** találhatóak.

Megjegyzés 2: Az **ajánlásban** hivatkozott azon szabványok melyek angol nyelven lettek közzé téve, magyar nyelvű kivonatos, nem hivatalos fordításai az ***A.2. függelékben*** találhatóak.

Megjegyzés 3: Az **ajánlásban** található **szakkifejezések** és rövidítések jelentése az ***A.3. függelékben*** találhatóak.

1.2.4. Átviteli jellemzők

A riasztórendszer állapotának átvitele megvalósítható:

1. folytonosan, vagy
2. időszakosan, és/vagy
3. valahányszor a rendszer állapota megváltozik.

Ha az átvitel nem folytonos, az átvitelt vezérelje:

1. a riasztórendszer, és/vagy
2. a riasztásfogadó központ, és/vagy
3. a riasztásátviteli rendszer.

1.2.5. A riasztásátviteli rendszerek kockázati osztályba sorolása

A riasztásátviteli rendszerek kockázati osztályba sorolását az alábbi paraméterek alapján történik:

- az átviteli idő (B3/1. táblázat);
- a leghosszabb idő (B3/2. táblázat);
- a jelentési idő (B3/3. táblázat);
- a rendelkezésre állás (B3/4. táblázat)

A riasztásátviteli rendszerkövetelményeket a jelzésátviteli biztonságra az ***MSZ EN 50136-1-1*** szabvány *6.5. szakasza*, a távolról történő paramétermódosításra az ***MSZ EN 50136-2-1*** szabvány *5.2.3.1. szakasza*, a jogosultsági szintekre az ***MSZ EN 50136-2-1*** szabvány szerinti követelmények vonatkoznak.

B.3. 01. táblázat: Az átviteli idő szerinti osztályozás

	Átviteli idő, másodperc				
Osztály	**D0**	**D1**	**D2**	**D3**	**D4**
Az összes átvitel számtani középértéke	-	120	60	20	10
Az összes átvitel 95 %-a	240	240	80	30	15

B.3. 02. táblázat: Legnagyobb átviteli idő értékek szerinti osztályozás

	Átviteli idő, legfeljebb, másodperc				
Osztály	**M0**	**M1**	**M2**	**M3**	**M4**
A leghosszabb elfogadható átviteli idő	-	480	120	60	20

B.3. 03. táblázat: Jelentési idő szerinti osztályozás

	Jelentési idő					
Osztály	**T1**	**T2**	**T3**	**T4**	**T5**	**T6**
Legnagyobb időtartam	32 nap	25 óra	300 perc	180 s	90 s	20 s

B.3. 04. táblázat: A rendelkezésre állás szerinti osztályozás

	Rendelkezésre állás				
Osztály	**A0**	**A1**	**A2**	**A3**	**A4**
A teljes rendszer rendelkezésre-állása bármely 12 hónapos időszakban	nincs követelmény	97 %	99,3 %	99,5 %	99,8 %
Havi rendelkezésre-állás	nincs követelmény	75 %	91 %	95%	98,5 %

A riasztórendszer és a riasztásfogadó központ közötti kommunikáció folyamatosan feleljen meg a ***B.3. 01. táblázat*** megfelelő osztálya követelményeinek, miközben ugyanazon a riasztásátviteli rendszeren egyéb szokványos üzenetek átvitele is folyik.

A riasztásátviteli rendszer olyan legyen, hogy egy újabb riasztórendszer hozzáadása, egy riasztórendszer paramétereinek megváltoztatása vagy egy riasztórendszer eltávolítása ne veszélyeztesse a többi riasztórendszertől származó üzeneteket.

A riasztórendszer és a riasztásfogadó központ közötti kommunikáció folyamatosan feleljen meg a ***B.3. 01. táblázat*** megfelelő átviteli idő szerinti osztályára és a ***B.3. 02. táblázat*** legnagyobb átviteli idő szerinti osztályára vonatkozó követelményeknek, ha a riasztási vagy hibaüzenetek keletkezési üteme:

A riasztások átviteli idejének számtani középértéke és a mért átviteli idők 95%-ának értéke ne haladja meg a ***B.3. 01. táblázat*** a megfelelő osztályra megadott értékeket, az ***MSZ EN 50136-2-1*** *szabvány 7.4. szakaszban* leírt ellenőrzési módszer szerint értékelve.

Egy adott rendszerre a ***B.3. 02. táblázat*** meghatározott, elfogadható legnagyobb átviteli időt meghaladó átviteli időt az ***MSZ EN 50136-2-1*** *szabvány 6.4.3. szakasznak* megfelelően az átviteli rendszer hibájának kell minősíteni.

A riasztórendszer és a riasztásátviteli rendszer közötti összeköttetés hibája esetén riasztást vagy hibaüzenetet kell létrehozni és továbbítani a riasztásfogadó központhoz. Az összes átvitt üzenetre vonatkozó átviteli idő számtani középértéke, illetve az átvitt üzenetek 95%-ának átviteli ideje ne haladja meg a ***B.3. 01. táblázat*** a meg- felelő osztályra megadott értéket.

Bármely esemény, amely üzeneteket generál és továbbít, legnagyobb átviteli ideje ne haladja meg a ***B.3. 02. táblázat*** a megfelelő osztályra megadott értéket.

Automatikus ellenőrzéssel rendelkező rendszerek esetében a riasztásátviteli rendszerben a hiba keletkezésétől a hibainformációnak a riasztásfogadó központhoz, illetve az ellenőrzőközponthoz történő jelentéséig eltelt idő ne haladja meg a ***B.3. 03. táblázat*** a megfelelő osztályra megadott értéket.

Ahol az elvárt rendelkezésre állási osztály követelményeinek teljesítése érdekében járulékos átviteli utakra vagy berendezésekre van szükség, az elsődleges és a járulékos átviteli utakat és berendezéseket is ellenőrizni kell.

Minden hibát annyi időn belül kell jelenteni, ami nem haladja meg a ***B.3. 03. táblázat*** a megfelelő osztályra megadott értéket, még akkor is, ha a redundancia miatt a szolgáltatás nem szűnik meg.

Az idő alatt, amikor egy redundáns átviteli utat elsődlegesen nem riasztásátvitelre használnak (készenléti idő), annak jelentési idő szerinti osztálya eltérhet az elsődleges átviteli útra vonatkozótól.

A riasztásátviteli rendszer elsődleges átviteli útjain vagy berendezéseiben fellépő rövid idejű hibákat akkor nem kell jelenteni, ha az ***MSZ EN 50136-2-1*** szabvány *6.3.2.* szakasz szerinti követelmény még teljesül.

A riasztásátviteli rendszer redundáns átviteli útjain vagy berendezéseiben fellépő rövid idejű hibákat akkor nem kell jelenteni, ha az ***MSZ EN 50136-2-1*** szabvány *6.3.2.* szakasz szerinti követelmény teljesült volna valamennyi lehetséges átviteli út vagy berendezés előzetes meghibásodása esetén.

A „rövid időtartam véges értékét” a riasztásátviteli rendszer üzemeltetőjének kell meghatároznia, hogy lehetővé tegye a rendelkezésre állás szempontjából való értékelést.

1.2.5.1. Helyettesítéssel szembeni biztonság

A riasztásátviteli rendszerhez kapcsolódó felügyelt objektumok adó-vevőjének hasonló berendezéssel való illetéktelen helyettesítése elleni védelemről a következő módszerek egyikével kell gondoskodni (az ***MSZ EN 50136-2-1*** szabvány szerint*).*

- **S0** Nincs intézkedés.
- **S1** Intézkedés a felügyelt objektumok adó-vevője helyettesítésének észlelésére a riasztásátviteli úton továbbított valamennyi üzenetben egy azonosító vagy a cím hozzáadása révén.
- **S2** Intézkedés a felügyelt objektumok adó-vevője helyettesítésének észlelésére a következő módon:
  - **a)** titkosított azonosító vagy cím elküldése a riasztásátviteli úton átvitt valamennyi üzenetben, vagy
  - **b)** a felügyelt objektumok adó-vevőjének hitelesítése különféle és fedett kóddal minden egyes csatlakoztatott adó-vevő esetén, vagy
  - **c)** más, a gyártó által megadott intézkedés.

A hitelesítés mindig elegendő számú kulcsot tesz szükségessé azért, hogy minden egyes csatlakoztatott adó- vevőt egyedi kóddal lehessen ellátni.

Az **S2** kategóriában az azonosítási tartomány legalább 250 egyedi címből álljon.

1.2.5.2. Információbiztonság

A riasztásátviteli rendszer által továbbított információ védelméről a következő módszerek egyikével kell gondoskodni (az ***MSZ EN 50136-2-1*** szabvány szerint*).*

- **I0** Nincs intézkedés.
- **I1** Intézkedés az átvitt információ illetéktelen olvasásának megakadályozására.
  MEGJEGYZÉS: Ez titkosítással érhető el.
- **I2** Intézkedés az átvitt információ illetéktelen módosításának megakadályozására.
  MEGJEGYZÉS: Ez titkosítással vagy kriptográfiai hitelesítési módszerrel érhető el.
- **I3** Intézkedés az átvitt információ illetéktelen olvasásának és illetéktelen módosításának megakadályozására.

A titkosítási algoritmusoknak olyannak kell lenniük, hogy szinkron riasztásátviteli rendszerek esetén tetszőleges egymást követő 100 bit adatmintázata ne ismétlődjön 10 000 000 egymást követő bitben, vagy aszinkron átviteli rendszerek esetén tetszőleges egymást követő 100 byte adatmintázata ne ismétlődjön 1 000 000 egymást követő byte-on belül.

1.2.5.3. Átviteli idő

Az átviteli időt attól az időponttól kell számítani, amikor a felügyelt objektumhoz rendelt adó-vevő riasztórendszer felőli interfészénél az állapotváltozás bekövetkezik, addig az időpontig, amikor az új állapot jelentése megjelenik a felügyeleti központ adó-vevője riasztásmegjelenítő berendezés felőli interfészénél.

Az átviteli idő minden olyan állapotváltozásra vonatkozik, amelynek átvitele a riasztórendszertől a felügyelt objektumhoz rendelt adó-vevő riasztásátviteli rendszer felőli interfészén át végbemegy.

A riasztórendszer és a riasztásfogadó központ közötti kommunikáció folyamatosan feleljen meg a ***B.3. 01. táblázat*** megfelelő átviteli idő szerinti osztályára és a B3/*2. táblázat* legnagyobb átviteli idő szerinti osztályára vonatkozó követelményeknek, ha a riasztási vagy hibaüzenetek keletkezési üteme:

a) a rendszer kapacitásának legfeljebb 0,1%-át kitevő számú, felügyelt objektumban telepített adó-vevőktől percenként egy üzenet, és

b) legalább percenként 2 riasztásüzenet a felügyeleti központ adó-vevője riasztásmegjelenítő berendezés felőli interfészénél.

Az értékelést akkor kell elvégezni, amikor a riasztásátviteli rendszer stabil állapotban van az előírt üzenetgyakoriság mellett.

A riasztásátviteli rendszerre telepített minden egyes új riasztórendszer esetén ellenőrizni kell a riasztási üzenetek helyes átvitelét és megérkezését a rendeltetési végállomásra, és ahol megtehető, ott a rendszerellenőrzéssel kapcsolatos riasztási vagy hibaüzenetek átvitelét is. Egy riasztási üzenet (pl. egy tesztriasztási üzenet) átvitele által igénybevett időnek összhangban kell lennie az ***MSZ EN 50136-2-1*** *szabvány* 6.3.2. szakaszával.

Az ellenőrzést biztosító rendszerek esetén az az időtartam, amely a felügyelt objektumoktól a riasztásfogadó központig terjedő átviteli út hibájából eredő hibafeltételnek a felismerésére és átvitelére lett igénybe véve, legyen összhangban az ***MSZ EN 50136-2-1*** *szabvány* 6.3.4. szakasszal.

Azt a rutinellenőrzést, amely kiterjed a riasztási és a hibaüzenetek időzítésére, minden egyes csatlakoztatott riasztórendszer vonatkozásában legalább évente egyszer, vagy pedig a riasztórendszer szabályos szervizelési időközének megfelelően meg kell ismételni, ha ez utóbbi időköz hosszabb.

Ha a riasztásátviteli rendszer képes eltérő prioritású vagy időzítésű különféle üzenetek átvitelére, az ellenőrzést minden egyes kategóriára külön-külön kell végrehajtani. Ilyen esetekben az eredményeket minden összetevő csoportra meg kell határozni.

Ha a riasztási üzenetek átviteli gyakorisága a rendszeren keresztül előre látható módon változik az idő függvényében, vagy ha a riasztásátviteli rendszerrel közösen használt berendezések más szolgáltatás általi igénybevétele az idővel változik (pl. nyilvános kapcsolt távbeszélő-hálózatot használó rendszerek esetében), akkor a működőképesség-ellenőrzés időeloszlásának tükröznie kell azt az időelosztást, amelynek megfelelően a tényleges üzenetek a nap vagy a hét során várhatóan előfordulnak.

Az ellenőrzés eredményeit minden csatlakoztatott riasztórendszer esetén elemezni kell a riasztásátviteli rendszer szempontjából egymást követő három hónapos periódusokban. Ez nem jelenti azt, hogy minden csatlakoztatott rendszert aktiválni és vizsgálni kell minden három hónapos periódusban.

1.2.5.4 Rendelkezésre állás

Az **ajánlás *B.3. 04. táblázat*** megadott értékek meghatározásához a vizsgálatokat az alábbi mérési módszerrel állapítjuk meg rendelkezésre állási osztályonként:

A1. Egy vagy több hiba 11 napnál kevesebb összes időtartammal, valamennyi csatlakoztatott riasztórendszerre átlagolva, de nem több mint 7 nap valamennyi csatlakoztatott riasztórendszerre bármelyik hónapban átlagolva.
Példa: 2 olyan hiba az év során, amely minden csatlakoztatott riasztórendszerre hatással van, és mindegyik 5-5 napot vesz igénybe az azonosításra és a kijavításra; vagy egyetlen olyan hiba, amely egész éven át tart, de a csatlakoztatott riasztórendszereknek csak 3%-ára van hatással.

A2. Egy vagy több hiba 25 napnál kevesebb eredő időtartammal, valamennyi csatlakoztatott riasztórendszerre átlagolva.
Példa: egy olyan rendszer esetén, amelyhez 7 riasztórendszer van csatlakoztatva egyetlen főáramkörön keresztül, és abból egynél, 1 napig tartó hiba van jelen a fő áramkörön, plusz 3 napig tartó hibák két egyedileg csatlakoztatott rendszerben. Ezek eredőjének ezen osztály értékein belül kell maradnia.

A3. Egy vagy több hiba 44 óránál kevesebb eredő időtartammal, valamennyi csatlakoztatott riasztórendszerre átlagolva.

Ezt kielégíti egy olyan rendszer, amelyben átlagosan csak egy hiba fordul, elő csatlakoztatott riasztórendszerenként évente, és a hibák azonosítása és kijavítása a következő munkanap végéig megtörténik.

A4. Egy vagy több hiba 17 óránál kevesebb eredő időtartammal, valamennyi csatlakoztatott riasztórendszerre átlagolva.

A hibák statisztikai feldolgozásához az ***MSZ EN 50136-1-1*** *szabvány 7.5.3. szakaszának* módszere nyújt segítséget.

1.2.5.5. Feljegyzések:

Minden hibáról és a riasztásátviteli rendszeren elvégzett minden működőképesség-ellenőrzésről feljegyzést kell vezetni.

Feljegyzést kell vezetni minden rendszerhibáról, ideértve azokat is, amelyek redundáns útvonalakat vagy berendezéseket érintenek, ahol ezekre szükség van a megadott rendelkezésre állási osztálynak való megfeleléshez, és akkor is, ha a szolgáltatás teljesült.

A feljegyzésnek minden hiba esetén tartalmaznia kell:
a) a hiba azonosításának dátumát és idejét;
b) a hibát megelőző utolsó olyan dátumot és időpontot, amikor a hiba még biztosan nem létezett;
c) valamennyi hiba időtartamát;
d) azoknak a csatlakoztatott riasztórendszereknek a számát, amelyek szolgáltatását a hiba befolyásolta.

A feljegyzéseket legalább két évig meg kell őrizni.

1.2.5.6. A feljegyzés ellenőrzése

A feljegyzések álljanak rendelkezésre a biztosító képviselője által végzett ellenőrzés céljára.

Legyen lehetséges nyomon követni az egyedi rendszerhiba befoglalását az olyan összesített adatok közé, amelyekre szükség van az ***MSZ EN 50136-2-1*** szabványnak való megfeleléshez, és legyen lehetséges visszavezetni a nyilvánosságra hozott működőképességi adatokat az egyedi működőképesség-ellenőrzésekre vagy -hibákra.

1.3. A riasztásátviteli úttal kapcsolatos követelmények

A riasztórendszer és a riasztásfogadó központ közötti kommunikáció folyamatosan feleljen meg a ***B.3. 01. táblázat*** megfelelő osztálya követelményeinek, miközben ugyanazon a riasztásátviteli rendszeren egyéb szokványos üzenetek átvitele is folyik / folyhat.

A riasztásátviteli rendszer olyan legyen, hogy egy újabb riasztórendszer hozzáadása, egy riasztórendszer paramétereinek megváltoztatása vagy egy riasztórendszer eltávolítása ne veszélyeztesse a többi riasztórendszertől származó üzeneteket.

A nem riasztórendszerekkel közösen használt átviteli szolgáltatások biztosítsák, hogy a nem riasztórendszerek működése és karbantartása ne hiúsítsa meg a riasztásátviteli rendszer az e szabvány szerinti követelményeknek való megfelelőségét.
MEGJEGYZÉS: Kapcsolt hálózatok esetében az előbbiek a kapcsolat létrejötte utáni állapotra vonatkoznak.

Ha a felügyelt objektumoknál vagy a riasztásfogadó központnál a riasztásátviteli rendszerhez több interfész kapcsolódik, a riasztásátviteli rendszert akkor kell rendelkezésre állónak tekinteni egy vagy több interfészt érintő hiba esetén, ha:
a) legalább egy riasztásátviteli út rendelkezésre áll a riasztórendszer egy interfésze és a riasztásfogadó központ egy interfésze között, és ha
b) az üzenetek adása és vétele ezen interfészeken előírás szerinti, vagy
az üzenetek adása és vétele az egyik elsődleges interfész mindkét oldalán előírás szerint történik, de hiba esetén a rendszer automatikusan átvált a redundáns interfészre.

Legyen lehetőség megbizonyosodni arról, hogy minden egyes riasztási üzenet helyesen jutott el a riasztásfogadó központ berendezéseihez. Ez megoldható például a távoli központnál lévő felügyeleti központ adó-vevőjétől érkező nyugtázóüzenettel.

A rendszer rendelkezésre állását az előforduló hibák / meghibásodások alapvetően befolyásolják, ezért az alábbi hibákat súlyozottan kell figyelembe venni:
a) riasztásátviteli rendszerben fellépő minden olyan hiba, amely meggátolja egy riasztási üzenet átvitelét bármelyik engedélyezett riasztórendszertől a hozzá tartozó felügyeleti központhoz (még akkor is, ha a riasztási üzenetet sikerül átirányítani egy alternatív felügyeleti központhoz).
MEGJEGYZÉS: A felügyeleti központ adó-vevője és a riasztásmegjelenítő berendezés közötti foglaltsági kapcsolatok nem képeznek riasztásátviteli rendszerhibákat.
b) Minden olyan hiba, amely megakadályozza egy riasztási üzenetnek az átvitelét úgy, hogy az átvitt információ részben vagy teljesen elvész (kivéve, ha az információ a riasztási üzenet automatikus újra átvitele révén visszanyerhető, biztosítva, hogy a ***B.3. 02. táblázat*** a megfelelő osztályra megadott legnagyobb elfogadható átviteli időn belül a riasztási üzenet vétele megtörténjék).
c) Minden olyan hiba, amely úgy késleltet egy riasztási üzenetet, hogy a teljes átviteli ideje meghaladja a ***B.3. 02. táblázat*** megadott legnagyobb elfogadható átviteli időt.
d) Karbantartás miatti kiesést, hacsak alternatív berendezésekről nem gondoskodnak.

A riasztásátviteli rendszert úgy kell tekinteni, mint ami nem áll rendelkezésre, amíg bármelyik fenti feltétel fennáll.

A hiba időtartamának értelmezése:

Hibaidőtartamnak tekintjük azt az időszakot, amely alatt a riasztásátviteli rendszert úgy kell tekinteni, mint ami nem áll rendelkezésre, vagyis, amely attól az utolsó időponttól, amikor a rendszerről ismeretes volt, hogy rendelkezésre állt (vagyis hibátlan volt) addig az időpontig tart, ameddig a hibát észlelték, kijavították, és a rendszert megvizsgálták. Minden egyes hiba esetén a rendelkezésre állás kiesését legalább 15 percnek kell venni.
MEGJEGYZÉS: A rendszer veszélyeztetésére irányuló szándékos kísérletek miatti hibák nem számítanak, feltéve, hogy a 3. táblázatban a megfelelő osztályra meghatározott időn belül észlelésük és jelentésük megtörtént.

A riasztási üzenet elvesztése ellen a riasztásfogadó központ adó-vevője által fogadott üzeneteket biztosítani kell (pl. a felügyeleti központ adó-vevőjénél vagy a riasztásmegjelenítő készüléknél).

A gyártónak a dokumentációjában nyilatkoznia kell, hogy a felügyeleti központ adó-vevőjét a riasztásmegjelenítő berendezéshez kell-e vagy sem kapcsolni, hogy teljesüljön ez a követelmény.

Ha az átviteli hálózatot több riasztórendszert kiszolgáló riasztásátviteli rendszer közös részeként használnak, a működőképesség ellenőrzését a hálózat kezdeti telepítése után és nagyobb bővítéseit követően is végre kell hajtani annak biztosítására, hogy a hálózat valamennyi részének ellenőrzése hatékony legyen, és hiba észlelése esetén a riasztási vagy hibaüzenetek létrehozása és sikeres átvitele megtörténjék.

A működőképesség ellenőrzése:

Egy riasztásátviteli rendszer működőképességének ellenőrzése terjedjen ki a következőkben felsorolt szempontokra:

a) Annak vizsgálata, hogy egy megfelelően létrehozott riasztási bemenetet a riasztásátviteli rendszer elfogad-e.
   MEGJEGYZÉS: A felügyelt objektumok riasztórendszer felőli interfészének vizsgálatát az MSZ EN 50136-2-1 részletezi.
b) Annak vizsgálata, hogy a hibaüzenetek eljutnak a rendszeren keresztül a rendeltetési végállomáshoz,
c) A riasztás átviteli idejének ellenőrzése.
d) Minden olyan járulékos, szabványossági- vagy rutinellenőrzés, amely szükséges a rendszer rendelkezésre állásának megállapításához vagy annak megerősítéséhez.

A működőképesség ellenőrzésének igazolnia kell, hogy a rendszer kiépítése és a várható számban csatlakoztatott riasztórendszerek esetén a riasztásátviteli rendszer képes az **MSZ EN 5016-1** *szabvány 6.1. szakasza* szerinti követelményeknek teljesítésére. Ezt a következő eljárások valamelyikével kell elvégezni:

- az üzembe helyezett rendszer gyakorlati működőképességének ellenőrzésével, vagy
- a berendezés tesztelésével és vizsgálatával, amikor benyújtják azt az **MSZ EN 50136-2-1** szerinti vizsgálatra, vagy
- a berendezések és összeállításuk elemzésével, vagy
- ezek kombinációjával.

A működőképesség számszerű meghatározásához az ***MSZ EN 50136-1*** *szabvány 7.5.3. szakasza* ad támpontot.

1.3.1. Bérelt (dedikált) riasztási útvonalakat használó rendszerek követelményei

A riasztásátviteli rendszerek használhatnak vezetékes összeköttetéseket (pl. egyenfeszültségű vagy modulált jel csavart érpárú kábelen át), beszédátviteli összeköttetéseket vagy adatátviteli összeköttetéseket, és tartalmazhatnak multiplexereket vagy üzenet-feldolgozó processzorokat.

Az **ajánlás** olyan riasztásátviteli rendszerekre is alkalmazható, amelyekben a jelzésátviteli összeköttetéseket más szolgáltatásokkal megosztva használják.

Ilyen szolgáltatások lehetnek a szokásos előfizetői telefonvonal a felügyelt objektumtól a helyi távbeszélőközpontig, a kábeltévé vagy az energiaelosztó-hálózatok, de az **ajánlás** ugyanígy alkalmazható más, hasonló rendszerek esetében is.

A több felhasználó által használt átviteli úttal szemben támasztott megszorító kikötések:

Ha egy riasztórendszertől érkező átviteli úton keletkező hibák vagy szándékos zavarás nem befolyásolhatják más riasztórendszertől jövő átviteli utak működőképességét, akkor a csatlakoztatható átviteli utak teljes számát a rendszerrendelkezésre állásával szembeni követelmények korlátozzák.

Ha egy átviteli úton keletkező hibák vagy szándékos zavarás befolyásolhatják a többi út működőképességét, és meggátolják, hogy azok teljesítsék ezen **ajánlás** követelményeit, akkor a csatlakoztatható átviteli utak teljes számát az alkalmazás és a biztonsági követelmények korlátozzák, és azt meg kell adni a rendszer ismertetőjében.

1.3.2. Megosztott jelzésátviteli összeköttetések telefonvonalak használatával

A riasztórendszer átviteli összeköttetését úgy kell megosztani a szokásos telefonvonallal, hogy mind a beszéd, mind pedig a riasztórendszer információja egyidejűleg átvihető legyen.
A helyi telefonközpontban a riasztórendszer információját el kell választani a beszédcsatornától, és a riasztásfogadó vagy az ellenőrzőközponthoz kell továbbítani, közvetlenül vagy közbenső feldolgozás után.
Példa: A vonal megosztható, például frekvencia- vagy időmegosztási módszerrel, vagy pedig egy ISDN-vonal D csatornájának használatával.

1.3.3. Megosztott jelzésátviteli összeköttetések kábeltévé-elosztóhálózatok használatával

A riasztórendszer átviteli összeköttetését úgy kell megosztani a kábeltévé elosztóhálózatával, hogy a hálózaton mind a TV-jelek, mind a riasztórendszer információja egyidejűleg átvihető legyen.

Az elosztóhálózat valamely pontján a riasztórendszer információját el kell választani a TV-jelektől, és a riasztásfogadó vagy egy ellenőrzőközponthoz kell továbbítani, közvetlenül vagy közbenső feldolgozás után.

1.3.4 Megosztott jelzésátviteli összeköttetések energiaelosztó-rendszerek használatával

A riasztórendszer átviteli összeköttetését úgy kell megosztani a helyi energiaelosztó-rendszerrel, hogy a hálózaton mind az energia, mind a riasztórendszer információja egyidejűleg átvihető legyen.

Az elosztóhálózat valamely pontján a riasztórendszer információját le kell választani a tápvonalakról, és egy riasztásfogadó vagy egy ellenőrzőközponthoz kell továbbítani, közvetlenül vagy közbenső feldolgozás után.

1.3.5. Nyilvános, kapcsolt távbeszélő-hálózatot használó, digitális kommunikátoros rendszerek követelményei

Ez a pont olyan kapcsolt összeköttetésekre vonatkozik, amelyek eseményvezérelt jelzés átvitelét biztosítják a riasztórendszer és egy távfelügyeleti központ között. Az információ digitalizált jelek formájában kerül átvitelre a távfelügyeleti központokban lévő automata fogadóközpont adó-vevői felé.

A távfelügyeleti központ általában egy riasztásfogadó központ, de lehet olyan, riasztástovábbításra szolgáló távfelügyeleti központ is, amely az **MSZ *EN 50136-1-2*** követelményeinek megfelelő riasztásátviteli rendszert használ.

Az átviteli útnak meg kell felelnie az ***ETS 300 001*** általános műszaki követelményeinek.

Ahol az átviteli út nem kizárólagosan a riasztásátviteli rendszerhez tartozik, és az átviteli út egy tényleges fizikai vonal, a következő követelményt kell teljesíteni:

Ne lehessen a hívást letiltani vagy a riasztás átvitelét zavarni egy másik olyan rendszer alkalmazásával, amely ugyanazt az átviteli utat használja.

Ha a helyi kapcsolóközpont és a riasztásfogadó központ között az átviteli út egy telefonvonal, akkor ezt a telefonvonalat kizárólagosan erre a célra kell használni és állandó felügyelet alatt kell tartani.

A beérkező átviteli utak számát úgy kell meghatározni, hogy a várható forgalmi terhelés mellett a felügyeleti központ adó-vevőjének rendelkezésre állási valószínűsége a beérkező riasztási hívások számára nagyobb legyen, mint 98%, csúcsterhelés mellett egy órás időtartamon keresztül mérve.

Ezen feltétel meglétét a szolgáltatónak szerződésben kell garantálnia, vagy (naponta mérni és regisztrálni kell három hónapon át, kivéve a meghibásodás, karbantartás vagy kivételes működési feltételek esetét) statisztikai mérésekkel kell igazolni.

1.3.6. Nyilvános, kapcsolt távbeszélő-hálózatot használó, beszédkommunikátoros rendszerekkel szemben támasztott követelmények

Ezek a követelmények olyan kapcsolt összeköttetésekre vonatkoznak, amelyek esemény vezérelt jelzés átvitelét biztosítják egy riasztórendszer és egy távfelügyeleti központ között. Az információ átvitele egy vagy több felelős személyhez és/vagy egy riasztásfogadó központhoz tárolt hangüzenetek formájában történik.

A nyilvános, kapcsolt távbeszélő-hálózaton (PSTN -en) keresztül megvalósuló kapcsolás létesítésének lehetősége a hálózatnak az esemény bekövetkeztekor fennálló állapotától függ. A sikeres hangátvitel valószínűségének növelése érdekében a beszédkommunikátornak több kísérletet kell végrehajtania a felelős személy vagy az alternatív fogadóközpontok felhívására és jelentéstételre.

A kapcsolat megvalósítása és az üzenet átvitelének módja szerint három kapcsolati formát különböztet meg az **ajánlás**, melyeket a ***B.3. 05. táblázat*** tartalmaz.

B.3. 05. táblázat:

Rendszer típus	1-es típus	2-es típus	3-as típus
Működési követelmények (ha létrejön a hívás:)	megtörténik az üzenet egyszeri vagy többszöri átvitele, majd a hívás befejeződik, de a hangüzenet helyes vételének nyugtázása nem történik meg	megtörténik az üzenet egyszeri vagy többszöri átvitele, majd a hívás befejeződik. A felelős személynek vagy a riasztásfogadó központnak meg kell erősítenie az üzenet helyes vételét a felügyelt objektumok megadott időn belüli visszahívásával. Ha visszahívás nem érkezik, a hívási ciklus megismétlődik	a felelős személynek vagy a riasztásfogadó központnak nyugtázó jelet kell küldenie a felügyelt objektumokba. Ha ez a jel nem érkezik meg, a felügyelt objektumok adóvevője lebont, és megismétli a hívási ciklust.

Ha az átviteli útvonal a PSTN első kapcsolóközpontjához vezető telefonvonal, úgy az megosztható más olyan rendszerekkel, amelyek megfelelnek az **ETS 300 001** követelményeinek

Ha az átviteli útvonal nem tartozik kizárólagosan a riasztásátviteli rendszerhez, ne legyen lehetséges a hívás letiltása vagy a riasztás átvitelének zavarása egy másik olyan rendszer alkalmazásával, amely ugyanazt az átviteli utat használja.

Ha a riasztórendszer adó-vevője külön dobozban van elhelyezve és nem közvetlenül a kapcsolódó riasztórendszer vezérlő- és jelzőberendezései mellett helyezik el, akkor az adóvevőnek olyan saját tápellátást ás tartalék akkumulátort kell tartalmaznia, amelynek készenléti ideje egyenlő a kapcsolódó riasztórendszer készenléti idejével, valamint elegendő többlet- kapacitással rendelkezik ahhoz, hogy biztosítsa az adó-vevő működését legalább két - leghosszabb időtartamú - adatátviteli ciklus időtartamára.

2. A riasztásfogadó központokkal szemben támasztott követelmények

A rendszerközpont minden részegysége rendelkezzen párhuzamosan működő melegtartalékkal, amely meghibásodás esetén képes legfeljebb egy közlemény kihagyásával automatikusan átvenni a meghibásodott részegység funkcióit.

A rendszerközpont összes berendezése rendelkezzen 24 órás autonóm üzemet biztosító szünetmentes táplálással.

2.1. Biztosított üzenetek a riasztástovábbítási rendszerben

A riasztási üzenet elvesztése ellen a riasztásfogadó központ adó-vevője által fogadott üzeneteket biztosítani kell (pl. a felügyeleti központ adó-vevőjénél vagy a riasztásmegjelenítő készüléknél).

A gyártónak ki kell jelenteni a dokumentációban, hogy a felügyeleti központ adó-vevőjét a riasztásmegjelenítő berendezéshez kell-e vagy sem kapcsolni, hogy teljesüljön ez a követelmény.

2.2. Átviteli jellemzők

A riasztórendszer állapotának átvitele folyamatosan, periodikusan és/vagy valahányszor a riasztórendszer állapota megváltozik történhet:
Ha az átvitel nem folyamatos, az átvitelt vezérelje: a riasztórendszert és/vagy a riasztásfogadó központot és/vagy a riasztásátviteli rendszert.

2.3. Funkcionális követelmények

2.3.1. Hozzáférési szintek

A riasztásfogadó központnak (és amennyiben szoftver vezérelt a riasztástovábbító rendszer, akkor annak minden elemének) legalább három hozzáférési szintje legyen:

1. szint Korlátozás nélküli
2. szint Felhasználói
3. szint Konfigurálási

1. hozzáférési szint

A hozzáférés nincs korlátozva. Az 1. szint olyan feliratokhoz, fényjelzésekhez stb. használatosak, amelyek közvetlenül láthatóak. A berendezés élesítése vagy hatástalanítása, továbbá a konfiguráció változtatása nem engedélyezett.

2. hozzáférési szint

A 2. hozzáférési szint a felhasználói szint, ahol engedélyezett az üzemi állapot módosítása (a rendszer konfigurációjának megváltoztatása nélkül).

A hozzáférést kulccsal, kódkapcsolóval vagy zárral, illetve más egyenértékű módon kell korlátozni.

3. hozzáférési szint

A 3. hozzáférési szint hozzáférést engedélyez a rendszer konfigurációját érintő valamennyi művelethez.

A hozzáférést kulccsal, szerszámmal, kódkapcsolóval vagy zárral kell korlátozni. A 3. szintű hozzáférés lehetővé teszi a 2. szintű hozzáférést.

A hozzáférést a távoli központhoz be kell jelenteni, mielőtt a módosítások hatályba lépnek.

2.3.2. Szoftvert alkalmazó berendezések

Ha egy berendezésben szoftvert használnak, akkor e szoftvertől független megfigyelőeszköznek (pl. egy „watchdog” eszköznek) kell biztosítania a program hibátlan végrehajtását. A program hibás végrehajtása esetén hibajelzést kell generálni.

2.3.3. Konfigurációs paraméter módosítása

A konfigurációs paraméterek módosítása az 2.3.1. pont szerinti 3. hozzáférési szinten legyen engedélyezett.

Ha a paraméterek módosítását egy távoli központból engedélyezik, akkor a módosításra szolgáló riasztásátviteli útvonalat a felügyelt objektumnál a 3. hozzáférési szinthez kell rendelni.

2.3.4. A paraméterek kiolvasása

A beállított paraméterek kiolvasását lehetővé kell tenni. A kiolvasás azon a hozzáférési szinten szükséges és megengedett, amelyen a módosítás elvégezhető.

2.3.5. A paraméterek tárolása

Ha a riasztórendszer adó-vevőjében és/vagy a riasztásfogadó központban különféle paramétereket tárolnak (pl. hívószámokat, kódkulcsokat, eseményeket stb.), a működtető tápegység kiesését követően legalább hat hónapos időtartamig gondoskodni kell e paraméterek biztonságos tárolásáról.

Ha energiatárolásra külön eszközt használnak (pl. akkumulátort), akkor ennek az eszköznek a cseréjét a 3. hozzáférési szinten kell elvégezni.

A tápellátásra, az alkalmazott akkumulátorok tárolókapacitására vonatkozó követelmények az **MSZ EN 50131-6** *szabvány* – megfelelő biztonsági fokozatára vonatkozó - előírásainak feleljenek meg.

Ha a riasztórendszer adó-vevőjének paramétereit távolról lehet konfigurálni, az adó-vevőnél legyen lehetőség a távoli paramétermódosítás manuális letiltására és engedélyezésére a 3. hozzáférési szinten.

2.3.6. Az átvitel vizsgálata

A 2. vagy a 3. hozzáférési szinten legyen lehetőség a felügyelt objektum adó-vevőjétől vizsgálati célú üzenet manuális küldésére, annak feldolgozására és kiértékelésére a távoli központban.

2.3.7. A felügyelt objektumban lévő adó-vevő függetlensége és tápellátása

A felügyelt objektumok adó-vevője táplálható a riasztórendszer tápegységéről vagy külön tápegységről. Ha külön tápegységet használnak, akkor annak meg kell felelnie a hozzá tartozó riasztórendszerek teljesítményre vonatkozó követelményei közül a legszigorúbbnak.

A felügyelt objektumban lévő adó-vevő tápellátásának teljes megszűnése előtt üzenet küldéséről kell gondoskodni a riasztásfogadó központba, hacsak a tápellátás kiesése nem azonnali (pl. zárlat miatt).

2.3.8. Nyugtázójel

A riasztásátvitel visszaigazolása megvalósítható nyugtázójellel, lásd az **MSZ EN 50136-1-1** *szabvány 6.4.2. szakaszát*.

Nyugtázójel alkalmazása esetén azt az időpontot, amikor a nyugtázójel generálódik, a termék műszaki ismertetőjében meg kell adni.

2.3.9. A riasztásjelentés megszakítása

Lehetőséget kell biztosítani a riasztási üzenet jelentési folyamatának megszakítására – riasztórendszertől függően a 2. vagy 3. hozzáférési szinten – az alatt az időtartam alatt, mielőtt még a kommunikációs kapcsolat létrejön.

2.3.10. Burkolat és szabotázsvédelem

Ha a felügyelt objektum adó-vevője külön burkolatban van, a riasztásátviteli berendezés szabotázsvédelmére és burkolatára vonatkozó követelmények azonosak vagy szigorúbbak legyenek, mint a kapcsolódó riasztórendszer berendezéseire vonatkozóak.

Ha egy riasztásátviteli adó-vevőre más követelményt nem adnak meg, alapkövetelményként teljesítenie kell az **MSZ EN 60529** *szabványban* megadott IP3X védettségi fokozatra vonatkozó követelményeket. Ha interfész- és/vagy protokollillesztő egység szükséges és ez az egység külön burkolatban van, akkor arra is teljesülnie kell fenti követelményeknek.

2.3.11. Tápegység a riasztásfogadó központban

A riasztásfogadó központ adó-vevőjének tápegysége ugyanazoknak a követelményeknek feleljen meg, mint amelyeket az **MSZ EN 50136-4** *szabvány* határoz meg a kapcsolódó riasztásmegjelenítő berendezésre.

2.3.12. Átviteli idő

A felügyelt objektum adó-vevőjének átviteli idejét attól kezdve kell mérni, hogy a felügyelt objektum adó-vevője riasztórendszer felőli interfészének az állapota megváltozott.

***Megjegyzés*:** Ahol ez nem hozzáférhető (pl. ha a felügyelt objektum adó-vevője egybeépített a vezérlő- és kijelzőberendezéssel), vagy ha célszerűbb, az átviteli idő mérhető a vezérlő- és kijelzőberendezés állapotának észlelhető változásától vagy attól az időponttól, amikor egy, a vezérlő- és kijelzőberendezéshez csatlakoztatott egyszerű kapcsoló vagy érzékelő működésbe lép

Átviteli időnek nevezzük azt az időtartamot, amely alatt a felügyelt objektum adó-vevőjének riasztórendszer felőli interfészén megjelenő, az új állapotról szóló jelentés elküldése az átviteli hálózat felé megtörténik.

Megjegyzés: Ahol ez nem hozzáférhető, vagy ha célszerűbb, az átviteli idő mérhető addig az időpontig, amíg az új állapot jelentése a felügyelt objektum adó-vevőjének az átviteli hálózat felőli interfészén megjelenik.

Bármelyik módszert is használják, azt meg kell adni a termék műszaki leírásában, és ennek megfelelően kell vizsgálni.

Az átviteli idő a vezérlő- és kijelzőberendezés valamennyi továbbított állapotváltozására vonatkozik.

A riasztórendszeren és a riasztásmegjelenítő berendezésen belüli átviteli időket a gyártónak a gyártmány dokumentációban meg kell adnia – ennek hiányában ezeket az értékeket méréssel kell megállapítani és dokumentálni.

2.3.13. Interfészek általános követelményei

A gyártónak meg kell adnia, hogy milyen interfészekkel látta el a riasztórendszer adó-vevőjét.

Ezek lehetnek gyártóspecifikus vagy nyilvánosan elérhető interfészek, vagy valamelyik az **MSZ EN 50136-2-1** *szabvány 5.12. szakaszában* megadott követelményeknek megfelelő interfész.

2.3.14. A felügyelt objektum adó-vevőjének a riasztórendszer felőli interfésze épségének felügyelete

A felügyelet módszerével és az esetleges korlátozásokkal kapcsolatos részleteket a termék műszaki leírásában kell megadni.

A riasztórendszer és a riasztásátviteli berendezés közötti kapcsolat hibája esetén riasztási vagy hibaüzenetet kell létrehozni és azt a riasztásfogadó központba kell továbbítani.

A jelzés észlelésének és elküldésének idejére vonatkozó követelményeket a felügyelt objektum adó-vevőjére kell megadni.

Az **MSZ EN 50136-1-1** *szabvány 6.3.4. szakaszában* meghatározott időtartamot a gyártónak kell megadnia.

Párhuzamos interfész alkalmazása esetén a riasztórendszer valamennyi alapállapotban (nincs riasztás) lévő kimenetén a felügyelt objektum adó- vevőjének figyelnie kell a riasztórendszerrel való összeköttetéseket.
Bármely vezeték zárlata vagy szakadása esetén, ami megakadályozná a riasztórendszertől származó riasztási üzenet átvitelét, 10 másodpercen belül riasztási vagy hibaállapotot kell létrehozni.

Soros adatinterfész alkalmazása esetén felügyelt objektum adó-vevője riasztórendszer felőli interfészének épségét folyamatos felügyelet alatt kell tartani, és a riasztási vagy hibaüzenetet 10 másodpercen belül kell létrehozni.

2.3.15. A riasztásfogadó központ adó-vevőjének a riasztásmegjelenítő berendezés felőli interfésze épségének felügyelete

A felügyelet módszerével és az esetleges korlátozásokkal kapcsolatos részleteket a termék műszaki leírásában meg kell adni.

Párhuzamos interfész: a felügyeletének ki kell terjednie az összeköttetésnek a hibájának észlelésére is.

Soros adatinterfész: az interfészt felügyelni kell.

2.3.16. A riasztásátviteli rendszeren belüli egyéb interfészek épségének felügyelete

A riasztórendszerek és a riasztásmegjelenítő berendezések felé szolgáló interfészeken túl, egyes riasztásátviteli berendezéseknek lehet interfésze más berendezések felé is.

Ilyen interfészek esetén a felügyelet módszerével és az esetleges korlátozásokkal kapcsolatos részleteket a termék műszaki leírásában meg kell adni.

2.3.17. Üzenetbiztosítás

A riasztásátviteli rendszeren továbbított üzeneteket a riasztásfogadó központ adó-vevőjének kell biztosítania.
Ha a riasztásfogadó központ adó-vevője egy riasztásmegjelenítő berendezéshez van kapcsolva, a riasztásfogadó központ adó-vevőjének nem kell biztosítania az üzeneteket.
Ebben az esetben a riasztásfogadó központ adó-vevője csak akkor nyugtázhatja az üzenet vételét, miután megkapta a nyugtázást a riasztásmegjelenítő berendezéstől.

2.3.18. Események tárolása, dokumentálása

A rendszerközpont vezérlő egysége időponttal ellátva folyamatosan naplózza, archiválja (szükség szerint nyomatassa) a következőket:

- a beérkező biztonsági információkat;
- a kezelő által tett intézkedéseket;
- a vezérlő egység be- és kikapcsolását;
- a jelzésfogadó központi egységbe való kezelői be- és kijelentkezéseket;
- az eseménytárhoz történő hozzáférési kísérleteket;
- az eltárolt adatok archiválásának megtörténtét;
- az eseménytár törlésének tényét;
- az adatbázis megváltoztatását, az eseménytár adataihoz való hozzáférést;

Az eseménytár 80 %-os telítettségének állapotát a központnak a kezelő felé jeleznie kell.

Az eseménytár csak az archiválás megtörténte után legyen törölhető.

Az eseménytár törlését csak a rendszergazda végezheti el.

3. Közös követelmények

3.1. Önvédelem

Ne lehessen jogosulatlan személy részére szerszámok használata nélkül a riasztásátviteli rendszerek részegységeinek belső részeihez hozzáférnie.

A riasztásátviteli rendszerek rendszer szabotázs elleni védelme az **ajánlás B.1. fejezet:**– megfelelő kockázati osztályra vonatkozó előírásinak feleljen meg.

3.2. Programozottság-védelem

Biztonságos megoldás álljon rendelkezésre a riasztásátviteli rendszerek és részegységeinek az előre meghatározott szabályok jogosulatlan módosításának megakadályozására.

Az **MSZ EN 50130**-*as szabványsorozat* követelményei szerint ez egynél több jelszó használatával valósítható meg.

A különböző lehetséges kódok száma és a jogosult személyek száma közti arány legalább 1000 az 1-hez legyen.

A kódváltozatok kockázati osztályokhoz rendelt minimális számát a ***B.3. 06. táblázat*** tartalmazza.

B.3. 06. táblázat

	1. biztonsági fokozat	2. biztonsági fokozat	3. biztonsági fokozat	4. biztonsági fokozat
a különböző kódváltozatok száma	10 000	100 000	1.000 000	1.000 000*
* Csak rendszergazdának legyen lehetősége ezeknek a jelszavaknak a megváltoztatására				

3.3. „Halott ember” funkció alkalmazása

Az úgynevezett „halott ember” funkciót a riasztásfogadó központokban a kezelő rendelkezésre állásának a felügyelésére kell alkalmazni - aki a jelzésadó berendezés által szolgáltatott információ feldolgozásával van megbízva. Ezt a funkciót a jelzésadó berendezésbe lehet beprogramozni:

- azon leghosszabb idő beprogramozásával, ami alatt a kezelő nem végez tevékenységet; vagy
- ha ez az idő letelt, helyi információ keltésével vagy riasztás-kijelzés aktiválásával vagy egy másodlagos riasztásfogadó központba (pl. a területileg illetékes rendőrség) riasztás küldésével.

3.4. Üzemeltetés

A riasztásátviteli rendszer minden elemét szervezetten és rendszeresen karban kell tartani-

Minden felügyelt elektronikus biztonsági rendszer rendelkezzen központi azonosítási lehetőséggel.

A távfelügyeleti rendszerközpont legyen képes a felügyelt elektronikus biztonsági rendszerek 10 %-ától egyidejűleg érkező riasztásjelzések fogadására és lekezelésére.

A rendszer kezelése grafikus felületen billentyűzettel és egérrel történjen.

A rendszerközpont biztosítsa szöveges és grafikus formában az üzemi- és a rendkívüli események kijelzését a következő esetekben:
- riasztás- és szabotázsjelzések a felügyelt biztonsági elektronikus rendszerekben és az átviteli úton;
- hibajelzés a felügyelt biztonsági elektronikus rendszerekben és az átviteli úton.
- a rendkívüli események okozta állapotváltozások megszűnése, az eredeti állapot visszaállása.
- a felügyelt biztonsági elektronikus rendszerek üzemi állapotait és az azokban bekövetkező változásokat.
- objektumvédelmi rendszereknél a védett objektum szintenkénti helyiség részletességű alaprajzát, a telepített érzékelőket és más rendszerelemeket valamint azok állapotát;
- riasztásátviteli rendszereknél a riasztásjelzés helyének pontos meghatározását és a helyszínvázlatot;
- a kamerák által a rendszerközpontba továbbított képeket (amennyiben van képátviteli funkció);
- a személyzet részére kialakított kezelői felületet.
- A normál, a hiba, és a rendkívüli esemény színmegjelenítése egymástól eltérő legyen.
- A rendszerközpont vezérlő egysége - egyidejű hangjelzéssel - vizuálisan jelenítse meg a beérkező riasztás- és hibajelzéseket. A hangjelzés a vétel nyugtázásával szűnjön meg. A riasztás jelzés megszüntetési funkciója (törlése) kezelői kóddal legyen hozzáférhető.
- A rendszerközpont vezérlő egysége rendelkezzen olyan intézkedéstámogató rendszerrel, amely - adatbázisát felhasználva - megjeleníti a veszélyeztetett objektum szükséges adatait, a szükséges beavatkozásokat, rögzítési lehetőséget biztosít a kezelő részre a végrehajtással kapcsolatos intézkedéseinek dokumentálására és megőrzésére.

4. Megfelelőségi vizsgálatok és követelmények

4.1. Általános műszaki, rendszertechnikai vizsgálatok és követelmények

Az **ajánlás** előírásainak általános megfelelőségének vizsgálata az ***MSZ EN 50130*** **szabványsorozatban** leírtak szerint történik.

4.2. Környezetállósági vizsgálatok és követelmények

A riasztásátviteli rendszer környezetállósági követelményei feleljenek meg ***MSZ EN 50136-2-1 szabvány*** *6.4. szakasza* követelményeinek.

4.3. EMC vizsgálatok és követelmények

A riasztásátviteli rendszer környezetállósági követelményei feleljenek meg ***MSZ EN 50136-2-1 szabvány*** *7.1. szakasza* követelményeinek.

4.4. Jelölés, azonosítás

A riasztásátviteli rendszer valamennyi részegységét el kell látni címkével.

A címkének legalább a következő információkat kell hordoznia:
– a termék megfelelőségéért felelős szervezet neve (pl. a gyártó, forgalmazó stb.),
– a termék típusa,
– a gyártóra való utalás,
– szabványok által megkívánt jelölések.

A jelölés legyen olvasható, rögzített és tartós, lehet a részegységeken belül vagy kívül.

5. A riasztásfogadó központban teljesített diszpécser-szolgálattal szembeni követelmények

5.1. Működési Utasítás

A riasztásfogadó központ személyzetének munkáját *Működési Utasítás* szabályozza, melynek legalább a következőket kell tartalmazza.

- a biztonsági felügyeleti központ rendeltetése;
- a diszpécser szolgálat szervezeti felépítése, a szolgálat függelmi viszonyai;
- a riasztásfogadó központban folyó tevékenység részletes szabályozása. (Szolgálat átadás-átvétel, ellenőrzési és jelentési kötelességek, teendő a felügyelt objektumoktól érkező jelzések vétele ill. azok kimaradása esetén, teendő technikai eszközök meghibásodása esetén, teendő a biztonsági felügyeleti központot ért támadás, rendkívüli esemény esetén, okmányok vezetése, étkezés és pihenés megszervezése, stb.);
- a riasztásfogadó központ és a védett objektumok kapcsolatrendszerének meghatározása;
- a riasztásfogadó központba belépésre jogosultak köre és a belépés módja.

A *Működési Utasítást* a riasztásfogadó központ ügyeleti helyiségében kell tárolni.

A *Működési Utasítás* kötelező *mellékletei:*

- legfontosabb telefonszámok, kapcsolatok táblázata;
- a fontosabb teendők rövid tevékenységi leírása;
- eseményről szóló jelentés mintája;
- előfizetői szerződésminta (több féle szerződési lehetőség esetén az ügyfeleket egyértelműen hozzá kell rendelni az egyes szolgáltatási típusokhoz);
- a riasztásfogadó központ személyzetének munkaköri leírása;
- teendők a riasztásfogadó központban keletkező tűz vagy más rendkívüli esemény bekövetkezte esetén,
- utasítás a bizalmas dokumentumok, okmányok kezelésére.

A *Működési Utasítás* mellékletei a diszpécser fennakadásmentes tevékenységét segítik, ezért jól látható helyen kell kifüggeszteni.

5.2. Technikai leírás

A riasztásfogadó központ rendelkezzen **Technikai leírással**.

A Technikai leírás tartalmazza a következőket.

- A biztonsági felügyeleti rendszer működési leírása.
- A központi egység kezelési utasítása, egyszerű hibaelhárítás.
- A kihelyezett egységek működési leírása, használati utasítása.

A Technikai leírást a biztonsági felügyeleti központ ügyeleti helyiségében kell tárolni.

5.3. A riasztásfogadó központ technikai védelmével szemben támasztott követelmények

5.3.1. Védelmi intézkedések

A riasztásfogadó központ

- mechanika védelmi-
- elektronikai védelmi-
- a területileg illetékes rendőrkapitányságra bekötött riasztásátviteli rendszerének

az **ajánlás *A fejezetének* KO 5 osztálynak** megfelelő követelményeket kell kielégítenie.

A riasztásfogadó központ és az ott szolgálatot adó személyek védelmére elektronikus támadásjelző rendszert kell kialakítani, amely közvetlen támadás esetén lehetővé teszi a beavatkozó erők értesítését.

A támadásjelző rendszer és a jelzésátviteli út legyen szabotázsvédett. Megfelelő technikai lehetőségek hiánya esetén a támadásjelző rendszer rendelkezzen legalább két, eltérő műszaki megoldással kivitelezett jelzésátviteli úttal.

Biztosítani kell a védett objektumok és azok tulajdonosainak adatait tároló információtárolók illetéktelen hozzáférés elleni védelmét.

5.3.2. Bejutás korlátozási intézkedések

Biztosítani kell a biztonsági felügyeleti központ ügyeleti és technológiai helyiségeibe való belépés engedélyezésének, korlátozásának technikai feltételeit az ajánlás A fejezetének **KO 5 kockázati osztálynak** megfelelő beléptető és belépést korlátozó rendszerrel.

5.3.3. Egyéb technikai követelmények

A riasztásfogadó központ az átvitel-technikai összeköttetéseken túl, rendelkezzen a bejövő és kimenő telefonhívások végrehajtására használatos, különböző hívószámokkal rendelkező telefonvonalakkal.

A helyi távközlési szolgáltatóval kötött szerződés keretében biztosítsa ezen vonalak ráhívás elleni védelmét, a hívószámok titkosítását, a hívásbontás kezdeményezésének lehetőséget.

A kimenő hívások biztonsága érdekében a riasztásfogadó központ rendelkezzen legalább két eltérő rendszerű távbeszélő összeköttetéssel (pl. vezetékes és mobil telefon)

A riasztásfogadó rendszerközpont rendelkezzen olyan tartalék áramforrással, amely a hálózati feszültség kiesése esetén is legalább 6 órán keresztül képes biztosítani a felügyeleti munka ellátását.

5.4. A riasztásfogadó központ dokumentációja

- működési utasítás (ld. 6. fejezet a. pont)
- technikai leírás (ld. 6. fejezet b. pont)
- a biztonsági felügyeleti rendszer és elemeinek részletes műszaki dokumentációja
- a rendszerközpont egységeinek telepítési dokumentációja a főbb részegységek, naplózó egységek azonosításra alkalmas nyilvántartási számai
- a rendszerközpont egységeinek karbantartási utasítása és a karbantartások végrehajtását igazoló naplója
- a kihelyezett egységek telepítési/beszerelési utasítása
- tervezői nyilatkozat
- kivitelezői nyilatkozat
- oktatási jegyzőkönyv

6. A riasztásátviteli rendszerek és részegségeinek kockázati osztályba sorolásának menete

Amennyiben a termék rendelkezik az **ajánlás B.3. fejezet 1.2.1. pont** szerinti tanúsítványokkal, akkor a tanúsítványokat és az azokat megalapozó vizsgálati jegyzőkönyveket a kockázati osztályba soroláshoz a **MABISZ** rendelkezésére kell bocsátani.

A tanúsítványok ill. a **MABISZ** által elfogadott vizsgálati jegyzőkönyvek, valamint a termék dokumentációja alapján a **MABISZ** a terméket kockázati osztályba sorolja.

A termék kockázati osztályba sorolási értéke a tanúsítványok, ill. a vizsgálati jegyzőkönyvek és a termék dokumentációból származtatott értékelésen kapott legalacsonyabb kockázati osztály értéke.

7. Dokumentáció

A vizsgálatokhoz és a felhasználó által történő működtetéshez szükséges teljes dokumentációnak rendelkezésre kell állnia.

A termék műszaki leírásának a következő információkat kell tartalmazza:

a) a villamos tápellátással szemben támasztott követelmények, ideértve a feszültségtartományt, az áramerősséget és a frekvenciát;
b) azon riasztásátviteli rendszer(ek) típusa, amely(ek)hez a berendezés alkalmazható, és azon berendezések leírása, amelyekhez való összeköttetésre szánják a berendezést;
c) a riasztási üzenetek átviteli ideje, és - ahol ez alkalmazható - a létrehozásukra előírt idő;
d) a nyugtázójel generálására előírt idő, ha ilyen jelet használnak;
e) a hibák észlelésére és jelentésére előírt idő;
f) a szükséges interfész típusa, beleértve minden különleges, az interfész felügyeletére vonatkozó követelményt;
g) a kimeneti jelszintek és/vagy a bemeneti jel érzékenysége (azaz a legnagyobb és a legkisebb megengedhető csillapítás), ideértve a választható beállítások részletezését;
h) a riasztásátviteli berendezésnek az átviteli útvonalon előforduló zavarokra vonatkozó tűrése;
i) hivatkozás arra a zavar-kibocsátási szabványra, amelyet a berendezés kielégít;
j) a jelzésátviteli biztonság szintjére vonatkozó adatok, beleértve a választható beállítások részletezését;
k) telepítési és kábelezési utasítások;
l) beállítási utasítások, ideértve minden szükséges szerszám vagy vizsgálóberendezés jellemzőit;
m) az egység telepítését követően a helyes működés ellenőrzése céljából végrehajtandó vizsgálatok és útmutató az egyszerű, illetve általános hibák azonosításához;
n) a soros adatinterfészhez való csatlakoztatás és az interfész beállításának részletezése, ha van ilyen, és a támogatott soros protokollok leírása;

o) a berendezés felhasználója számára szükséges információk, ideértve valamennyi kezelőszerv működésének magyarázatát és a kijelzések jelentését;
p) alkalmasság megosztott átviteli útvonalakon való használatra, és annak meghatározása, hogy milyen típusú megosztott útvonalakhoz vagy rendszerekhez alkalmas a berendezés.

A berendezéshez telepítési útmutatót kell mellékelni, amelynek legalább a (j) – (n) pontokban felsorolt információkat kell tartalmaznia.

Ahol szükséges, ott felhasználói útmutatót is kell mellékelni a berendezéshez, amely legalább az (o) pontban leírt információt tartalmazza.

II. rész Riasztásfogadó központokkal szemben támasztott követelmények

8. Bevezetés

Ez az **ajánlás** az összes biztonsági riasztásfogadó- és riasztás-felügyeleti központra (továbbiakban: riasztásfogadó) vonatkozik, melyek a vészhelyzet esetén reagálást váró riasztórendszereket felügyelik.

A riasztásfogadó központtal kommunikáló riasztórendszereknek eleget kell tenniük azoknak a szabványoknak, amelyek a riasztórendszerekre és a riasztásfogadó központokra vonatkoznak.

A riasztásátviteli rendszer és a riasztásfogadó központ nyilvános és/vagy zárt telekommunikációs hálózathoz kapcsolódó adóvevője rendelkezzen egy ilyen típusú kapcsolódáshoz szükséges minősítéssel.

9. Cél

Ez az **ajánlás** azon riasztásfogadó központok modelljét, felépítését, kezelőszemélyzetét, berendezéseit, és működését határozza meg, melyek riasztóberendezésektől kapnak jelzéseket.

10. Rendelkező hivatkozások

Ez az ajánlás az alábbi szabványok alapján határoz meg követelményeket

EN 50136 Riasztórendszerek- riasztás-átviteli rendszerek és berendezések
EN 357 Épületüvegezés – Biztonsági üvegezés tesztelése és osztályozása kézi támadás ellen.
EN 1522 Ablakok, ajtók, redőnyök és zsalugáterek - Átlövés elleni ellenállás - követelmények és osztályozás.
EN 1523 Ablakok, ajtók, redőnyök és zsalugáterek - Átlövés elleni ellenállás - .Tesztelési eljárások.
EN 12543 Sorozat – Épületüvegezés - Többrétegű üveg és többrétegű biztonsági üveg.
EN 13541 Épületüvegezés - Biztonsági üvegezés - Ellenállás tesztelése és osztályozása robbanás által keltett lökéshullámra.
CLC/TC79/NL001/NPF: 2006 –Megfigyelő és riasztásfogadó központ követelményei

A hatályos szabványok gyűjteménye az ***A 1 függelékben*** található

11. Szakkifejezések és rövidítések

Az **ajánlás** ***A.3. függeléke szerint***

12. Riasztásfogadó és riasztás-felügyeleti központ vizsgálata

A **MABISZ** jogosult az általa elfogadott riasztásfogadó központ vizsgálatára. Ez a vizsgálat bármilyen ésszerű, előre egyeztetett időben megtörténhet.

13. A helyszín kiválasztása

Belépés a területre.

A riasztásfogadó központot olyan épületben kell elhelyezni, hogy az épület azon területét ahonnan a riasztásfogadó bejárata elérhető, kizárólag a központot működtető cég foglalja el.

Ezekre a területekre illetéktelen nem juthat be az épület más részéből.

A terület megközelítése.

A területre nem nyílhatnak bejáratok semmilyen más szomszédos területről, kivéve azokat a szomszédos területeket, melyek teljes mértékben a riasztásfogadó központot működtető céghez tartoznak.

Ezekre a szomszédos területekre sem juthat be illetéktelen az épületből.

A terület védelme.

Az épület azon területét, amely a riasztásfogadó központot működtető céghez tartozik és ahol a riasztásfogadó központ található, a behatolásjelző rendszerek vonatkozó szabványai szerint telepített behatolásjelző rendszerrel kell védeni. Ilyen behatolásjelző rendszernek magában kell foglalnia egy figyelmeztető eszközt, amely behatolás esetén azonnal figyelmezteti a központ személyzetét.

A terület foglaltsága.

A fentiek szerint, egy riasztásfogadó központot működtető cég tulajdonolhat bármely más vállalatot, de csakis a biztonságtechnikai iparon belül, ahol a cég vezetését (részben vagy egészében) az a menedzsment végzi, amely már gyakorlott az olyan cégek vezetésében, mellyel az ügyfelek távfelügyelet biztosítására kötnek szerződést.

14. Kialakítás

A riasztásfogadó központ kialakítása.

A riasztásfogadó központnak egy zárt helyiségből és egy odavezető előtérből kell állnia. Mindkét helyiség szerkezetének építési anyaga a ***B.3. 07 táblázat*** szerinti vagy azzal megegyező biztonsági szintű legyen.

A zárt helyiség, az odavezető előtér és a környezet szerkezete legalább 1 órás tűzállósággal rendelkezzen.

B.3. 07 táblázat: A riasztásfogadó központok építési anyagai

Építési elemek	Anyagok	Méret és egyéb előírások
Körülvevő falak (beleérve az állomás és előtér közti fal)	Téglafa	Min. 20 cm vastagságú
	Beton	Min. 150 mm vastagságú, 20 MPa nyomást elvisel
	Acéllemez	Min. 3 mm vastagságú
Belső falak	Nincs előírás	Nincs előírás
Padló talajon	Beton	Min. 150 mm vastagságú 20 MPa nyomást elvisel
Padló emeleteken plafon, tető	Beton	Min. 150 mm vastagságú 20 MPa nyomást elvisel Mélység és megerősítés meghatározása feszítés és terhelés által.
	Alacsony széntartalmú acéllapok	Min.1.5 mm vastag (lapok összehegesztve, csavarokkal biztosítva)
Megjegyzés: az építési elemek támadás elhárításra általánosan elfogadottak, azonban más építési anyagok használatával is el lehet érni ugyanazt a biztonsági szintet.)		

Kiegészítő helyiségek. A WC és a mosdó a riasztásfogadó központon belül legyen. Étel és ital készítésére helyiséget kell biztosítani a riasztásfogadó központon belül. Ahol főző berendezés is van, azt 30 perces tűzállóságú fallal kell elkülöníteni a munkateremtől**.**

Nyílászárók. A riasztásfogadó központ szerkezetén nyílászárók csak az alábbi helyeken lehetnek:

- normál bejárat;
- vészkijárat;
- üvegezett felületek;
- szellőzés;
- kábel ki- és bevezetések.

Bejárat.

A bejárat két ajtóból álljon, melyek méretei nem haladhatják meg a 2,5 m magasságot, 1,1 m szélességet. A két ajtó közti terület az előtér, melynek területe nem haladhatja meg a 6 m²-t. A két ajtó távolsága legalább 1,5 m kell, hogy legyen. Az ajtók kényszerkapcsolatban legyenek, hogy ne lehessen egyidejűleg nyitva mindkettő, csak ellenőrzött körülmények között. A riasztásfogadó központ ajtaja az előtérbe, az előtér külső ajtaja mindig kifelé nyíljon. Mindkét ajtó min. 1 órás tűzállósággal rendelkezzen.

A riasztásfogadó központnak alábbiak szerinti szilárdságú szerkezettel kell rendelkezniük:

(a) min. 50 mm vastagságú tömör keményfa, vagy keményfa ajtó esetén az előtérbe vezető külső ajtó mindkét oldala min.1,5 mm vastagságú acéllemezzel borítva, vagy csak az egyik oldalán vagy az ajtó szerkezetén belül 3 mm vastagságú acéllemezzel ellátva. Ha ilyen lemezek vannak az ajtó egyik vagy mindkét oldalán, azokat úgy kell rögzíteni, hogy kívülről ne lehessen leválasztani.
(b) Vasajtó, min. 6 mm vastagságú alacsony széntartalmú acéllemezből

Másfajta ajtó csak akkor megengedett, ha legalább olyan ellenállással rendelkezik, mint az (a) és (b) pontokban taglaltak, és ha tervezésük és építésük megfelel ezen Szabályzat vonatkozó előírásainak.

Mindkét ajtó sarokvasa rendelkezzen két, megerősített acél, fix (toló)zárral hogy megelőzze az ajtó elmozdítását. Mindkét ajtó és az egész előtér belátható legyen a riasztásfogadó központból, az ajtók zárt állapota mellett. Ez történhet leső nyíláson ill. videó megfigyelő rendszeren keresztül, vagy mindkettővel. Mindkét ajtót fel kell szerelni nyitó berendezéssel, amelyet alaphelyzetben csak a központból működtetnek, továbbá fel kell szerelni automatikusan csukó és záró berendezéssel. Az ajtókat elektromosan kényszerkapcsolatba kell hozni, ezzel megakadályozva, hogy zárjaik egyidejűleg nyitva legyenek. A riasztásfogadó központon belül eszközt kell biztosítani a zárszerkezetek nyitására vészhelyzet esetén. Az előtér külső ajtajának zárja az előtérből kézzel vagy elektromosan működtethető legyen.

Az ajtó külső felén lévő valamennyi szerelvénye olyan legyen, hogy anyaguk ne segítse elő az erőszakos behatolást. Az ajtókeret kialakítása, az ajtókerethez való illesztése, továbbá az ajtókeret falszerkezethez való rögzítése olyan legyen, hogy a fentiekben meghatározott védelem szintje ne csökkenjen.

Elektromos záró/nyitó szerkezetek.

A bejárati előtér ajtóira felszerelt bármely elektromos záró/nyitó eszköz bevésett vagy védőpánttal szerelt legyen. A zárnyelv, vagy a fogadó elektromosan vezérelhető legyen. Az eszköz automatikusan zárjon, ha az ajtó becsukódik. A rögzítő csavarok az ajtó csukott állapotában támadás ellen védettek legyenek. A zár vészhelyzet esetére mechanikus kulccsal legyen nyitható és védve legyen véletlenszerű használat ellen. Áramszünet esetén a zárnak zárva kell maradnia. Ha a zárszerkezet az ajtóra van felszerelve, akkor a zárhoz vezető elektromos kábelt fémborításban kell vezetni ill. a külsővezetésű kábelt mechanikusan védeni kell.

Vészkijárat.

Ahol külön vészkijárat van, ott a kijárati ajtó(k) és sarokvasai, kerete, rögzítése, záró pontjai és nyitó szerkezetük feleljenek meg ugyanazon fizikai erőhatás elleni ellenállásnak, melyek az előtérhez vezető külső bejárati ajtóra vonatkoznak. A kijárati ajtó(k) csak bentről és vészhelyzetben nyitható és fel kell szerelni nyitószerkezettel (pl.: pánik retesz). A nyitószerkezetek csak a központ belsejéből működtethetők.

Üvegezett felületek.

Ahol üvegezett felület található, annak kerete és rögzítése álljon ellen a behatolást eredményező fizikai támadásnak, és legyen legalább egyenértékű az **MSZ EN 357** és **MSZ EN 1522** előírásaival.

A riasztásfogadó központ belseje az üvegezett felületen keresztül nem lehet látható sehonnan az épületen kívülről.

Szellőzés.

A szellőző bevezető és kivezető nyílásainak keresztmetszete nem haladhatja meg a 0,09 m^2-t (300 mm x 300 mm) és biztosítani kell, hogy a riasztásfogadó központ belseje ne legyen egyenes látóvonalban a szellőző cső kimenő végével.

Ahol a szellőző bevezető vagy kivezető nyílásainak keresztmetszete meghaladja a 0.02 m^2 – t, oda behatolás érzékelőt kell szerelni, amely észleli a behatolási kísérletet a szellőzőbe.

A riasztásfogadó központ szerkezetén lévő szellőző be- és kivezető nyílásait fizikai védelemmel kell ellátni. Minden szellőzőt olyan hermetikusan záródó szeleppel kell védeni, melyet a riasztásfogadó központból be lehet zárni.

Kábel ki- és bevezetések.

A riasztásfogadó központ szerkezetén lévő, a szolgáltatáshoz szükséges kábelek vagy csövek bevezetései számára szolgáló rések keresztmetszete nem haladhatja meg a 0.02 m^2-t. A kitöltő anyag oly mértékben álljon ellen tűznek vagy fizikai támadásnak, mint a riasztásfogadó központ szerkezete.

15. Elektronikus védelem

Általános követelmények

A biztonság mértékének olyannak kell lennie, hogy a riasztásfogadó központ, beleértve falakat, ajtókat, tetőt vagy mennyezetet védve legyen, ellátva olyan elektronikus védőrendszerrel, amely megfelel a lentebb leírt követelményeknek és az **MSZ EN 50130 szabványsorozat** szerint telepített (lásd az 5.3. pont követelményeit) behatolásjelző rendszerrel.

Ahol a riasztásfogadó központ nem a földszinten helyezkedik el, vagy ahol lentről el lehet érni (pl.: pincéből) akkor a riasztásfogadó központ padlóját is védeni kell elektronikus védőrendszerrel. (Lásd ***B.3. 07. táblázat***, emeletek.)

Védelem.

Az érzékelő eszközöket a behatolásjelző rendszerek szabványai szerint úgy kell telepíteni, hogy észleljék a riasztásfogadó központ épületét érő erőszakos támadást. A riasztásfogadó központ telefonvonalait elektronikus védőrendszerrel kell ellátni, érzékelni kell a távközlési szolgáltató azon kábelaknájának vagy elosztódobozának fedő vagy ajtó nyitását, amelyen keresztül a riasztásfogadó központ a távbeszélő szolgáltatást kapja.

Tűzvédelem.

Egy, a vonatkozó szabvány szerint telepített tűzjelző rendszer biztosítsa a riasztásfogadó központ védelmét.

A riasztásfogadó központ legyen ellátva legalább szénmonoxid- és füstérzékelő rendszerrel, amely figyelmezteti a riasztásfogadó központ személyzetét, mielőtt eléri azt a koncentrációt, amikor a kiürítés szükségessé válik.

Villámvédelem.

Az épületet - valamint a riasztásfogadó központot és részegységeit - amelyben a riasztásfogadó központ található, fokozottan védeni kell villámcsapás közvetlen és követett hatásaitól a vonatkozó szabványok előírásainak megfelelően. (lásd: az *ajánlás **A.4. fejezetét*** is)

Ajtók védelme.

Egy látható vagy hallható jel keletkezzen, ha bármely a riasztásfogadó központhoz vezető vagy előtéri ajtó zárja nincs zárva. A behatolásjelző rendszerekre vonatkozó szabványnak megfelelően telepített érzékelőket kell minden bejárat és vészkijárat ajtajára szerelni, hogy riasztás állapot jöjjön létre, bármelyik ajtó nyitása esetén.

Vészbehatolási eljárás.

Megengedhető, hogy a vészbejárat a normál bejárati ajtó is egyben. Ebben az esetben úgy kell a védelmét megtervezni, hogy jelzést kezdeményezzen egy másik riasztásfogadó központba, amikor vészbehatolás történik.

Ahol kulcsokat használnak ehhez, ott úgy kell megtervezni a védelmét, hogy azok biztosan csak a szervezethez tartozó, felhatalmazott személyek számára legyenek hozzáférhetők oly módon, hogy ne veszélyeztesse a riasztásfogadó központ biztonságát.

Támadásjelző eszközök.

A behatolásjelző rendszerek vonatkozó szabványa szerint telepített támadásjelző eszközöket kell felszerelni a riasztásfogadó központban a bejárat és a vészkijárat(ok) mellett, továbbá a riasztásfogadó központ állományának munkahelyein.

Jelzés az elektronikus védőrendszerektől.

A vezérlő berendezésnek olyannak kell lennie, hogy az elektronikus védőrendszer által generált riasztás állapotot automatikusan továbbítsa egy másik – ezen **ajánlásnak** megfelelő - riasztásfogadó központba, vagy a területileg illetékes rendőrségre.

Ilyen riasztás állapot továbbítása két különálló átviteli úton kell, hogy rendelkezésre álljon, melyek nem ugyanazt a fizikai infrastruktúrát használják.

Videómegfigyelő rendszer.

A riasztásfogadó központ legyen ellátva videó megfigyelő eszközökkel, amelyekhez tartozó kamerák úgy legyenek felszerelve, hogy elkülönítve mutassák az alábbi helyszíneket.

- A cég által használt épületrész külső bejárata.
- A riasztásfogadó központ külső bejárati ajtaja, kívülről.
- A riasztásfogadó központ vészkijárata, kívülről.

A fentebb felsorolt területek megfigyelésére szolgáló monitor(oka)t, a kapcsoló vagy multiplexer berendezéssel együtt a riasztásfogadó központban kell elhelyezni, az ügyeleti személyzet kezelésében, hogy mindenkor biztosítva legyen ezen területek folyamatos megfigyelése.

A jó látási viszonyok érdekében megfelelő világításról gondoskodni kell.

A videó megfigyelő rendszernek egy megfelelő képrögzítő rendszert is tartalmaznia kell, hogy minden mozgás felvehető legyen, ami ezeken a pontokon történik.

16. Kommunikációs berendezések

A következő kommunikációs berendezéseket kell biztosítani:

Beszédkommunikáció a bejárati előtérbe és azon keresztül.

A riasztásfogadó központot olyan berendezéssel kell ellátni, amely minden a riasztással és az azzal kapcsolatos intézkedésekkel foglalkozó távbeszélő forgalmat automatikusan rögzít.

Ezeket a felvételeket meg kell őrizni a vonatkozó eseménytől számított 3 hónapig.

17. Jelzések fogadása

Általános követelmények.

A riasztásfogadó és riasztás-felügyeleti központban minden kapott jelzésnek a fajtája és eredete egyenként azonosítható legyen és minden jelzést automatikusan rögzíteni kell, legalább az alábbi információk megadásával:

- Ügyfél vagy felhasználó azonosítás
- A jelzés természete
- A jelzés vételének dátuma és ideje

Ügyeletes intézkedése.

Ahol az ügyeletes a kapott jelzés alapján intézkedik, az intézkedés részleteit rögzíteni kell, beleértve az intézkedés dátumát és idejét és azonosítani kell azt a személyt/személyeket, akik ezt elvégezték.

Üzenetek.

Magnetofonról lejátszott vagy elektronikusan generált olyan hangüzeneteket, amelyek a rendőrség beavatkozását igényelnék, tilos a behatolásjelző rendszer automatikus hívó egységeiből a riasztásfogadó központba elküldeni.

18. Áramellátás

Hálózati áramellátás.

A közüzemi áramellátó hálózatot úgy kell kezelni, mint a riasztásfogadó központ elektromos táplálásának alapvető forrását. A a riasztásjelzés fogadó berendezés, a hangjelzést alkalmazó figyelmeztető berendezés és az elektronikus védelmi berendezés tápegységeit biztosítékok és megszakítók védjék a riasztásfogadó központon belül elkülönítve minden más áramellátástól.

Tartalék áramellátás.

A riasztásfogadó központon belül megfelelő berendezést kell biztosítani, amely a hálózati tápellátás megszakadása esetén automatikusan tartalék ellátásra kapcsol át.

A tartalék tápegységhez tartozzon a riasztásfogadó központban elhelyezett tölthető akkumulátortelep is. Ennek a telepnek elegendő kapacitással kell rendelkeznie, hogy működtetni tudja a riasztásjelzést fogadó berendezést, az elektronikus védelmet, és az előírt videó megfigyelő rendszert nem kevesebb, mint 24 órán át illetve nem kevesebb, mint 4 órán át, egy tartalék generátor rendelkezésre állása esetén, vagy 30 percen át ha két generátor van. Számítógéppel ellátott riasztásfogadó központoknál az akkumulátortelepnek egy szünetmentes áramellátó rendszeren keresztül kell működnie.

A tartalék tápegység A/h kapacitását, az óránkénti átlagfogyasztást 1,5-el szorozva kell kiszámolni. Bármely töltőberendezés kapacitásának elegendőnek kell lennie, hogy kielégítse a maximális terhelési igényeket és egyben újratöltse az akkumulátort teljesen lemerült állapotból a követelmények szerinti kapacitás 80%-áig, legfeljebb 24 óra alatt. A hálózati áramellátás megszakadása esetén a felügyeleti rendszer munkájához szükséges összes lényeges berendezésnek folytatnia kell a működést, a biztonság vagy a hatékonyság oly mértékű csökkenése nélkül, hogy a felügyeleti rendszer vételi, feldolgozási és intézkedési képessége ne károsodjon (bele értve a szükség- és tartalék világítást és a szellőző berendezések működését is)

Tartalék generátor.

Ahol tartalék generátor van telepítve, (nem feltétlenül a védett területen) annak elegendő kapacitással kell rendelkeznie a tartalék táplálás biztosítására. Gondoskodni kell megfelelő üzemanyag tartalékról, mely működteti a generátort legalább 24 órán keresztül. A generátornak automatikus indításúnak kell lennie. A tartalék generátor indításához szükséges akkumulátorok töltése a generátor működésétől függetlenül történjen.

A tartalék generátort a gyártó előírásainak megfelelően kell karbantartani, és biztonságos környezetben kell tárolni. A munkateremben ki kell jelezni az éppen üzemelő áramforrást.

19. Kezelői és működési folyamatok

Kezelőszemélyzet.

A felügyeleti rendszereket folyamatosan legalább két ügyeletes kezelje. Ahol a riasztásfogadó és riasztás-felügyeleti központ együttműködik egy másik riasztásfogadó és riasztás-felügyeleti központtal - és az egyidejűség, valamint a működési módszerek biztosítják, hogy hatásuk ugyanaz, mint a legalább két emberrel ellátott riasztásfogadó és riasztás-felügyeleti központoknak, akkor egy fő kezelővel is megfelelnek ezen követelménynek.

Átvilágítás.

A riasztásfogadó és riasztás-felügyeleti központ teljes állományát át kell világítani, előző munkahelyeikre való tekintet nélkül.

Alapkövetelmény, hogy minden személyt át kell világítani legalább10 évre visszamenőleg a valós munkaviszony kezdetéig, vagy valós munkaviszonyba való áthelyezésig vagy a nappali iskola idejéig visszamenőleg.

A riasztásfogadó központ nem alkalmazhat olyan személyeket, akiknek előmenetelük vagy történetük azt mutatja, hogy nem tudnak ellenállni törvénytelen személyes nyereségnek vagy vesztegetésnek, vagy más a biztonságot károsító olyan lehetőségeknek, amelyekkel ez a munkakör járhat.

Kiképzés.

Biztosítani kell egy minimális időtartamú begyakorlási időt, mielőtt megengedik a kezelőknek, hogy felügyelet nélkül kezeljék a riasztásokat. A gyakorlás célja, hogy megfelelően biztosítsa a hozzáértést a specifikus feladatok elvégzéséhez (pl.: behatolásjelző rendszer kezelése, videomegfigyelő rendszer kezelése, stb.). Továbbképzéseket kell folytatni új berendezések alkalmazása, vagy a működtetési folyamatokban történő változások esetén.

Értesítések a riasztórendszerektől.

Érthető irányelvek alapján kell meghatározni az élesített vagy részben élesített behatolásjelző rendszertől érkező hívásokat követő tevékenységet (lásd „A” függelék).

A rendőrséget, vagy más felhatalmazottat (pl. az ügyfél) értesíteni kell minden olyan a megfigyelt területről érkező érvényes riasztás jelzésről, mely a behatolásjelző rendszer vagy annak egy része élesített állapotában érkezik.

Élesítés és hatástalanítás előzetes egyeztetése.

Szükség esetén, az ügyfélnek -biztonsági okok miatt - informálnia kell azon szándékáról a riasztásfogadó központot, hogy élesítsék, vagy hatástalanítsák a rendszert egy előre meghatározott időben. Ezt a folyamatot egyértelműen dokumentált eljárás alapján kell végezni.

Tesztelés.

A riasztásfogadó központ berendezéseinek megfelelő működését ellenőrizni és az eredményeket rögzíteni kell, a következők szerint:

24 órát nem meghaladó intervallumokon belül:

- Kimenő kommunikáció a rendőrséggel vagy más hatóságokkal.
- A riasztásjelzést fogadó berendezés, és minden olyan berendezés belső órái, amelyek biztosítják, hogy valamennyi esemény - beleértve az ügyeletes tevékenységét is - pontos dátummal és idővel legyen ellátva.

7 napot nem meghaladó intervallumokon belül:

- Fő és tartalék áramellátók, automatikus átkapcsoló berendezés, vészvilágítás és a riasztásfogadó központ riasztórendszere.
- Minden vonal, mely biztosítja a riasztás jelzések fogadását és a riasztásfogadó központ bejövő és kimenő kommunikációját.

Hibakezelés, jelentés.

A berendezés mindazon része, amely részt vesz a riasztásjelzés fogadásban, megjelenítésében vagy továbbításában rendelkezzen olyan tartalék berendezéssel vagy folyamattal, amely automatikusan vagy a riasztásfogadó központ ügyeletese által beindítható, a hibának az ügyeletes általi észlelését követő 1órán belül. (teljes redundancia)

Megfelelő szerződés(ek)t kell kötni az illetékes szállító(k)val, hogy egy megegyezés szerint időn belül jelenjen meg a helyszínen, és kezdje meg azon hiba elhárítását, amely a ***tesztelés*** során derült ki.

Beléptetés.

A riasztásfogadó és riasztás-felügyeleti központba történő bejutásnak - kivéve vészbejárat használatát - dokumentált és az ügyeletes által engedélyezett folyamatnak kell lennie.

Ez a folyamat határozza meg a riasztásfogadó központba belépni kívánó személyek azonosítását és követelje meg ezen személyek a pozitív azonosítását mielőtt a belépést engedélyezik. A riasztásfogadó központba való belépést pozitív azonosítás esetén is ellenőriznie kell valamelyik ügyeletesnek.

Három főnél többen semmilyen esetben sem tartózkodhatnak egyszerre az előtérben. Mindig az ügyeletes által már ismert, feljogosított személyek lépjenek be először az előtérbe.

A riasztásfogadó központ minden látogatójáról nyilvántartást kell vezetni.

Egészség, biztonság.

Látható vagy hallható jelzést kell előidézni a riasztásfogadó és riasztás-felügyeleti központban óránként legalább egyszer és a kezelőnek ezt a jelzést 1 percen belül nyugtáznia kell („halott ember2 funkció).

A jelzés nyugtázásának elmulasztása esetén jelzést kell küldeni egy másik – ezen szabályzatnak megfelelő - riasztásfogadó központba.

Riasztásfogadó és riasztás-felügyeleti központokba más riasztásfogadó és riasztás-felügyeleti központtól érkező jelzései.

Egy riasztásfogadó központot figyelni kell egy másik riasztásfogadó központ által.

Az alábbi helyzetekben kell a másik riasztásfogadó és riasztás-felügyeleti központnak riasztás jelzéseket kapnia:

- vészkijárat kinyitása
- mindkét a központhoz vezető bejárati ajtó egyidejű nyitása
- támadás
- tűzriasztás
- „halott ember” funkció

Felülvizsgálat.

A riasztásfogadó központnak félévenként egy teljes felülvizsgálati dokumentációt kell készítenie, amely bizonyítja, hogy megfelel ezen **ajánlás** valamennyi követelményének..

Panaszeljárás. A riasztásfogadó központnak rendelkeznie kell egy érthetően megfogalmazott és közreadott eljárással a panaszok fogadására és kezelésére.

Az ügyfeleknek meg kell adni a kapcsolattartó személy adatait, amennyiben panaszt kívánnak emelni a szolgáltatás bármely része ellen.

20. Adatkezelés és adattárolás

Megjegyzés: A hatályos adatvédelemi örvény szerint.

Ügyfél adatok

A riasztásfogadó központhoz kapcsolódó valamennyi riasztórendszer adatainak rendelkezésre kell állnia az ügyeletesek számára.

Az adat lehet írott vagy elektronikus memóriában tárolt. Ez esetben nyomtatott formában is elérhetőnek kell lennie.

Az adat tartalma:

- Az ügyfél neve, címe, elérhetősége(i);
- Terület/épület azonosító száma és minden speciális körülmény;
- Felhasználók nevei, címük, telefonszámaik;
- Végrehajtandó műveletek riasztás esetén - mikor kell értesíteni a rendőrséget, stb;
- Megegyezés szerinti élesítés, hatástalanítás ideje, ha szükséges.

Adatkommunikáció

Rögzíteni kell minden a riasztásfogadó központtal történő kommunikációt és meg kell őrizni legalább az alábbi időpontokig:

- 3 hónapig - Minden távbeszélőn folytatott kommunikációt a riasztásfogadó központból, központba, dátummal, idővel és visszajátszási lehetőséggel.
- 12 hónapig - Minden adatkommunikációt a riasztásfogadó központból, központba, a felügyelt eseményekről dátummal és idővel ellátva.
- 12 hónapig – Az eseményekre vonatkozó távbeszélő és adatkommunikáció tárolási idejének meg kell felelnie az adatvédelmi törvény követelményeinek.

Biztonság

Minden adatot biztonságosan, tűzálló helyen kell tárolni. Az elektronikus adatokat naponta archiválni kell.

Kezelés

Minden bizalmas természetű adatot biztonságosan kell kezelni.

Nyilvántartások

A riasztásfogadó központnak nyilvántartást kell vezetnie az összes rendszeres tesztelésről, karbantartásról és a riasztásfogadó központ berendezéseinek hibaelhárításairól.

21. Riasztás kezelés

A riasztásfogadó központnak olyan eljárásokat kell alkalmaznia, melyek felmérik minden riasztás jelzés valódiságát mielőtt a rendőrségnek továbbítaná, kivéve az átviteli hibákkal kapcsolatos hibákat, a kézzel adott riasztás jelzéseket vagy bármely más jelzést, amelyről írásban az ügyféllel megállapodtak, hogy nem továbbítandó a rendőrség felé.
Megjegyzés: a riasztás kezelés célja, ahol lehetséges biztosítani, hogy csak valós riasztás jelzések kerüljenek továbbításra a rendőrség felé.

A riasztásfogadó központnak riasztás kezelési folyamata feleljen meg. az „A” függelékben meghatározottaknak.

22. Vészhelyzet terv

Arra az esetre, ha a riasztásfogadó központ kiesik, vészhelyzeti tervet kell készíteni a helyzet kezelésére.

A vészhelyzeti tervnek foglalkoznia kell minden a riasztásfogadó központban valószínűsíthetően előforduló rendkívüli eseménnyel.

Ez magában foglalja a riasztásfogadó központ bármely problémáját, amely a szolgáltatás csökkenését okozhatja.

A vészhelyzet tervnek le kell fednie a technikai, személyzeti és más jellegű szituációkat.

A vészhelyzet tervben található:

a) utasítások a készenléti szervezetek informálására;
b) utasítások a tartalék riasztásfogadó központ indítására és/vagy a jelzések átirányítására;
c) utasítások a felhasználók értesítésére a rendszer problémájáról;
d) utasítások az ügyfelek/felhasználók értesítésére.

A vészhelyzet tervnek számolnia kell a lehetséges veszélyekkel, melyek bekövetkezhetnek. Ezek közül néhány:

a) Riasztásfogadó központ teljes kiesése;
b) Közművek hibája vagy károsodása;
c) Tűz vagy a szomszédos területeken keletkezett tűz hatása;
d) Árvíz vagy vízvezetéktörés;
e) Távközlési infrastruktúra meghibásodása
f) Jármű baleset, beleértve vonat és repülőgép szerencsétlenségeket
g) Szándékos rongálás
h) Bűncselekmény elkövetése, bombafenyegetések és kényszerítések
i) Abnormális működés vagy létszámhiány

Válasz vészhelyzetre

Ezt a műveletet a helyi vállalkozókkal és a készenléti szervezetekkel úgy kell kidolgozni, hogy a riasztásfogadó központ felügyelő funkciója működjön a vészhelyzetet okozó incidens vizsgálata, elhárítása vagy a javítás alatt.

Állomány tevékenysége

A riasztásfogadó központ vezetőjének felelőssége, hogy biztosítsa az állomány teljes felkészültségét és cselekvőképességét vészhelyzet esetén.

A teljes állományt ki kell képezni a vészhelyzet esetén használandó készülékek helyéről és használatáról.

Egy részletes akciótervet kell kidolgozni, amely tartalmazza a nem feltétlenül szükséges személyzet részleges evakuációját és azokat a helyzeteket mikor a teljes evakuáció szükségessé válik.

A tervnek tartalmaznia kell az újraindítás és/vagy az incidens utáni helyreállítás műveletét.

Legalább félévente minden a riasztásfogadó központban dolgozónak oktatáson kell részt vennie a vészhelyzet kezeléséről.

Feljegyzések

A gyakorlatok alatti eseményekről készült feljegyzéseket meg kell őrizni, minthogy ez a működési napló részét képezi.

23. A. Függelék - Riasztás kezelés

A.1. Riasztás feldolgozási eljárás

Megjegyzés: igazolt riasztás állapot esetén a riasztás feldolgozási eljárást nem mindig kell alkalmazni.

A riasztás jelzés fogadását követően - lehetővé téve a riasztás felhatalmazott használó által való törlését - a riasztásfogadó központ legfeljebb 120 másodpercnyi késést engedhet meg, mielőtt a rendőrséget szervezetet értesíti.

A kézi működtetésű eszközöktől érkező riasztás jelzések esetén a riasztás feldolgozási eljárás elmarad.

A riasztás feldolgozási eljárás késleltetése alatt a riasztásfogadó központ megkísérelheti a felügyelt területen lévő felhasználóval való kapcsolatteremtést és/vagy telefonhívást fogadhat a felhasználótól, hogy kiderítse a riasztás állapot okát és eldöntse valósnak vagy hamisnak minősítse azt.

Ha a felhasználó a riasztást szűrő késleltetési idő alatt - jogosított kódját használva - törli a riasztás állapotot, a riasztás tévesnek minősíthető.

A.2. A riasztás feldolgozási folyamat időparaméterei

Megjegyzés: igazolt riasztás állapot esetén az igazolt riasztás időparamétereit kell alkalmazni.

Riasztás jelzés fogadása esetén, a riasztásfogadó központnak kapcsolatot kell létesítenie a készenléti szolgálattal vagy meg kell kezdenie a kapcsolat felvételi eljárást, a következő időintervallumokon belül:

a) kézi működtetésű riasztások esetén: 30 másodperc alatt a fogadott jelzések 80%-ára, 60 másodperc alatt a fogadott jelzések 98.5%-ára vonatkoztatva;
b) minden más riasztás esetén 90 másodperc alatt a fogadott jelzések 80%-ára, 180 másodperc alatt a fogadott jelzések 98.5%-ára vonatkoztatva.

A.3. Átviteli hiba kezelése

Ha a riasztásfogadó központ átviteli hibajelzést kap vagy az átvitel megszakadását észleli, a következőknek megfelelően kell kezelni:

a) A riasztásfogadó központ ügyeletesének meg kell kísérelnie kapcsolatba lépni a védett területekkel és/vagy a felhasználókkal, hogy megállapítsák az okot.
b) Ha az átviteli hiba 90 másodpercen túl is fennáll, a riasztásfogadó központnak végre kell hajtania a szerződés szerinti megállapodásban rögzítetteket.

A.4. Igazolt riasztások

Megjegyzés: Az igazolt riasztás során követendő eljárásról írásos szerződésben kell megegyezni.

Igazolt riasztásnak tekinthető a riasztás állapot akkor, ha a felügyelt területen történt, a behatolás és támadásjelző rendszer által érzékelt és a riasztásfogadó központ felé továbbított jogtalan behatolás vagy jogtalan behatolási kísérlet, valós behatolásnak vagy valós behatolási kísérletnek minősül valamely, a következőkben ismertetett módszer alapján:

A.4.1. Folyamat által igazolt riasztások

Eljárások a folyamat által igazolt riasztás állapot megállapításához:

a) **I. eljárás**

Két különálló riasztás jelzés együtthatása jut a riasztásfogadó központba ugyanarról a felügyelt területről.

A riasztásfogadó központba az (AA detektortól vagy processzortól származó) „A” riasztás jelzés fogadását követően, egy második a (BB detektortól vagy processzortól származó) „B” riasztás jelzés érkezik egy meghatározott időintervallumon belül, ugyanarról a felügyelt területről.

Amennyiben a telepítő cég informálja a riasztásfogadó központot arról, hogy az AA és BB forrásból érkező riasztás jelzések bizonyítékot jelentenek a folyamat által igazolt riasztás állapotra, akkor a riasztásfogadó központnak jeleznie kell a két riasztás jelzés („A” és „B”) kombinációját, amely igazolt riasztás állapotot jelent.

Ha a második riasztás jelzés nem érkezik meg a szerződés szerinti igazolási időkorláton belül, akkor a riasztásfogadó központ ügyeletese tévesnek minősíti a riasztást. Erről az állapotról a felhasználót értesíthetik, de a rendőrséget nem informálják.

b) **II. eljárás**

Ott ahol csak egy riasztás jelzést küldenek a felügyelt területről, azt a riasztásfogadó központ folyamat által igazolt riasztás állapotként azonosítja. (A felügyelt területek vezérlő és kijelző berendezése két önálló, egymástól független riasztás állapotot vesz a behatolás és támadásjelző rendszertől, és ezeket egyesítve küldi el a riasztásfogadó központnak a folyamat által igazolt riasztás jelzést).

Ha a riasztásfogadó központ egy „C” riasztás jelzést kap, amelyet a riasztásfogadó központ a védett területen folyamat által igazolt riasztás állapot meglétéről szóló jelentésként azonosított, akkor a riasztásfogadó központnak a „C” jelzést folyamat által igazolt riasztás jelzésnek kell tekintenie.

c) **III. eljárás**

Átviteli hibák (több átjelző vonallal rendelkező behatolás és támadásjelző rendszertől eredő) és hibaállapotok kezelhetők úgy, mint az I. eljárás első „A” jelzése, a folyamat általi igazolás módszerének megfelelően.

A.4.2. Vizuálisan igazolt riasztás

Ahhoz, hogy egy riasztás állapot vizuálisan igazolt legyen, a riasztásfogadó központ ügyeletesének legalább 30 másodperc (de az A.2 pontban meghatározott időparamétereken belül) alatt eleget kell tennie a következőknek, ha nincs ezt megelőző bizonyító információ:

a) A riasztásfogadó központ ügyeletesének közvetlenül, azonos időben kell látnia a felügyelt területről továbbított képeket; és/vagy
b) A képeket a riasztásfogadó központban üzemelő képfelvevő berendezéssel rögzíteni kell és a riasztásfogadó központ ügyeletese nézi vissza a felvett kép(ek)et; és/vagy
c) A képeket a felügyelt területen a behatolás és támadásjelző rendszer képfelvevő berendezésével kell rögzíteni, és a riasztásfogadó központ ügyeletese nézi vissza a felvett kép(ek)et.

Amint a riasztásfogadó központ ügyeletese a vonatkozó utasításoknak megfelelően eldönti, hogy a felügyelt területről kapott képek megerősítik azt, hogy a felügyelt területen valós behatolás vagy valós behatolási kísérlet történt, a riasztás jelzést vizuálisan igazolt riasztás jelzésnek kell minősíteni.

A.4.3. Hallás útján igazolt riasztás

Ahhoz, hogy egy riasztás állapot a riasztásfogadó központban hallás útján igazolható legyen, a felügyelt területeken egy vagy több mikrofont be kell kapcsolni és a belehallgatási periódusnak legalább. 30 másodpercig kell tartania, a következőkben megadottak szerint vagy előzetes bizonyító információ szükséges:

a) A riasztásfogadó központ ügyeletesének közvetlenül azonos időben kell lehallgatnia a felügyelt területről átvitt hangokat; és/vagy
b) A hanganyagot a riasztásfogadó központban üzemelő hangfelvevő berendezéssel rögzíteni kell és a riasztásfogadó központ ügyeletese hallgatja vissza a felvételt; és/vagy
c) A hanganyagot a felügyelt területen a behatolás és támadásjelző rendszer hangfelvevő berendezésével kell rögzíteni és a riasztásfogadó központ ügyeletese hallgatja vissza a felvételt.

Amint a riasztásfogadó és riasztás-felügyeleti központ ügyeletese a vonatkozó utasításoknak megfelelően eldönti, hogy a felügyelt területről kapott hanganyag megerősíti azt, hogy a felügyelt területen valós behatolás vagy valós behatolási kísérlet történt, a riasztás jelzést hallás útján igazolt riasztás jelzésnek kell minősíteni.

A.4.4. Ügyfél ill. felhasználó által igazolt riasztás

Ahhoz, hogy egy riasztás állapot a szerződő fél ill. a felhasználó által legyen igazolt, a riasztásfogadó központ megköveteli hogy az ügyfél ill. felhasználó típusú hitelesítést a megfelelően felhatalmazott szerződő fél ill. egy felhasználó vagy a szerződő fél ill. a felhasználó biztonsági őrei (kivonuló szolgálat) végezzék.

Ebben az esetben a riasztásfogadó központ csak a szerződő féllel vagy a felhasználóval vagy a felügyelt területeken szolgálatot teljesítő biztonsági őrrel lép kapcsolatba, aki megállapítja a riasztás állapot okát és hamisnak vagy valósnak minősíti.

Az ügyfeleknek legalább két olyan kapcsolattartó személy nevét kell megadniuk a riasztásfogadó központnak, akik képesek arra, hogy rendelkezésre álljanak és rendelkezésre is állnak a felügyelt területen, a riasztásfogadó központból kapott hívás után, általában 30 percen belül, továbbá rendelkeznek kulccsal és képesek hatástalanítani a riasztórendszer