Elektronické zabezpečovacie systémy budov

Článok obsahuje všeobecnú charkteristiku problematiky zabezpečenia objektov a budov. S požiadavkami, návrhom a realizáciou zabezpečovacieho systému sa čitateľ môže podrobnejšie zoznámiť v uvedených štandardoch a odbornej literatúre, alebo odporúčame konzultácie v spoločnostiach dlhodobo pracujúcich v tomto odbore.

Úvod a základné pojmy

Všeobecne sa pojmom elektrické zabezpečovacie systémy označujú aj rôzne zariadenia určené na ochranu majetku a osôb v objektoch. Myslíme tým hlavne systém na riadenie a kontrolu vstupov (SKV), kamerový sledovací systém (známa je anglická skratka CCTV – Closed Circuit Television, alebo slovenský ekvivalent UTO – uzavretý televízny okruh), elektrickú požiarnu signalizáciu (EPS), bezpečnostný a evakuačný rozhlas, ako aj vlastný elektronický zabezpečovací systém (EZS) v užšom zmysle slova. Názov aj skratka sa znovu začali používať, keď sa po zavedení európskych noriem (EN) pre bezpečnostné systémy využíval ich český preklad. Medzitým sa začalo používať (a doteraz sa používa) aj pomenovanie poplachový systém na hlásenie narušenia (PSN). Všetky systémy môžu spoločne s mechanickými zábranami, prostriedkami, organizačnými opatreniami a strážnou službou vytvoriť komplexné zabezpečenie ako integrovaný bezpečnostný systém (IBS). Tieto systémy sa na zabezpečenie komfortu a bezpečnosti inštalujú aj v inteligentných budovách, a to buď vyčlenené oddelene na ochranu budovy, alebo aj v spoločnej štruktúre a pod spoločnou správou. V oboch prípadoch musí byť zabezpečená aj ich vzájomná súčinnosť, hoci niekedy sú požiadavky na ich prevádzku protichodné. Takéto protichodné požiadavky existujú už medzi základnými bezpečnostnými systémami. Napríklad sa tak prejavujú požiadavky na ovládanie dverí pri súčasnom zabezpečení priestoru systémami PSN, SKV a EPS (požiadavky na zabezpečenie majetku, autentizované prechody a únikový východ v prípade požiaru).

Určenie a zloženie EZS

Elektronický zabezpečovací systém zabezpečuje detekciu a signalizáciu vstupu alebo pokusu o vstup narušiteľa do strážených objektov a priestorov.

Základom systému je ústredňa. Jej výber závisí od stavby a fyzického rozsahu objektu (priestorov), vyhodnotenia analýzy rizík objektu a stanovenia požadovaného stupňa zabezpečenia podľa noriem a príslušnej legislatívy (napr. ochrana utajovaných skutočností), požiadaviek a finančných možností klienta, poistných podmienok a spôsobu obsluhy systému a vykonávania zásahu.

Systém možno modulárne rozširovať pomocou expandérov a programovať podľa potrieb používateľa. Ale aj pri menšej pravdepodobnosti rozširovania v budúcnosti by sa nemal robiť výber ústredne a jej projektovanie na maximálnu kapacitu. Rozširovanie počtu vstupov a výstupov sa realizuje cez rozširovacie moduly (expandéry), ktoré sa k ústredni pripájajú cez sériovú zbernicu, ktorou je obvykle alternatíva štandardu RS485.

Ústredne, expandéry a detektory sa napájajú zo zdrojov zálohovaných batériou, ktorej kapacita sa projektuje podľa požiadaviek noriem alebo klienta.Detektory sa k ústredni pripájajú jednotlivo na samostatné vstupy, aj keď existuje možnosť pripojiť viac detektorov na jeden vstup. Používa sa nastavenie na dvojito vyvážený vstup, čo umožňuje na jednom dvojvodičovom vedení vyhodnotiť poplachový stav detektora, pokus o narušenie detektora alebo vedenia, a to aj v čase, keď systém nie je zapnutý na stráženie. V súčasnosti sa začínajú objavovať aj systémy s trojito vyváženými vstupmi, ktoré umožňujú cez jedno vedenie pripojiť aj detektor s antimaskingom. Okrem funkčnosti dbajú výrobcovia aj na vzhľad a estetiku detektorov.

Existujú rôzne typy detektorov pracujúcich na rôznom fyzikálnom princípe, niektoré kombinované detektory využívajú aj dva rôzne typy senzorov. Najčastejšie sa používajú PIR (Passive IfraRed) detektory pohybu – pracujú na základe vyhodnotenia zmeny tepelného vyžarovania oproti pozadiu. Sú schopné zabezpečiť celý priestor miestnosti, alebo s inou snímacou charakteristikou rad okien na chodbe.

Magnetické kontakty slúžia na detekciu otvorenia vstupných dverí alebo montážnych skriniek.

Ďalej možno inštalovať detektory rozbitia skla detegujúce zvuk tlakovej vlny a následné rozbíjanie skla. Na rámy okien, na steny alebo trezory sa používajú aj otrasové detektory.

V systéme možno použiť aj tiesňové tlačidlá na privolanie pomoci, a to drôtové alebo bezdrôtové.

Bezdrôtové systémy a detektory umožňujú realizovať systém bez inštalácie káblov prakticky do vzdialenosti asi 30 m medzi detektorom a bezdrôtovým expandérom.

Ako signalizačné zariadenia sa používajú sirény so svetelným majákom, vonkajšie volíme so zálohovaným napájaním z vlastnej batérie.

Na ovládanie systému sa používa jeden alebo viac ovládacích panelov. Sú to klávesnice s LCD displejom, jednoduchšie s LED diódami. Okrem ovládania systému, zapínania a vypínania stráženia umožňujú signalizovať stavy systému na displeji, LED diódami alebo interným bzučiakom. Ovládanie systému je možné na základe zadania číselného kódu, po doplnení snímača aj priložením bezkontaktného identifikátora. Niektoré systémy majú ovládanie aj cez dotykové obrazovky alebo navádzajú používateľa hlasovými pokynmi. K systémom EZS existujú aj softvérové nadstavby na ich ovládanie, monitorovanie a programovanie. Možný je lokálny aj vzdialený prístup, vzdialený sa využíva na servisnú kontrolu na základe povolenia správcom systému.

Na diaľkové monitorovanie v strediskách registrovania poplachov sa používajú komunikátory s prenosom cez rôzne rozhrania. Na Slovensku sa najčastejšie využíva pripojenie a prenos cez analógové telefónne linky (v tzv. hovorom alebo nahovorovom pásme). Existuje možnosť pripojenia na monitorovanie a ovládanie systému cez mobilný telefón hlasom aj SMS, alebo dátovým prenosom (GSM, GPRS...). V Českej republike sú viac rozšírené systémy s rádiovým prenosom, vo svete zase cez linky ISDN alebo Internet.

Monitorovacia stena v centre na dohľad nad križovatkami a cestnými úsekmi

Funkcie EZS

Ako sme už uviedli, EZS umožňuje privolať pomoc pri napadnutí alebo pomoc pre zdravotne či telesne postihnuté osoby alebo starších ľudí. Okrem ochrany a stráženia priestorov umožňujú ústredne pripojiť aj požiarne hlásiče (nenahradzujú ústredne EPS tam, kde je to stanovené legislatívou).

EZS možno programovo deliť na podsystémy a tie potom samostatne ovládať a monitorovať. Okrem signalizácie poplachu sirénou je možnosť signalizácie „tichého poplachu“, napr. zadaním kódu pod nátlakom.Niektoré systémy poskytujú možnosť priamej integrácie snímačov identifikátorov a systému kontroly vstupu.Samozrejmosťou je aj možnosť monitorovania technických zariadení v objekte a ich programové alebo diaľkové ovládanie.

Prístupový systém – turniket

Návrh a realizácia EZS

Pri návrhu EZS by si mal používateľ stanoviť základné požiadavky, ktoré neskôr môže konzultovať a upresňovať, a vybrať si vhodného dodávateľa. Návrh a ponuka by sa mali vytvoriť na základe preskúmania požiadaviek, rizikovej analýzy a stavebných dispozícií, zladenia s legislatívou a technickými normami, navrhnutý systém by mal byť primeraný významu chráneného záujmu a výške strážených hodnôt. Pritom je dôležité zachovať systémový prístup a zladiť návrh systému s režimom prevádzky objektu, zabezpečiť režimové a organizačnými opatrenia, mechanické zabezpečenie, prenos a signalizáciu poplachových signálov, pripojenie k SRP polície alebo SBS a zabezpečiť dokumentáciu informácií.

Po prerokovaní návrhov a uzavretí zmluvy sa vytvorí projekt a plán inštalácie. Nasleduje vlastná inštalácia systému, jeho oživenie a nastavenie. Vykoná sa východisková revízia, stanovené funkčné skúšky, do dokumentácie sa zapracuje skutkový stav. Nasleduje preukázateľné zaškolenie obsluhy, skúšobná prevádzka, odovzdanie diela s príslušnou dokumentáciou. Počas prevádzky sa vykonávajú pravidelné plánované prehliadky alebo operatívne zásahy pri prípadných poruchách. Neskôr možno vykonávať bezpečnostný a technický audit a na základe jeho výsledkov plánovať modernizáciu systému.

Dispečing mestskej polície s napojenými EZS rôznych inštitúcií a firiem

Falošné poplachy a trendy

Správne navrhnutý a nainštalovaný EZS je osožný pre všetky zúčastnené strany: pre používateľa aj pre políciu alebo SBS (SRP), servisnú organizáciu a poisťovňu. Používateľ sa môže spoľahnúť, že každý pokus o vniknutie do jeho priestorov vyvolá adekvátny zásah. Naopak polícia alebo SBS bude reagovať rýchlo a s vedomím, že nejde o falošný poplach. To by malo viesť k tomu, že sa vo vyššej miere zabráni škodám a zabezpečí zaistenie páchateľa. Poisťovňa bude mať úžitok z nižších strát, čo by sa malo odraziť aj na poistnom.

Ak predpokladáme, že bude narastať počet monitorovaných systémov, tak budú narastať aj požiadavky na zásahové jednotky. Preto sa z priemerného ročného počtu falošných poplachov na systém presúva zameranie na to, koľko zásahov sa skutočne vykonáva. Napríklad vo Veľkej Británii existujú pozitívne snahy, ktoré si všímajú aktuálne trendy a technické požiadavky na poplachové systémy. Uviedli do života smernicu PD 6662, pomocou ktorej by sa mala dosiahnuť znesiteľná úroveň falošných poplachov. Upresňujú požiadavky na diaľkový servis a diagnostiku, čo spolu s novými prenosovými systémami bude hrať dôležitú úlohu pri odhaľovaní porúch a vykonávaní prehliadok bez potreby výjazdu technika k objektu. Elektronický prenos dát a väčšie množstvo relevantných informácií poskytovaných na SRP umožnia identifikáciu skutočných a v niektorých prípadoch aj falošných poplachov, budú šetriť náklady a zabezpečia efektívne zhodnotenie kvalitných EZS.

Hlavný výsledok tejto stratégie je v tom, že reakcia na EZS sa výrazne zlepší a uvoľní sa viac zdrojov zásahových síl, zníži sa výskyt falošných volaní a zvýšia sa šance úspešných zásahov na základe signalizácie EZS. To môže byť výhodné nielen pre políciu, ale aj pre spoločnosti zaoberajúce sa bezpečnosťou a, samozrejme, najmä pre verejnosť.

Ing. Dušan Pivko

QUADRIQ, a. s.
e-mail: dusan.pivko@quadriq.sk