V tomto dokumente sú uvedené všeobecné informácie potrebné na špecifikáciu technických požiadaviek na vypracovanie projektovej dokumentácie SBT.

Všeobecné požiadavky na bezpečnostné mechanické zábranné prostriedky

Požiadavky na bezpečnostné triedy (dvere/gátre):

Bezpečnostné dvere musia byť odolné proti vlámaniu. Je to vlastnosť dverí odolávať pokusu o násilný vstup do chráneného priestoru použitím fyzickej sily a s pomocou náradia.

Bezpečnosť dverí sa deklaruje certifikátom vydaným autorizovanou skúšobňou. Certifikát v slovenskom alebo v českom jazyku. Bezpečnostné dvere musia spĺňať požiadavky podľa noriem STN EN 1627-1630. Cylindrické vložky musia spĺňať požiadavky normy STN EN 1303. Pripúšťajú sa ekvivalentné normy. Norma stanovuje odolnosť dverí do príslušných bezpečnostných tried od 1 po 6. Pred samotnou skúškou odolnosti proti ručnému pokusu o vlámanie musia dvere prejsť ešte statickou a dynamickou skúškou.

Fyzikálne vlastnosti stavebných materiálov a konštrukcií by mali byť adekvátne a zodpovedať triede mechanickej zábrany.

Prechodové/deliace gátre/dvere (interiér) musia byť minimálne v bezpečnostnej triede 3. Ak sa jedná o dvere, musia byť naviac požiarne odolné (špecifikáciu by mal dodať špecialista požiarnej ochrany). Tento typ prechodových/deliacich gátrov/dvier bude vybavený kovaním v príslušnej bezpečnostnej triede v kombinácii guľa/kľučka podľa požiadaviek zákazníka a lokalizácie mechanickej zábrany. Zároveň budú vybavené elektrickým zámkom na ich ovládanie, vstupným a kontrolným systémom so svetelnou signalizáciou stavu prechodového/deliaceho gátra/dvier (odomknuté/zamknuté). Elektrický zámok musí vedieť signalizovať stav – zamknuté/odomknuté. Prechodové/deliace gátre/dvere budú vybavené polarizovanými magnetmi na snímanie polohy (otvorené/zatvorené) – skrytá montáž, neprístupná pri zatvorenej mechanickej zábrane. Súčasť zámku musí byť vložka/pol vložka so systémom generálneho kľúča (pre núdzové otvorenie mechanickej zábrany, ktorá bude signalizovaná ako násilné otvorenie).

Dvere na perimetri budovy (obvodovom plášti-exteriér) musia byť rovnako minimálne bezpečnostnej triedy 3, požiarne odolné (špecifikáciu by mal dodať špecialista požiarnej ochrany). Tieto bezpečnostné dvere obsahujú oceľové platne, oceľový rám a oceľovú výstuž po celom obvode dverí. Celá konštrukcia dverí je pevná a masívna, doplnená o tepelno-zvukovo izolačné parametre. Kovanie v príslušnej bezpečnostnej triede v kombinácii guľa/kľučka podľa požiadaviek zákazníka a lokalizácie dvier. Zároveň budú vybavené elektrickým zámkom na ich ovládanie, vstupným a kontrolným systémom so svetelnou signalizáciou stavu dvier (odomknuté/zamknuté). Elektrický zámok musí vedieť signalizovať stav – zamknuté/odomknuté. Dvere budú vybavené polarizovanými magnetmi na snímanie polohy zábrany (otvorené/zatvorené) – skrytá montáž, neprístupná pri zatvorenej mechanickej zábrane. Súčasť zámku musí byť vložka/pol vložka so systémom generálneho kľúča (pre núdzové otvorenie mechanickej zábrany, ktorá bude signalizovaná ako násilné otvorenie).

Celové dvere má oddelenie logistiky (v spolupráci s Referátom bezpečnosti pri práci a požiarnej ochrany) vyšpecifikované a disponuje konštrukčnou dokumentáciou, za ***SIKT:*** dvere aj vnútorné gátre (ak budú osadené) budú odomykané mechanicky systémom generálneho kľúča. Celové dvere aj vnútorné gátre budú vybavené polarizovanými magnetmi na snímanie polohy (otvorené/zatvorené) – skrytá montáž, neprístupná pri zatvorenej mechanickej zábrane. Zároveň bude osadený kontakt na signalizáciu zamknuté/odomknuté.

Dvere na miestach so zvýšeným bezpečnostným rizikom (serverovňa, strážne stanovište a pod.) musia byť minimálne bezpečnostnej triedy 3, požiarne odolné (špecifikáciu by mal dodať špecialista požiarnej ochrany). Typ dverí (interiér/exteriér) určí celková dispozícia priestorov akceptujúc bezpečnostné riziká. Celá konštrukcia dverí je pevná a masívna, doplnená o tepelno-zvukovo izolačné parametre. Kovanie v príslušnej bezpečnostnej triede v kombinácii guľa/kľučka podľa požiadaviek zákazníka a lokalizácie dvier. Tento typ dvier je ovládaný mechanicky systémom generálneho kľúča. Dvere budú vybavené polarizovanými magnetmi na snímanie polohy zábrany (otvorené/zatvorené) – skrytá montáž, neprístupná pri zatvorenej mechanickej zábrane. Zároveň bude osadený kontakt na signalizáciu zamknuté/odomknuté.

Dodatočne môžu byť vybavené polarizovanými magnetmi na snímanie polohy (otvorené/zatvorené) – skrytá montáž, neprístupná pri zatvorenej mechanickej zábrane aj iné interiérové dvere, resp. deliace mreže (napr. „predokenné“ mreže, deliace mreže).

Príjazdová cesta pre vjazd/výjazd vozidiel do/zo zariadenia pri obj. č. 22 – Sociálna budova ÚOA musí byť vybavená cestným blokátorom v celej šírke vjazdovej/výjazdovej brány. Blokátor musí byť certifikovaný min. PAS 68 V/7500(N2)/80/90:0/1.2 alebo IWA 14-1 IWA 14-1 Bollard V/7200(N2A)/64/90/1.2 (prípustné sú aj ekvivalentné normy). Certifikát musí byť vydaný autorizovanou skúšobňou. Súčasťou musí byť svetelné výstražné a signalizačné zariadenie, tzv. „semafór“.

Príjazdová brána pre vjazd/výjazd vozidiel do/zo zariadenia musí byť vybavená snímačmi otvorenia/zatvorenia a ovládanie pohonu musí umožniť vzájomné blokovanie podľa požiadaviek zákazníka.

Všeobecné pojmy pre bezpečnostnú časť (zariadenie musí obsahovať):

SBT – Signálno-bezpečnostná technika
IBS – Integrovaný bezpečnostný systém
CCTV – Kamerový systém
VaKS – Vstupný a kontrolný systém
SKH – Systém komunikačných hlások
ŠK – Štruktúrovaná kabeláž
DR – Drôtový rozhlas
ER – Evakuačný rozhlas
EPS – Elektrická požiarna signalizácia
EZS – Elektrický zabezpečovací systém
STA – Spoločná televízna anténa
Ak nie sú vznesené požiadavky na podsystémy nižšie, platia požiadavky noriem a všeobecných záväzných predpisov.

Minimálne požiadavky k SBT (súbor všetkých systémov a podsystémov určených pre bezpečnostné aplikácie):

- bežná dostupnosť riešenia a použitých komponentov na trhu prostredníctvom viacerých partnerov (nie výhradnosť, jedinečnosť a pod.),
- kvalita použitých komponentov (riešenia overené rozsiahlymi a náročnými inštaláciami),
- stabilita, vysoká dostupnosť, hardvérová redundancia,
- jednoduché a rýchle hľadanie v záznamoch, logoch,
- priaznivá licenčná politika počas životnosti zariadenia,
- nasadenie vo väzenskom prostredí,
- otvorené SDK (API) a možnosť integrácie existujúcich IT technológií zákazníka,
- kontinualita existujúcich systémov používaných u zákazníka.

Z hľadiska bezpečnosti platí pravidlo, že každý systém musí byť nezávisle funkčný voči nadstavbovému systému aby v prípade zlyhania bolo možné systém ovládať cez ovládacie panely, či iné riadiace moduly.

Základné normy a legislatíva:

STN 34 2300 Predpisy pre vnútorné oznamovacie vedenia
STN 33 2000-1 Elektrické inštalácie budov. Časť 1: Rozsah platnosti, účel a základné princípy
STN 33 2000-3 Elektrické inštalácie budov. Časť 3: Stanovenie základných charakteristík
STN 33 2000-5-52 Elektrické inštalácie budov. Časť 5: Výber a stavba elektrického zariadenia. Kap.52: Rozvody
STN 33 2000-5-54 Elektrické inštalácie budov. Časť 5: Výber a stavba elektrického zariadenia. Kap.54: Uzemňovacie sústavy a ochranné vodiče
STN 33 2000-4-43 Elektrické inštalácie budov. Časť 4: Zaistenie bezpečnosti Kap.43: Ochrana proti nadprúdom
STN 33 2000-4-473 Elektrické inštalácie budov. Časť 4: Zaistenie bezpečnosti Kap.47: Použitie ochranných opatrení pre zaistenie bezpečnosti.
STN 33 2000-5-523(2004) Elektrické inštalácie budov, Časť 5: Výber a stavba DEZ, Oddiel 523: Prúdová zaťažiteľnosť elektrických rozvodov
STN 33 2000-5-51(2007) Elektrotechnické predpisy – EZ – Časť 5: Výber a stavba EZ Kap.51: Všeobecné predpisy
STN 33 2000-4-41(2007) Elektrické inštalácie budov. Časť 4: Zaistenie bezpečnosti. Kap.41: Ochrana pred zásahom elektrickým prúdom
STN EN 50131 Poplachové systémy. Elektrické zabezpečovacie a tiesňové poplachové systémy
STN EN 50134 Poplachové systémy. Systémy privolania pomoci
STN EN 50136 Poplachové systémy. Poplachové prenosové systémy a zariadenia
STN EN 50173-1 (ISO/IEC 11801 2nd Edition) Základná medzinárodná norma o univerzálnych štruktúrovaných kabelážnych systémoch pre prenos dát, telefónie, obrazu a iných nízkonapäťových signálov v budovách a areáloch
STN EN 50174-1 Informačná technika. Inštalácie káblových rozvodov.
STN EN 50174-2 Informačná technika. Inštalácie káblových rozvodov.
STN EN 50174-3 Informačná technika. Inštalácie káblových rozvodov.
STN EN 50310 Použitie pospájania a uzemnenia v budovách so zariadeniami informačnej techniky.
STN EN 50346 Informačná technika. Káblové rozvody. Skúšanie inštalovaných káblových rozvodov.
STN 92 0203 Požiarna bezpečnosť stavieb. Trvalá dodávka elektrickej energie pri požiari.
STN 33 2000-6-61 Východisková revízia
Vyhláška MPSVaR SR č. 508/2009 Z. z. na zaistenie bezpečnosti a ochrany zdravia pri práci a bezpečnosti technických zariadení,
Vyhláška MV SR č. 94/2004 Z. z., ktorou sa ustanovujú technické požiadavky na požiarnu bezpečnosť pri výstavbe a pri užívaní stavieb,
Zákon 473/2005 Z.z.
Vyhláška MV SR č.634/2005

Projekt skutočného vyhotovenia (konštrukčná dokumentácia) musia byť vyhotovená v stupni utajenia „Vyhradené“.

Technické riešenie objektov:

Elektrický zabezpečovací systém EZS a Vstupný a kontrolný systém (VaKS)

Hybridný bezpečnostný systém s integrovaným prístupovým systémom (vstupný a kontrolný systém). Všetky prvky, ktoré zabezpečujú signalizáciu narušenia, otvorenia, pohybu, požiaru atď. sú pripojené prostredníctvom expandérov komunikujúcich cez zbernicu do hardvérovo redundantných ústrední. Ústredne sú veľkokapacitné a sú nakonfigurované podľa potreby zákazníka, prípadne iných bezpečnostných smerníc. Ovládajú sa cez klávesnice, v prípade riadenia prístupu cez čítačky RFID a pod.. Vzhľadom na predpokladaný rozsah môže byť ovládanie cez klávesnice užívateľsky náročné a neprehľadné (najmä na operačnom stredisku), musí byť tento systém integrovaný do nadstavbového riadiaceho softvéru. Tento systém patrí medzi hlavný bezpečnostný systém. Používa sa aj na riadenie prístupu, nakoľko umožňuje pripojiť moduly na ovládanie prechodov, dverí, turniketov atď. Je nevyhnutné používať funkciu prístupu v rámci ústredne, nakoľko sa dajú väzby medzi stavmi zabezpečovacej a prístupovej časti jednoducho naprogramovať na základe spoločnej hardvérovo softvérovej úrovni. Jedná sa o rôzne blokácie (či iné funkčné previazania) v prípade poplachov či iných stavoch bezpečnostného systému, čo je pre potreby zboru žiadúce. Súčasťou bezpečnostného systému sú aj rôzne druhy perimetrických ochrán, ktoré sú pripojené do zabezpečovacieho systému a zároveň integrované do nadstavbového bezpečnostného systému. Elektrický zabezpečovací systém (EZS – ústredňa) musí mať certifikáciu minimálne na stupeň 4. Zbernice EZS musia byť riešené kruhovou topológiou. Vedenie zbernice EZS musí byť riešené v chránených káblových trasách. Rozširujúce moduly, napájacie zdroje a istiace prvky v jednotlivých objektoch musia byť osadené v uzamykateľných rozvádzačoch (buď v oceľovej skrini, alebo v 19“racku v serverovni) chránené minimálne tamperom. Zbernice musia byť chránené na vstupe aj výstupe izolátormi zbernice alebo inou vhodnou technológiou. Izolátor zbernice je požadovaný na oddelenie úsekov kruhovej linky pri poruche úseku spôsobenej napríklad skratom na dátovom vedení. Prechody zbernice medzi jednotlivými budovami, ako aj vedenia zbernice k podružným rozvádzačom, budú vybavené ochranou proti prepätiu. Pre ovládanie systému budú na určených miestach osadené LCD klávesnice. EZS musí byť nezávislá na IBS a musí vedieť samostatne fungovať. EZS musí podporovať viacero typov vyvažovania koncových prvkov a viacero typov komunikačných rozhraní. Signalizované prostredníctvom EZS sú spravidla záujmové miesta, rozvádzače, rôzne výplne (dvere, okná, mreže) a v rámci vnútornej bezpečnosti sa tiež používajú PANIC tlačidlá (primerane na chodby, skrytá montáž do kancelárskych priestorov a pod.).

Vstupný a kontrolný systém

Bude spravidla pri každom prechodovom/deliacom gátri/dverách (interiér) ako aj dverách na perimetri budov (exteriér). Štandardne bude obsahovať funkciu anti-passback. Zákazník osadenie špecifikuje podľa celkovej dispozície priestorov akceptujúc bezpečnostné riziká. Vstupný a kontrolný systém (VaKS) - vedenie (napájanie/data) k zámkom, kontaktom, snímačom a čítačkám bude v prevedení antivandal – v celej dĺžke musí byť vedené v kovovej konštrukcii. Pre identifikáciu a signalizáciu stavu elektronicky ovládaných dverí a zámku, bude na dverách nainštalovaná optická signalizácia. Všetky prepojovacie skrinky pre kabeláže budú vybavené sabotážnym kontaktom, rovnako ako ústredne EZS, RACK-y a pod..

Vzhľadom na charakter objektu elektro motorické/magnetické zámky zostanú v prípade výpadku resp. poruchy napájania v uzamknutom stave. Bude ich možné otvoriť len mechanicky bez použitia nástroja prostredníctvom vložky zámku so systémom generálneho kľúča. Pre otváranie dverných prechodov a dverí v celom objekte musia byť použité aspoň bezkontaktné prístupové čítačky pre bezkontaktné elektronické karty minimálne typu MIFARE iCLASS SE, MIFARE Classic, DESFire EV1. Komunikácia musí prebiehať po dvojvodiči. Čítačky musia byť dodané v prevedení podľa typu určeného prostredia (exteriér/interiér) a podporovať zvukovú a optickú signalizáciu.

Súčasné otvorenie vstupov a prechodov tvoriacich kľúčové oblastí (vonkajšie brány a dvere) bude navzájom systémovo blokované. Súčasné otvorenie vymedzených dverí, ktoré tvoria vstupný koridor môže byť realizované len pri povolení právomocí z nadradeného systému IBS alebo klávesnice EZS z miesta určeného zákazníkom.

Systém komunikačných hlások (SKH) vrátane prepážkových systémov a bezkontaktných návštev, ***Drôtový rozhlas (DR)***, ***Evakuačný rozhlas (ER)***

Komunikačné systémy sú tvorené komunikačnými zariadeniami pre komunikáciu klient / obsluha (prípadne klient s návštevou, návšteva s obsluhou, alebo medzi záujmovými pracoviskami). Komunikačné systémy sú vytvorené špeciálne pre účely väzenských priestorov (zvýšená odolnosť, vyššia akustika, prevádzka 24/7 a pod.). Systémy určené a vyvíjané do väzenského prostredia. Komunikačné terminály budú všade tam, kde je vyžadovaná bezkontaktná komunikácia (napr. bezkontaktné návštevy, hlavný chod a pod.). Zároveň budú strategicky rozmiestňované na chodbách, spoločných priestoroch a pri vstupných a prechodových gátroch/dverách tak aby mohli dopĺňať, alebo suplovať tiesňové tlačidlá. Primárne budú komunikačné terminály dislokované v celách, kultúrnych miestnostiach, chodby, spojovacie trakty, jedálne, vychádzkové dvory a pracoviskách referentov režimu, pracoviskách pre väznené osoby, na strážnych stanovištiach. Nad každou celou/celovými dverami bude optická signalizácia, ktorá signalizuje stavy celovej hlásky (porucha, žiadosť o hovor, PANIC dozorca). V celom systéme bude možné realizovať presmerovania podľa požiadaviek zákazníka (nútené, plánované a pod.).

Základnou úrovňou je komunikačný terminál – „Hláska“ v prevedení:

- izbová/celová hláska,
- „SOS“ hláska (chodbová),
- prepážkový terminál
- terminál pre operátora,
- terminál pre referentov režimu/strážne stanoviská.

Hláska umožňuje prenos audio, signalizácie a stavu na príslušné pracovisko podľa požiadaviek zákazníka (hovor z izby/cely, aj tiesňové volanie, v prípade prítomnosti personálu na izbe/cele „Panic dozorca“). Komunikačný server bude dohliadaný a monitorovaný z operačného pracoviska. Mechanická konštrukcia hlások je mechanicky vysoko odolná (IK10). Konštrukcia hlásky musí zabezpečiť vysokú odolnosť voči úmyselnému poškodeniu reproduktora/mikrofónu (pred vniknutím ostrého predmetu) a rovnako aj senzorov signalizujúcich snahu o vypáčenie predného panelu.

Vybrané pracoviská budú vybavené terminálom displejom a programovateľnými tlačidlami. Terminál obsahuje externý mikrofón, multifunkčný modul, ktorý obsahuje funkčné tlačidlá, číselník s displejom pre zobrazovanie stavových informácií a príslušný počet tlačidlových modulov s voľne programovateľnými tlačidlami, ktoré umožňujú priamu voľbu účastníka alebo skupiny účastníkov. Systém SKH musí fungovať autonómne a musí byť nezávislý na IBS.

Hovory z hlásky

Prichádzajúci hovor je opticky signalizovaný na displeji terminálu alebo graficky zmenou farby ikony na monitore dohľadového PC klienta spolu s akustickou signalizáciou. Prijatie hovoru je možné uskutočniť zatlačením príslušného tlačidla, alebo kliknutím na príslušnú hlásku na monitore PC. Hlasová komunikácia môže byť vedená v auto half-duplexnom alebo simplexnom móde, ktorý ovláda obsluha z dohľadového/riadiaceho terminálu. Hovor je prerušený obsluhou z pultu. V prípade viacerých súčasných hovorov sú tieto radené do fronty postupne za sebou. Priorizované budú núdzové a SOS hlásenia. Obsluha si môže vybrať zatlačením príslušného tlačidla na pulte alebo kliknutím na ikonu príslušnej hlásky, ktorý hovor v akom poradí vybaví.

Tiesňový hovor z hlásky

Signalizácia tiesňového hovoru dozorcu z cely stlačením senzorového panela hlásky je zvýraznená blikaním na displeji terminálu, alebo graficky blikaním ikony plus poplachovou správou na monitore dohľadového PC klienta. Prijatie tiesňového hovoru je podobné ako pri štandardnom hovore. Následne je uskutočnené spojenie s hláskou.

Žiadosť o hovor z inej hlásky

Pri zatlačení hovorového tlačidla na hláske je táto požiadavka signalizovaná na príslušnom dohľadovom pracovisku. Obsluha tento štandardný hovor nemusí prijať, v tomto prípade sa po prednastavenom čase presmeruje hovor na ďalšiu riadiacu hlásku. Obsluha môže hovor zamietnuť.

Hovory s hláskou

Z príslušného dohľadového pracoviska je možné uskutočniť priamy hovor s hláskou prostredníctvom voľby čísla hlásky z číselníka, zatlačením tlačidla priamej voľby na pulte alebo kliknutím na ikonu hlásky v PC. V hláske je hovor automaticky prijatý. Hlasová komunikácia môže prebiehať v simplexnom alebo auto half-duplexnom móde.

Signalizácia sabotáže

Sabotáž - napr. pokus o poškodenie hlásky - môže byť signalizovaná na displeji terminálu, alebo poplachovou správou na monitore dohľadového PC. Súčasne je akusticky signalizovaná tým istým tónom ako klasický hovor na príslušnom pracovisku. Signalizácia sabotáže je indikovaná aj v nadstavbovom softvéri IBS.

Skupinové oznamy a hlásenia

Z dohľadového pracoviska alebo z operačného pracoviska je možné uskutočniť skupinové oznamy a hlásenia pre príslušné hlásky na podlaží alebo pre celý objekt.

Signalizácia porúch

Jednotlivé terminály musia byť systémom nepretržite kontrolované a dohľadované. Na operačnom pracovisku je automaticky signalizovaná porucha každej hlásky alebo vedenia a to na každej úrovni - či je to na vedení k hláske v cele alebo na vedení medzi budovami, cez ktoré sú hlásky pripojené.

Funkcia drôtového rozhlasu

Celová hláska umožňuje príjem audio signálu a jeho reprodukciu cez reproduktor hlásky. Funkciu drôtového rozhlasu je možné zapnúť alebo vypnúť (povoliť alebo zakázať) pre každý terminál v izbe samostatne na diaľku z pultu príslušného pracoviska.

Záznam a archivácia hlasovej komunikácie

Komunikačný systém musí umožňovať zaznamenávať a archivovať všetku hlasovú komunikáciu v systéme - pre vybrané koncové zariadenia (hlásky, dohľadové pracoviská) s funkciou zaznamenania meta údajov (čas, číslo hlásky a pod.) v rozsahu min. 3 mesiace.

Vysielanie hlasových oznamov s prioritou

Systém umožňuje vysielanie vopred nahratých správ alebo oznamov kombinovaním viacerých zvukových súborov (texty, tóny), spustenie vysielania samostatného oznamu alebo sekvencie správ z komunikačného systému (hlásky, dispečerského pultu), možnosť vysielania oznamov na jednotlivých hláskach alebo na skupinách hlások.

Integrácia so systémom ozvučenia

Komunikačný systém umožňuje pripojiť systém ozvučenia - evakuačný rozhlas a ovládať jeho funkcie z operačného pracoviska alebo z oprávnených koncových terminálov - hlások. Integrácia komunikačného systému a systému ozvučenia umožňuje efektívne a rýchlo vyhlasovať oznamy, hlásenia z oprávnených hlások do celého systému alebo len do určených zón - napr. z centrálneho dohľadového pracoviska je možné uskutočniť hlásenia v celom areáli zariadenia, z dohľadového pracoviska úseku len na príslušnom úseku a pod. Výhodou integrácie je, že ako koncové zariadenia - reproduktory pre hlasové oznamy slúžia nielen reproduktory systému ozvučenia, ale aj koncové zariadenia - hlásky - integrovaného

bezpečnostného komunikačného systému. Tým je možné optimalizovať náklady na systém ozvučenia a lepšie pokryť jednotlivé priestory a objekty.

Kamerový systém CCTV

V jednotlivých objektoch musí byť inštalovaný kamerový systém tak, aby bol zabezpečený celkový prehľad o okolí a v jednotlivých objektoch ideálne bez „hluchých priestorov“. Monitorovacie systémy majú architektúru klient/server (monitorovacie zariadenie – prenosová cesta – server), záznamy sú ukladané na serveroch. K serverom sú pripojený aj jednotlivý užívatelia na základe oprávnení prostredníctvom klientov. Systém podporuje FAIL OVER funkciu v prípade výpadku serveru. Systém je hardvérovo prepojený s bezpečnostným systémom EZS a SKH tak, aby v prípade poplachu/žiadosti o komunikáciu dostal na základe nastavenia príkazy na zobrazenie predprogramovaných kamier. Systém je rovnako integrovaný do nadstavbového systému pre zjednodušenie prehľadu a ovládania užívateľa. Uplatňujú sa funkcie video analýzy, face recognize a pod. pre zvýšenie bezpečnosti monitorovaných priestorov.

Pri komunikácii medzi kamerou a serverom je použitá minimálne možnosť ochrany dát 256 bitovým šifrovaním komunikácie a TLS protokolom. Podpora kamier od 1 do 30 mpx, ako aj termokamier, otočných kamier (PTZ), video vrátnikov a multisenzorových kamier. Licencie sú doživotné a nemajú žiadnu exspiráciu, to znamená že zákazník nemusí kupovať softvér znova po x rokoch. Podporovať musí:

- pravidlo 4 očí,
- prístup užívateľov len k sekundárnemu streamu,
- prístup užívateľov k záznamu len od doby zalogovania,
- dvojfaktorové overovanie užívateľov, meno + heslo a číselný kód z prideleného telefónu, ktorý sa automaticky mení každých 30 sekúnd,
- možnosť prepojenia softwaru s Active directory, pre efektívnejšiu správu užívateľov,
- HDSM technológia ktorá zabezpečí zníženie prenosu dát medzi klientom a serverom až o 80% čo samozrejme ovplyvňuje nároky na počítačovú sieť ako aj nároky na klientske stanice,
- analýza, rozpoznávanie objektov sa spracováva priamo na kamere, takže nezaťažuje analýzou samotný server,
- kamera určí o aký pohybujúci objekt sa jedná,
- podpora analýz aj na termokamerách a to do vzdialenosti až 200 metrov (podľa typu kamery),
- systém má možnosť zapínanie a vypínania stráženia po jednotlivých úsekoch, alebo skupinách úsekov,
- obsahujú vstavený IR prísvit (min. na 30m) pre zabezpečenie snímania aj v nočných podmienkach,
- vstup/výstup pre pripojenie externého zariadenia,
- ochrana min.IP66 a IK10,
- vysoký rozsah teplôt (min. -25° až +50°), s funkciou aktívneho duálneho napájania t.j. môže byť pripojené POE aj 12VDC/24VAC naraz pre prípad potreby zvýšenia spoľahlivosti a bezpečnosti systému,
- ONVIF kompatibilita.

Ďalej musí podporovať jednoduché a rýchle vyhľadávania, s možnosťou prehľadávania dlhších úsekov ako 1 deň:

a. podľa zmeny pixelov,
b. alarmov/logov pohybu,
c. pribudnutého alebo zmiznutého objektu (ponechaná batožina/predmet).

Možnosť vytvoriť virtuálnu maticu z neobmedzeným počtom monitorov a zároveň ovládať celý systém pomocou jednej klávesnice. Vytvorenie matice nevyžaduje žiadny proprietárny HW. Na virtuálnej matici môže operátor sledovať kamery, zobrazovať mapové podklady ako aj web stránky alebo rozhranie zariadení tretích strán ktoré majú k dispozícií webové rozhranie.

Operátory majú možnosť využívania „Alarmového pohľadu“ kde nesledujú všetky kamery, ale len alarmové stavy z kamier. Tento „Alarmový pohľad“ môže byť umiestnený na jednom z monitorov zatiaľ čo ostatné monitory budú zobrazovať živý obraz z kamier.

Kamerový systém (CCTV) – IP kamerový systém so zapracovanou digitálnou analýzou obrazu. Systém zároveň musí podporovať face recognition, čítanie EČV a pod.. Prepojenie kamier bude zrealizované na samostatnej sieťovej vrstve dátovej siete pre kamerový systém. Toto prepojenie zabezpečí úplnú autonómnosť a funkčnosť aj pri výpadku nadradeného integračného systému.

Situácia rozmiestnenia CCTV

Vonkajší perimeter jednotlivých objektov bude nepretržite monitorované statickými kamerami s IR prisvietením umiestnenými tak, aby nedochádzalo k mŕtvym uhlom. Účelom je zabezpečiť určené priestory hybridným bezpečnostným systémom trvalého monitoringu 24/7, ktorý jednak zabezpečí vizuálnu formu monitorovania vybraných úsekov na operačnom stredisku – prenosom video streamov na zobrazovacie panely, tak aj vyhodnotenie narušenia (alarmov) z definovaných priestorov formou analytických funkcií monitorovacieho systému s následným vizuálnym zobrazením poplachu z konkrétnej oblasti. Doplnený bude o PTZ, ktoré sa v prípade poplachu nasmerujú na definovaný úsek.

Priestor za ohradným múrom (okolie väzenského zariadenia) bude nepretržite monitorované otočnými PTZ kamerami s laserovým prisvietením osadenými na vonkajšej strane múru na príslušných výložníkoch a adaptéroch tak, aby bol zabezpečený celkový okamžitý prehľad z vonkajšej strany zariadenia.

Vnútroareálové priestory budú monitorované prehľadovými statickými kamerami s IR prisvietením doplnenými o otočné PTZ kamery s laserovým prisvietením osadenými tak, aby bol zabezpečený komplexný prehľad o vnútornej situácii.

Na vstupoch do objektov budú osadené antivandal statické fish-eye kamery s IR prisvietením na zabezpečenie prehľadu vstupujúcich a vystupujúcich osôb z a do objektov. Monitorovaný bude aj priestor vstupu pre peších a vjazdu pre motorové vozidlá tak, aby bolo možné identifikovať a vyhodnocovať činnosti v záujmovom priestore, alternatívne použitie face recongition, čítanie EČV vozidiel. Kamerovým systémom bude rovnako vybavený každý gáter/dvere (obojsmerne) ovládané VaKS/signalizované EZS.

Kamerovým systémom budú monitorované aj cely špecializovaného zaobchádzania, všetky chodby a schodiská a iné záujmové priestory. Zákazník určí záujmové priestory dodatočne vybavené CCTV, kde môže prichádzať ku styku obsluhy s väznenými osobami.

Systém musí automaticky nastavovať odosielané rozlíšenie medzi serverom a klientom na základe požiadavky klienta tak, aby bolo zabezpečené rovnomerné vyťažovanie siete aj pri kamerách s ultra vysokým rozlíšením (4K a viac).

Musí podporovať vyhľadávania osôb v celom zázname kamerového systému na základe údajov analytických kamier a digitálneho podpisu vytvoreného serverom, pre rýchle a zjednodušené dohľadávanie záujmovej osoby alebo vozidla aj na viacerých pripojených fyzických lokalitách súčasne.

Záznam, vyhodnocovanie analýz z monitorovaných priestorov, ukladanie záznamu, pripájanie klientských pracovísk, riadenie dátových tokov, zabezpečuje výkonný server s predinštalovaným monitorovacím systémom, vrátane všetkých potrebných licencií (softvérových, analytických, záznamových, databázových atď.)

Systém musí umožňovať pripojenie neobmedzujúce počtu bezplatných klientov v závislosti od výkonu servera a dátovej infraštruktúry.

Systém musí umožňovať integráciu do Integrovaného bezpečnostného systému (nadstavbového informačného systému) pre účely centralizácie riešenia, získavania dostupných dát (logy udalostí zo systému) za účelom ďalšieho spracovávania a vyhodnocovania. Aj v prípade integrácie systém musí fungovať úplne nezávisle od nadstavbového systému.

Sieťová bezpečnosť kamier - ochrana prístupu heslom, šifrovanie HTTPS, logovanie prihlásenia užívateľa, podpora protokolu 802.1x, WS autentifikácia.

Kapacita diskového úložiska dimenzovaná minimálne na 3 mesačný nepretržitý záznam zo všetkých kamier, z toho v pomere minimálne 1 mesiac hlavný stream a 2 mesiace sekundárny. Možnosť uzamknúť záznam operátorom/administrátorom.

Ďalšie požadované parametre monitorovacieho a záznamového systému :

- podpora kodekov min. MJPEG, H.264,
- neobmedzený počet kamier v jednom systéme,
- neobmedzený počet klientov v jednom systéme,
- možnosť spravovať neobmedzený počet serverov z jedného klienta,
- možnosť prihlásiť sa na neobmedzený počet serverov súčasne ako klient,
- možnosť zvoliť si ľubovoľnú kameru z ľubovoľného servera súčasne na jednom klientskom PC,
- plná podpora slovenského jazyka,
- software Onvif kompatibilný,
- automatický upgrade firmwéru na kamerách a verzie softvéru klientskych PC,
- možnosť upgradovania serverov na diaľku,
- možnosť automatického zálohového nahrávania kamier na druhý, tretí server pri výpadku spojenia so serverom alebo pri poruche servera, možnosť redundantého nahrávania kamier,
- možnosť nahrávať kamery až do rozlíšenia 30Mpx,
- možnosť zobraziť obraz na iOS alebo Android zariadeniach s využívaním digitálneho zoomovania,
- možnosť nahrávať až 60fps,
- pomoc pri vyhľadávaní/riešení udalosti na vzdialenej ploche bez použitia softwaru tretích strán - kooperácia medzi prihlásenými užívateľmi v systéme,
- možnosť nahrávať súčasne primárny aj sekundárny stream (v min. rozlíšení CIF) pri použití kodeku H264,
- možnosť nastaviť premazávanie primárneho streamu a nahradenie daného záznamu záznamom v CIF rozlíšení, pre získanie dlhšej doby záznamu pri použití kodeku H264,
- systém musí umožniť nižšiu kvalitu záznamu pre streamy bez zaznamenanej detekcie pohybu,
- systém zvládne posun času späť alebo dopredu pri zmene letného a zimného času bez straty dát,
- možnosť exportu záznamu v rôznych formátoch, napr.: AVI, JPEG, TIFF, PNG, WAV a iné,
- možnosť multi-exportu viacero kamier a viacerých časových úsekov do jedného súboru,
- možnosť vytvorenia vlastných zvukových správ, ktoré sa spustia automaticky pri vyvolaní alarmu,

- možnosť ovládať relé výstupy na kamerách pomocou klientského softwaru,
- možnosť zmeniť dátový tok zo servera na klientsky počítač priamo na klientskom počítači,
- možnosť ukladania nadefinovaných pohľadov u každého užívateľa jednotlivo,
- možnosť editácie (vytváranie vlastných) alarmových správ s možnosťou následného odosielania na emailové adresy ako aj zobrazenie správ push-up notifikáciami na ploche pozorovateľa kamerového systému,
- možnosť editovania veľkosti zobrazovacích okien na klientskej stanici,
- možnosť vyhľadávania na základe zmeny v obraze, možnosť označiť a vyhľadať zmenu len vo vybraných pixeloch,
- možnosť vytvorenia virtuálnej PTZ z viac megapixlových kamier,
- možnosť nastaviť min. 10 sekúnd pred alarmový čas,
- možnosť úplne vypnúť PTZ ovládanie na kamerách,
- automatické prepínanie streamov podľa veľkosti okna v ktorom sa zobrazujú pre minimalizáciu dátových tokov z klienta na server,
- zdieľanie užívateľských oprávnení automaticky medzi servermi,
- možnosť zamedziť prístup do archívu ako aj exportu nahrávok jednotlivým používateľom,
- možnosť nastavovania analýzy na kamerách priamo z klientského softwaru,
- analytické funkcie môžu byť prístupné aj na termokamerách,
- možnosť vyhľadávania klasifikovaného pohybu v zázname, označenie oblasti záujmu a následne vyhľadávanie osôb v tejto oblasti,
- možnosť vyhľadávania rovnakých osôb alebo áut v kamerovom systéme, medzi viacerými kamerami súčasne,
- možnosť vyhľadávania osôb na základe popisu oblečenia a pohlavia,
- systém musí umožniť zdieľanie licencii medzi servermi, licencie neviazané na konkrétny server,
- systém nebude vyžadovať žiadne ďalšie licenčné/servisné poplatky,
- možnosť obmedziť prístup k záznamu len na čas od zalogovania užívateľa a zabránenie prehľadávania starších záznamov,
- možnosť využívania externého úložiska na predĺženie doby záznamu,
- možnosť zálohovania dát v intervale min.1hodina,
- detekcia jednoduchého hesla a zamedzenie jeho používania,
- možnosť nastavenia intervalu zmeny hesla každých 30,60,90 alebo 120 dní,
- možnosť pripojenia nízkofrekvenčného radaru do systému (detekcia prítomnosti osoby),
- možnosť pripojenia IP video/audio vrátnika a prijímania hovorov cez kamerový software bez nutnosti použitia externých zariadení,
- možnosť zaheslovania exportu priamo v kamerovom systéme,
- možnosť prepnúť kamery do „stand by“ módu, kde kamery nebudú nahrávane a nebude možný ani živý náhľad,
- podpora nadstavbového bezpečnostného systému (vizualizácia prvkov, prehrávanie živého videa a záznamu, kontrola spojenia a pod.).

Analytické funkcie pre zabezpečenie monitoringu a stráženia vytýčeného koridoru :

- objekt je v oblasti záujmu,
- objekt nie je v oblasti záujmu,
- počet objektov prekročí hranicu,
- počet objektov je pod nastavenou hranicou,
- objekt prekročí definovanú čiaru,
- viacero objektov prekročí definovanú čiaru,

- objekt sa objaví v oblasti záujmu,
- objekt zmizne z oblasti záujmu,
- objekt vstúpi do oblasti záujmu,
- objekt opustí oblasť záujmu,
- nastavený počet objektov vstúpi do oblasti záujmu,
- nastavený počet objektov opustí oblasť záujmu,
- pokiaľ objekt postáva v oblasti záujmu,
- pokiaľ objekt stojí v oblasti záujmu,
- objekt sa pohybuje zakázaným smerom,
- náhla zmena scény,
- strata videosignálu.

Elektrická požiarna signalizácia EPS

Požiadavky na systém sú podľa platnej legislatívy. Systém naviac musí podporovať integráciu treťostranných aplikácií. Pre cely musia byť použité kombinované detektory.
V súčasnosti sú v ústave zabudované dva nezávislé systémy - ústredňa MHU 103 – LITES a ústredňa SCHRACK BMZ Integrál. Ústredňa MHU 103 – Lites je už technicky, fyzicky a morálne zastaraná. Ústredňa EPS SCHRACK BMZ Integrál bola nainštalovaná na objekte č. 20 (Hrad) pri celkovej rekonštrukcii tohto objektu v roku 2004 a spĺňa požiadavky na rozšírenie.

Spoločná televízna anténa STA

V ústave majú možnosť odsúdení a obvinení pozerať televízny príjem, ktorý je zabezpečený prostredníctvom šírenia pozemného digitálneho vysielania (DVBT) a satelitného príjmu. V ústave sa signál šíri pomocou systému Polytron SMP 1000 inštalovaného v r. 2005 a sústave ďalších zosilňovačov podľa potreby na jednotlivých objektoch.
Odsúdeným a obvineným je ústav povinný zabezpečiť možnosť počúvať rádio, ktoré je v ústave zabezpečené cez zosilňovač SK 11500 a vstupnú jednotku FS 3000 RGUB s výkonom 1500W. Distribúcia signálu prebieha pôvodným 100 voltový rozvodom po drôte inštalovaného v r. 1981.

Šírený bude signál v jednotlivých objektov, pričom systém musí byť rozšíriteľný o možnosť šíriť vlastné vysielanie. Zásuvky STA budú v každej cele (mimo cely špeciálneho zaobchádzania), v kultúrnych miestnostiach, operačnom stredisku a prípadne na iných miestach, ktoré určí zákazník.

Integrovaný bezpečnostný systém

Centralizáciu ovládania a riadenia bude tvoriť nadstavbový bezpečnostný softvér, ktorý zabezpečí prepojenie lokálnych systémov a centrálny zber dát. Má pripojené rozhrania jednotlivých podsystémov a komunikuje prostredníctvom TCP/IP ktoré sú do neho zaintegrované. Na základe toho obsluha môže pracovať v jednotnom prostredí, s jedným vizualizačným plánom čo umožňuje rýchlu a efektívnu obsluhu a tým aj optimalizáciu procesov, skrátenie reakčného času pri vyhodnocovaní bezpečnostných incidentov a zvýšenie bezpečnostnej úrovne riešenia. Nadstavbový softvér je na báze architektúry klient/server a musí podporovať aj záložný server. Licencuje sa server, klientska aplikácia je bezplatná na neobmedzený počet klientskych PC. Softvér musí obsahovať správu bezpečnostných incidentov a komplexné logovanie udalostí.

Základom je vybudovať riadiace stredisko zložené zo serverov v redundantnom zapojení a klientskeho pracoviska vrátane dostatočného počtu zobrazovacích jednotiek pre základnú správu a monitoring. Každý server bude mať predinštalovaný nadstavbový bezpečnostný systém, do ktorého sa doplnia všetky bezpečnostné systémy. Základom nadstavbového systému

je nezávislosť na hardvéry bezpečnostných systémov. To znamená, že v prípade poruchy servera, straty komunikácie, prípadne iných vážnych porúch nadstavbového bezpečnostného systému, nesmie byť ovplyvnená základná funkčnosť pripojených bezpečnostných systémov.

Základné požiadavky a funkcionality na nadstavbový bezpečnostný systém

Systém zabezpečuje centralizované a multiužívateľské riešenie pre správu zariadení objektovej bezpečnosti. Jedná sa o otvorený modulárny systém, ktorý umožňuje monitorovanie stavu všetkých integrovaných zariadení v rámci jednotlivých objektov, bez ohľadu na vzdialenosť. Systém pracuje na rôznych platformách operačného systému, na serveroch umiestnených v hlavnej serverovni. Do grafického nadstavbového systému sa integrujú všetky technologické zariadenia. Prepojenie zariadení bude zrealizované prostredníctvom sieťových a komunikačných rozhraní jednotlivých zariadení. Týmto sa umožní sledovať všetky monitorované technologické zariadenia v jednotnom prostredí vrátane ich jednotného ovládania z toho istého prostredia. Takýto spôsob monitorovania výrazne znižuje nároky na zaškolenie obsluhy systému. Užívateľ nemusí poznať detailne jednotlivé ovládané technologické zariadenia. Nastavovanie oprávnení, vydávanie príkazov na zariadenia a podobne sa prevádza rovnako pre všetky technologické zariadenia nezávisle od akého výrobcu je zariadenie. Obsluha jednotlivých zariadení z centrálneho servera prebieha paralelne, to znamená, že jednotlivé zariadenia na serveri nie sú vzájomne ovplyvňované. Množstvo obsluhovaných zariadení ako aj klientskych staníc, z ktorých je možné technologické zariadenia obsluhovať je limitované výhradne výkonom servera.

On-line sledovanie stavov na pripojených zariadeniach je užívateľovi dostupné už v základnej verzii. Užívateľ okamžite po pripojení zariadenia do systému vidí ako dané zariadenie pracuje. Server grafického nadstavbového systému zabezpečuje všetky operácie spojené s priamou obsluhou zariadení. Nastavenia systému, získavanie údajov o stave zariadení, priame ovládanie zariadení a podobne prebieha pod kontrolou serverovej časti aplikácie. Tento koncept výrazne zvyšuje stabilitu a bezpečnosť celkového riešenia.

Správa bezpečnostných incidentov: Systém zabezpečuje správu bezpečnostných incidentov tak, aby mala obsluha okamžitý dostatok informácií pre správne vyhodnocovanie krízových situácií. Potvrdenie vykonania akcie musí byť v systéme evidované a priložené k záznamu o udalosti pre potreby vyhodnocovania situácie v budúcnosti.

Prehľadná ergonómia aplikácie: Aplikácia sa chová k užívateľovi ako jeden celok (User friendly), kde má užívateľ okamžite k dispozícii všetky potrebné údaje k vybranému objektu. Či už ide o vybranú osobu, udalosť alebo zariadenie, má užívateľ okamžite k dispozícii informácie o ich nastaveniach ako aj udalostiach, ktoré sa vybraného objektu akýmkoľvek spôsobom dotýkajú. Pri poplachu alebo inej udalosti môže operátor poskytovať okamžité informácie špecifické pre jednotlivý objekt ktoré sú k nemu viazané. Tento systém má vysokú bezpečnosť práce s dátami a možnosť šifrovania na všetkých úrovniach prenosu. Systém využíva najnovšie technológie v oblasti bezpečnostných technológií. Prenos dát medzi klientom a serverom sa môže realizovať rovnakou bezpečnostnou technológiou, aká sa využíva v produktoch typu internet banking. Všetky užívateľské akcie sú zaznamenané a umožňujú jednoduché vyhľadávanie. Systém samozrejme spĺňa všetky kritériá kladené na prácu s osobnými údajmi GDPR.

Správa osôb je primárne navrhovaná tak, aby pokryla rôzne technológie s rôznou funkcionalitou a rôznymi riadiacimi parametrami. Operátorovi sa tieto informácie zobrazujú v jednotnom prostredí. To zabezpečuje užívateľovi jednoduchú správu hierarchických

prístupových oprávnení. Užívateľ nastavuje oprávnenia prístupu na dvere alebo čítačky a nie je zaťažovaný otázkami aké kódy, prípadne karty konkrétne dvere akceptujú a ani akým spôsobom sa tieto informácie dostanú do jednotlivých zariadení. O túto problematiku sa stará grafický nadstavbový systém.

V priestoroch operačného pracoviska budú na monitore zobrazované udalosti zo všetkých pripojených systémov.

V budúcnosti bude možné tento systém rozšíriť o nové technológie, pripojiť a integrovať ďalšie technológie zákazníka.

Všetky grafické návrhy pre zobrazovanie jednotlivých objektov v oknách systému budú vypracovávané na základe požiadaviek zákazníka počas integrácie a postupného pripájania jednotlivých zariadení. Dodávateľ konkrétnej technológie zabezpečí potrebnú dokumentáciu pre vypracovanie grafických podkladov pôdorysov a máp.

Správa osôb - možnosť nastavenia oprávnení užívateľom alebo skupinám do aplikácie: Pod správou osôb sa v systéme zaraďuje taktiež správa oprávnení týkajúca sa prístupu jednotlivých užívateľov, skupín užívateľov do systému. Systém umožňuje rozdeliť prácu medzi viaceré osoby, zodpovedné za konkrétne časti prevádzkových procesov (personálne oddelenie: správu zamestnancov, vedenie spoločnosti: získavanie prehľadov, atď.) Možnosť pridelenia jednotlivých úloh v systéme je riešená formou tzv. „Rolí". Pre jemnejšie doladenie oprávnení systém poskytuje taktiež detailné nastavenie oprávnení až po úroveň osoba - oprávnenie - objekt, na ktorý sa oprávnenie vzťahuje.

Súčasné ovládanie zariadení z viacerých miest: Systém umožňuje prácu viacerých dispečerských paralelných pracovísk. Taktiež tu sa prejavuje správa osôb a oprávnení, kde systém umožňuje nastaviť oprávnenia v dispečingu pre jednotlivých pracovníkov. Tieto oprávnenia sa týkajú možnosti sledovať udalosti len pre konkrétnu lokalitu, možnosť ovládať len určené zariadenia, možnosť sledovať stavy pridelených zariadení. Zároveň, ale vďaka tomu, že systém je centralizovaný, môže paralelne iný užívateľ na základe pridelených oprávnení sledovať stav všetkých lokalít súčasne. Systém taktiež umožňuje informovať všetkých zúčastnených o aktivitách ostatných pracovníkov a zabraňuje súčasnému vydávaniu príkazov z viacerých pracovísk.

Centrálna evidencia informácii: Tento systém umožňuje pracovať súčasne viacerým užívateľom nad spoločnými dátami zo všetkých obsluhovaných zariadení.

Jednotná centrálna databáza: Dáta spravované týmto systémom sú uložené v centrálnej databáze na samostatnom serveri umiestnenom v zabezpečenej miestnosti. K týmto údajom je prístup realizovaný výhradne technológiou (tzv. web-service), ktorá zabezpečuje, aby prihlásený užívateľ dostal, prípadne upravoval len tie informácie, ku ktorým má oprávnenia. Toto rozhodovanie sa deje už na strane servera (zabezpečeného centrálneho počítača), takže sa dá povedať, že bezpečnosť celého nasadenia sa odvíja od úrovne zabezpečenia ochrany servera.

Jednotná správa osôb pre všetky technológie: Systém umožňuje jednotnú správu osôb pre všetky technológie - všetky nastavenia týkajúce sa nastavenia prístupu osôb k jednotlivým zariadeniam sa užívateľovi zobrazujú v jednotnom rozhraní. Správa osôb je primárne navrhovaná tak, aby pokryla rôzne technológie (s rozličnou funkcionalitou a rozličnými

riadiacimi parametrami) tak, aby sa užívateľovi zobrazovali pokiaľ možno v jednotnom prostredí. To zabezpečuje užívateľovi následnú jednoduchú správu prístupových oprávnení.

Možnosť integrácie zariadení od rôznych výrobcov: Zákazník nie je v budúcnosti viazaný na dodávky jedného konkrétneho zariadenia, čo mu zabezpečuje nezávislosť od jedného výrobcu zariadení.

Hierarchická správa osôb a zariadení: Poslednou oblasťou v ponímaní správy osôb v systéme je podpora evidovania osôb v hierarchii. Pri správe osôb je táto technológia využívaná pre správu organizačnej štruktúry.

Hierarchia využíva prepracovanú technológiu stromu osôb bez obmedzenia počtu vnorení a s prístupom k informáciám o položke v ľubovoľnej úrovní bez vplyvu na rýchlosť systému ako celku.

Inteligentná automatická detekcia porúch: Pri nasadeniach monitorových systémov v sieťových prostrediach sa často objavujú situácie, kedy vzdialené zariadenie nie je možné monitorovať z dôvodov poruchy na prenosovej trase. Pri súčasných systémoch je táto porucha vyhodnotená ako porucha tohto vzdialeného zariadenia a je na užívateľskej obsluhe aby po zdĺhavej analýze vyhodnotila situáciu a v prípade poruchy na sieti riešila problém s oddelením dohľadu sietí. Grafický nadstavbový systém je aj v tomto smere silným nástrojom, ktorý pomáha obsluhe vyhodnotiť situáciu v zlomkoch sekúnd.

Vlastnosti vizualizačných prvkov: Pri grafickom znázorňovaní jednotlivých regiónov, pod regiónov a zariadení môžete používať rôzne preddefinované tvary. Sú to grafické prvky, ktorými sa na vyššej úrovni regiónu lokalizuje pod región. Preddefinované tvary sú teda prvky, ktoré sa využívajú pri vizualizácií regiónov a zariadení. Užívateľ si môže vybrať z ponuky kliknutím na tlačidlo a nastaviť tak preddefinovaný tvar.

Zálohovanie dát v systéme: Jednou z hlavných vlastností centrálnej databázy je jednoduchá údržba dát. To umožňuje integrovať grafický nadstavbový systém do procesov zálohy dát. V databáze sa nachádzajú aktuálne konfigurácie a história udalostí za dobu definovanú v projekte nasadenia. Doba udržiavanej histórie má vplyv na hardwarové nároky servera (pamäť a disky). Táto databáza sa priebežne zálohuje pre prípad zlyhania servera. Systém vykonáva zálohu všetkých dát každý deň o 23:00.

Aplikácia systémov v rámci siete LAN/WAN so zabezpečeným prenosom informácií: Komunikácia medzi klientskym PC grafického nadstavbového systému a serverom používa štandardný http protokol. K prevádzke vo vnútornej sieti pre grafický nadstavbový systém postačujú také nastavenia, ako pre intranet.

Zabezpečenie systému proti zámernému zahlteniu sieťového prenosu: Zahltenie prenosových trás sa rieši použitím VLAN technológie pre pripojenie jednotlivých vzdialených technológií. Pomocou VLAN môžeme zabezpečiť minimálnu a maximálnu priepustnosť nezávisle od zaťaženia zvyšku siete. Otázka ochrany servera pred vírusmi je riešená použitím antivírového programu.

Požaduje sa komplexná dokumentácia od výrobcu informačného systému. Podrobná dokumentácia bude vyžadovaná pre každú jednotlivú časť procesu nasadenia a prevádzky - inštalácia, pripojenie jednotlivých zariadení, administrácia a prevádzka systému. Taktiež bude vyžadované preukázanie spôsobilosti dodávateľov k implementácii a práci s jednotlivými technológiami.

Vzhľadom na nároky administrácie celkového riešenia, systém nesmie využívať technológie vyžadujúce zvýšené oprávnenia na strane klientskych počítačov. Preto systém nesmie využívať prvky na báze technológie ActiveX, Silverlight a pod.. Toto obmedzenie má význam aj z hľadiska celkovej bezpečnosti počítačovej siete organizácie, kde prípadné povolenie automatického inštalovania takýchto komponentov vzniká riziko neoprávneného prístupu k citlivým údajom.

Jednotné a previazané integrované riešenie: Toto riešenie zabezpečuje jednoduchú konfiguráciu celej aplikácie v jednotnom prostredí. Odpadá zložité paralelné konfigurovanie viacerých aplikácií.

Jednotná a hierarchická správa osôb: Umožňuje správu osôb v organizačnej štruktúre, prípadne doplnkovo aj zaraďovanie osôb do skupín. Práca s takouto hierarchiou umožní efektívne nastavovanie oprávnení - nastavenie oprávnení na oddelenie zabezpečí zdedenie oprávnení všetkým zaradeným osobám. Od tejto vlastnosti systému sa očakáva výrazné zníženie nárokov na administráciu, správu bezpečnostných incidentov a evidenciu krokov obsluhy v priebehu riešenia pre potreby vyhodnocovanie situácií v budúcnosti.

Ďalej systém umožňuje jednoduché užívateľské prepínanie medzi pohľadmi:

- Celkový náhľad na monitorované objekty
- Pohľad na vybrané poschodie/objekt/záujmovú oblasť

Centrálny bezpečnostný systém musí mať otvorenú platformu s možnosťou vývoja dodatočných aplikácii tretími stranami. Umožňovať prepojenia s externými informačnými systémami zákazníka. Rozhranie pre externý vývoj musí byť zákazníkovi prístupné a zdokumentované.

Ochrana pred bleskom a prepätím

Zariadenie musí byť chránené adekvátne povahe a bezpečnostnému charakteru objektu (napr. izolovaný (oddialený) bleskozvod). Dodržaná musí byť platná legislatíva.

Konštrukcia káblových rozvodov

Dátová sieť (infraštruktúra), vytvorená vhodnou technológiou (napr. technológiou optických vlákien). Topológia bude kruh/hviezda prípadne strom, ktorej súčasťou budú aktívne komunikačné zariadenia s podporou POE/POE+. Zariadenia budú mať v prípade potreby zvýšenú tepelnú odolnosť, odolnosť voči poveternostným podmienkam, mechanickým vplyvom, resp. priemyselné vyhotovenie. Táto sieť bude hardvérovo zdieľaná s infraštruktúrou určenou pre informačný systém zákazníka. Riešenie metalickej štruktúrovanej kabeláže v Cat.6A, tienenej – FTP. Štruktúrovaná sieť musí byť budovaná v topológii „hviezda“ (lokálne) / „kruh“ (medziobjektovo, topológia vnútroareálového rozvodu). Optické prepojenie musí byť navrhnuté unifikovane, tak aby vyhovovalo všetkým požiadavkám pre potreby jednotlivých technológií a informačného systému zboru. Počítačová sieť sa zriaďuje spravidla vo všetkých kancelárskych a administratívnych priestoroch podľa dispozície, navrhovaného obsadenia personálom a navrhovanom obsadení technológiou. Počítačová sieť bude zriadená aj na iných miestach podľa požiadaviek zákazníka .

Všeobecné vlastnosti a požiadavky na signálno-bezpečnostnú techniku

Pod pojmom signálno-bezpečnostná technika sa v podmienkach zákazníka rozumie súbor ďalších inštalovaných bezpečnostných zariadení/technológií určených na detekciu, ktoré

dopĺňajú komplexné systémy včasného varovania, odhaľovania nepovolených predmetov, signalizácie narušenia a iných stavov dôležitých pri vyhodnotení a riešení bezpečnostných incidentov.

Zahŕňa snímače rôznych veličín, ako napr.: duálne detektory pohybu, detektory rozbitia skla, magnetické kontakty, infrazávory, mikrovlnné bariéry s digitálnou analýzou, otrasové detektory, nášľapné systémy a rôzne iné detektory pohybu a fyzikálnych veličín.

Súčasťou sú aj detektory kovov, detektory prítomnosti osôb vo vozidle, scanner podvozku motorových vozidiel, detekcia mobilných telefónov, poloha mŕtveho muža, kľúčový management a pod.

Štandardným prvkom sú prídržné magnety na požiarnych úsekoch pre prípad požiaru/evakuácie.

Osvetlenie priestorov je požadované kontinuálne, v prípade strážených úsekov s rovnakou intenzitou.

Zdroj náhradnej energie (diesel agregát) pre bezpečnostnú časť musí byť umiestnený bezpečne v areáli, mimo väzenskú časť. Zariadenia musia byť chránené aj UPS na preklenutie času výpadku a nábehu NZE. Rozvod UPS nemusí byť centrálny pre areál, ale môže byť decentralizovaný (zvlášť pre väzenskú časť, zvlášť pre výrobnú časť).

Rádiový systém kompatibilný s aktuálne používaným v zbore. Krátka špecifikácia:

- UHF(400-470MHz),
- výkon 25W s možnosťou zmeny úrovne (základňová rádiostanica),
- výkon 5W s možnosťou zmeny úrovne (prenosná rádiostanica)
- v analógovom režime: scrambler, 5tone, CTCSS;
- v digitálnom režime DMR Tier II aj Tier III; možnosť GPS;
- podpora polohy mŕtveho muža

Používané zariadenia v rádiovom systéme - Motorola GM380, GM360, GP340, HYT TC700P, HYT MD785i.

V objektoch sa plánuje použitie centrálnej IP telefónnej platformy zboru na báze Cisco Unified Communications Manager 12.x..