

Definice technických podkladů projektů pro areály Záchranného útvaru HZS ČR.

1. Úvod

Cílem tohoto projektu je vypracování projektové dokumentace pro investiční záměr, který zahrnuje vybudování komplexní infrastruktury zahrnující optickou a metalickou síť, Poplachový zabezpečovací a tísňový systém (PZTS), Elektrickou požární signalizaci (EPS), dohledový videosystém (VSS), Elektronický systém kontroly vstupu a vjezdu vozidel (EKV), klíčové hospodářství prostřednictvím mechatronických klíčů, vyvedení výstupů všech těchto integrovaných systémů na centralizované místo v lokalitě Hlučín, nezbytné stavební úpravy technických místností v administrativních budovách jednotlivých areálů, případně zřízení nových technických místností v každé budově v jednotlivých areálech, a napojení na dohledové a poplachové přijímací centrum (DPPC) na centralizované místo v lokalitě Hlučín a na DPPC nižší úrovně v každém jednotlivém areálu. Zpracování projektové dokumentace zahrnuje také přípravu a předložení všech potřebných dokumentů pro legislativní akceptaci vč. řádného a schváleného provozu jednotlivých technologií a schválení realizace projektu.

2. Cíle projektu

Úkolem projektanta je:

- Vytvořit detailní technický projekt zahrnující všechny komponenty popsané v tomto dokumentu.
- Definovat technické specifikace a požadavky pro všechny systémy a sítě, aby vyhovovaly současným i budoucím potřebám.
- Návrh a specifikace systémů: Vytvořit návrh optické a metalické sítě, PZTS, EPS, VSS, EKV a klíčového hospodářství, včetně technických specifikací a implementačních plánů.
- Napojení na dohledové a poplachové přijímací centrum (DPPC): Navrhnout a specifikovat systém napojení na DPPC, včetně nezbytné infrastruktury a technických řešení pro zajištění nepřetržitého monitorování a reakce na bezpečnostní incidenty.
- Vyvedení výstupů na centralizované místo v lokalitě Hlučín: Zahrnout řešení pro přenos dat a monitorování všech systémů na vzdálené centralizované místo v lokalitě Hlučín.
- Stavební úpravy technických místností v administrativních budovách jednotlivých areálů: Navrhnout nezbytné stavební úpravy technické místnosti v administrativní budově pro umístění všech technologií, včetně zajištění klimatizace, elektroinstalací, požárního zabezpečení a zabezpečení přístupu.
- Zpracování finančního rozpočtu: Vytvořit rozpočet projektu na základě zpracované technické dokumentace.
- Předložení legislativně nezbytných dokumentů: Připravit a předložit všechny potřebné dokumenty pro získání případných stavebních povolení a dalších právních náležitostí pro realizaci projektu a řádný a schválený provoz jednotlivých technologií.

3. Požadavky na projekt

3.1. Optická a metalická síť

- Optická síť: Detailní návrh trasy optických kabelů, specifikace vhodného typu vláken, návrh infrastruktury zahrnující optické rozvaděče, spojovací boxy a další nezbytné komponenty.
- Metalická síť: Návrh tras pro metalické kabely, výběr vhodných kabelů (např. Cat 6, Cat 7), návrh příslušné infrastruktury (zásuvky, rozvaděče) a jejich umístění.
- Veškeré sítě budou realizovány zemními chráničkami (HDPE trubky) včetně rezervy pro případné souběžné vedení, kdy hlavní chránička je již plně obsazená.
- Hloubka zemního výkopu musí být zohledněna pro ochranu při přejezdu speciálních technik.
- V projektové dokumentaci musí být zahrnuta i oprava komunikací, které bude nezbytné uvést do původního stavu v místě výkopových prací a odstranění původní vrstvy komunikace v případě, že nebude zvolena jiná technologie, která by povrch nepoškodila.

3.2. Struktura sítě v každé dislokaci

3.2.1. Centrální uzel sítě

Centrální uzel sítě bude umístěn vždy v administrativní budově každého areálu a bude sloužit jako hlavní bod, kde se sbíhají všechny datové toky z celého areálu. Tento uzel bude obsahovat následující prvky:

- Datový rozvaděč: Pro umístění hlavních síťových prvků, jako jsou přepínače (switches), směrovače (routers), servery, optické převodníky a další síťové zařízení.
- Optické spoje: Propojení administrativní budovy s ostatními budovami pomocí optických kabelů pro vysokorychlostní přenos dat.
- Záložní napájení (UPS): Pro zajištění nepřetržitého napájení síťových zařízení v případě výpadku elektřiny.

3.2.2. Optická síť

Optická síť bude zajišťovat hlavní propojení mezi budovami v každém jednotlivém areálu. Optické kabely nabídnou vysokou přenosovou kapacitu a odolnost vůči rušení, což z nich činí ideální médium pro mezibudovová spojení.

- Optické kabely: Každá budova areálu bude propojena s administrativní budovou vícevláknovými optickými kabely s minimálně 24 vlákny. Pokud je více budov propojeno za sebou (například při kaskádovitém propojení), budou optické kabely zajišťovat součet minimálně 24 vláken pro každou další budovu. To znamená, že pokud jsou za sebou propojeny dvě budovy, musí optický kabel mezi první a druhou budovou obsahovat minimálně 48 vláken a mezi druhou a třetí budovou minimálně 72 vláken atd. Optické kabely budou vedeny v chráněných trasách, jako jsou podzemní kabelové kanály nebo závěsné kabelové trasy.

- Optické převodníky: V technologických místnostech každé budovy v jednotlivých areálech budou instalovány převodníky, které umožní konverzi optického signálu na metalický a naopak, pro další distribuci v rámci lokálních sítí.

3.2.3. Metalická síť

Metalická síť (LAN) bude zajišťovat přenos dat v rámci jednotlivých budov a mezi technologickými místnostmi a koncovými zařízeními.

- Výměna stávajících rozvodů LAN: V každé budově bude provedena výměna stávajících LAN rozvodů za nové kabely kategorie 6A nebo vyšší, které podporují vysokorychlostní přenosy až do 10 Gbps, případně vybudování nových LAN rozvodů.

- Propojení technologických místností: Každá budova bude mít vlastní technologickou místnost, kde budou umístěny datové rozvaděče s přepínači. Tyto místnosti budou propojeny optickými kabely s centrálním uzlem v administrativní budově.

- Metalické kabely (Cat 6A): Pro rozvody uvnitř budov budou použity metalické kabely kategorie 6A, které zajistí vysokou rychlost a spolehlivost připojení.

3.2.4. Datové zásuvky a rozvody v budovách dle Přílohy č. 2

V každé budově bude instalován dostatečný počet datových zásuvek, aby bylo možné připojit všechna potřebná technologická zařízení (počítače, IP telefony, bezpečnostní kamery, tiskárny apod.).

- Umístění datových zásuvek: Datové zásuvky budou rozmístěny v souladu s potřebami jednotlivých prostor a technologií. Důraz bude kladen na pokrytí pracovních míst, technologických prostor, vstupních míst, zasedacích místností, ubytovacích místností a dalších klíčových oblastí.

- Počet datových zásuvek: Počet zásuvek bude navržen s ohledem na aktuální požadavky a s rezervou pro budoucí rozšíření.

- Patch panely: Datové zásuvky budou propojeny s patch panely umístěnými v technologických místnostech, což umožní snadnou správu a změny v rozvodech.

3.2.5. Rozvody pro příjem rozhlasového a televizního vysílání dle Přílohy č. 2

Rozvody pro příjem rozhlasového a televizního vysílání budou realizovány výhradně v administrativní budově a budovách určených pro ubytování. Klíčové prvky tohoto systému zahrnují:

- Anténní systém: Instalace centrální antény pro příjem pozemního digitálního televizního vysílání (DVB-T/T2) a rozhlasového vysílání (FM/DAB). Anténa bude umístěna na střeše administrativní budovy.

- Koaxiální kabeláž: Propojení anténního systému s centrálním rozvaděčem v administrativní budově prostřednictvím kvalitní koaxiální kabeláže (např. RG-6).

- Rozbočovače a zesilovače: Použití rozbočovačů a zesilovačů pro distribuci signálu do jednotlivých místností a kanceláří v administrativní budově a ubytovacích prostorech.

- Datové a TV zásuvky: Instalace kombinovaných datových a TV zásuvek v určených místnostech a kancelářích, které umožní připojení televizorů a rozhlasových přijímačů.

3.2.6 Propojení a integrace s centrálním uzlem dle Přílohy č. 2

- Propojení budov: Každá budova bude propojena s administrativní budovou optickým kabelem. V administrativní budově budou jednotlivé optické spoje konvertovány na metalické prostřednictvím optických převodníků a připojeny k centrálnímu síťovému zařízení.
- Centralizovaná správa: Všechna zařízení budou centrálně spravována z administrativní budovy v každém jednotlivém areálu, odkud bude zajištěna správa sítě, monitorování a řízení provozu.

3.3. PZTS, EPS a VSS dle Přílohy č. 2

- PZTS: Návrh a specifikace zabezpečovacího systému, který bude zahrnovat detekci neoprávněného vstupu, senzory, detektory a ovládací prvky.
- EPS: Návrh požárního systému zahrnujícího detektory kouře a tepla, sirény a další varovné prvky.
- VSS: Plán kamerového dohledu, zahrnující umístění kamer, specifikace nahrávacích zařízení a infrastruktury pro jejich provoz.

Návrh systému VSS, který je schopen uchovat data minimálně 14 dní. V každé dislokaci bude samostatné NVR s napojením na centralizované místo v lokalitě Hlučín. NVR bude mít systém RAID polí pro uchování a ochranu dat před poškozením s dostatečnou kapacitou.

3.4. EKV – elektronická kontrola vstupu dle Přílohy č. 2

Návrh moderního a bezpečného systému GSM vrátníku na vstupní části do objektu, který umožní kontrolovaný přístup do každého jednotlivého areálu pomocí mobilní sítě GSM. Tento systém umožní snadnou komunikaci a správu vstupu pro návštěvníky a personál, aniž by byla nutná přítomnost fyzické obsluhy u vrátnice.

3.4.1. Požadavky na systém GSM vrátníku

3.4.1.1 Funkčnost a základní prvky

GSM vrátník bude navržen tak, aby poskytoval spolehlivou a flexibilní kontrolu vstupu do objektu prostřednictvím mobilní sítě. Systém bude zahrnovat následující funkce a prvky:

- GSM modul: Centrální jednotka vrátníku bude vybavena GSM modulem, který umožní komunikaci prostřednictvím mobilní sítě. Tento modul zajistí přenos hovorů mezi vrátníci a mobilními telefony uživatelů, kteří mají oprávnění ke vstupu.
- Ovládání přístupové brány nebo závory: GSM vrátník bude připojen k systému pro ovládání přístupové brány nebo závory. Uživatelé budou moci otevřít bránu nebo závoru

pomocí mobilního telefonu buď prostřednictvím hovoru, nebo SMS zprávy, což jim umožní vzdáleně řídit přístup.

- Integrovaný mikrofón a reproduktor: Zařízení bude vybaveno mikrofónem a reproduktorem pro obousměrnou hlasovou komunikaci mezi návštěvníkem a uživatelem, což umožní ověření identity před povolením vstupu.
- Čtečka RFID nebo PIN klávesnice (volitelně): Pro zvýšení bezpečnosti může být systém vybaven čtečkou RFID karet nebo PIN klávesnicí, která umožní přístup autorizovaným osobám bez potřeby telefonního hovoru.
- Možnost správy pomocí mobilní aplikace: Některé pokročilé GSM vrátníky nabízejí možnost správy uživatelů a vstupů prostřednictvím mobilní aplikace. To umožňuje snadné přidávání a odebírání uživatelů, konfiguraci systému a sledování historie přístupů.

3.4.1.2. Instalace a propojení s dalšími systémy dle Přílohy č. 2

Systém GSM vrátníku bude nainstalován na vstupní části do objektu a bude integrován s ostatními bezpečnostními systémy, pokud jsou k dispozici. Klíčové aspekty instalace zahrnují:

- Umístění zařízení: GSM vrátník bude umístěn u hlavního vstupu do objektu, na přístupné a viditelné místo pro návštěvníky a personál. Umístění by mělo být chráněno před povětrnostními vlivy a vandalismem.
- Napájení: GSM vrátník bude napájen ze stávající elektrické sítě nebo z baterie, s možností záložního napájení pro zajištění nepřetržitého provozu v případě výpadku elektřiny.
- Propojení s přístupovými systémy: Systém bude propojen s motorizovanou bránou, závorou nebo dveřmi, které umožní vzdálené ovládání přístupu na základě oprávnění.
- Integrace s PZTS a VSS (volitelně): Pro zvýšení bezpečnosti může být GSM vrátník propojen s PZTS a VSS. Tímto způsobem lze monitorovat a zaznamenávat vstupy a výstupy v reálném čase.

3.4.1.3. Bezpečnostní opatření dle Přílohy č. 2

Pro zajištění bezpečnosti a ochrany před neoprávněným přístupem budou zavedena následující opatření:

- Šifrovaná komunikace: Veškerá komunikace mezi GSM vrátníkem a mobilními zařízeními bude šifrována, aby byla zajištěna ochrana proti odposlechu a manipulaci.
- Ochrana proti neoprávněné manipulaci: Zařízení bude vybaveno ochranou proti neoprávněné manipulaci (tamper switch), která spustí alarm v případě pokusu o násilné otevření nebo poškození zařízení.
- Logování přístupů: Systém bude uchovávat záznamy o všech přístupech, včetně datumu, času a identity uživatele. Tyto záznamy budou přístupné správcům systému pro účely bezpečnostního auditu.

3.4.2. Klíčové hospodářství prostřednictvím mechatronických klíčů dle Přílohy č. 2

- Návrh správy přístupových práv pomocí mechatronických klíčů, zahrnující specifikaci klíčů, zámků a softwaru pro jejich správu.

Systém mechatronických zámků:

Systém mechatronických zámků bude implementován pro zvýšení bezpečnosti a kontroly přístupu v rámci celého areálu. Tento systém bude kombinovat mechanické a elektronické prvky a nabídne flexibilitu v řízení přístupů:

- **Mechatronické zámky:** Každý zámek bude vybaven mechanickým klíčem a elektronickým prvkem, který umožní ovládání přístupu na základě autorizace. Elektronický prvek může zahrnovat RFID čip, biometrické ověření nebo kódový vstup.
- **Centralizovaná správa přístupů:** Přístupová práva budou spravována centrálně skrze centralizované místo v lokalitě Hlučín, což umožní snadné přidávání, odebrání a úpravu uživatelů. Administrátor bude mít možnost nastavovat různá přístupová oprávnění pro různé zóny a budovy v rámci areálu.
- **Propojení s existujícími systémy:** Mechatronické zámky budou integrovány do stávajícího bezpečnostního systému, což umožní propojení s PZTS a VSS, systémy pro zvýšení celkové bezpečnosti.
- **Záznamy přístupů:** Systém bude uchovávat záznamy o všech přístupech, včetně datumu, času a identity uživatele. Tyto záznamy budou přístupné správcům systému pro účely bezpečnostního auditu.
- **Odolnost a robustnost:** Mechatronické zámky budou navrženy tak, aby odolávaly extrémním podmínkám, včetně pokusů o fyzické narušení a klimatickým vlivům.

3.5. Ochrana perimetru areálu dle Přílohy č. 2

Ochrana perimetru bude zahrnovat technologie pro detekci neoprávněného vstupu na hranicích každého jednotlivého areálu a jejich integraci se systémy PZTS a VSS. Klíčové prvky zahrnují:

- **Perimetrické senzory:**
- **Infrapasivní a aktivní infračervené zábrany:** Instalace infračervených zábran podél hranic areálu, které budou detekovat průchod narušitele přes perimetr.
- **Mikrovlnné detekční systémy:** Použití mikrovlnných detektorů pro detekci pohybu v ochranném pásmu podél perimetru.
- **Kabelové senzorové systémy:** Instalace kabelových senzorů na oplocení, které budou detekovat pokusy o přelezení, prořezání nebo jiné mechanické narušení plotu.
- **Integrace s PZTS a VSS:**
- **Napojení na DPPC:** Perimetrické senzory budou integrovány s PZTS, což umožní okamžité spuštění poplachu při narušení perimetru.
- **Automatické ovládání VSS kamer:** V případě detekce narušení budou kamery VSS automaticky nasměrovány na místo narušení, čímž se zvýší šance na zachycení incidentu a jeho následné vyhodnocení.

- Monitorování a záznam událostí: Všechny incidenty detekované perimetrickým systémem budou zaznamenány a monitorovány centrálním monitorovacím systémem.

3.6. Systém kontroly registračních značek vozidel (LPR) dle Přílohy č. 2

Systém kontroly registračních značek vozidel (License Plate Recognition, LPR) bude instalován u všech vstupů a výjezdů z každého jednotlivého areálu, aby zajistil sledování a řízení vjezdu a výjezdu vozidel. Klíčové prvky zahrnují:

- Kamerový systém s LPR technologií: Kamery schopné rozpoznávat a číst registrační značky vozidel v reálném čase, umístěné u vjezdů a výjezdů z areálu.
- Centrální databáze vozidel: Systém bude propojen s databází, která bude obsahovat seznamy povolených a nepovolených vozidel, umožňující automatickou kontrolu vstupu.
- Automatické řízení závor: Na základě kontroly registrační značky systém automaticky povolí nebo odepře vjezd vozidlu, přičemž spustí závoru a případně upozorní bezpečnostní personál v případě potřeby.
- Integrace s EKV: Systém LPR bude propojen s EKV, což umožní sledovat nejen vozidla, ale i osoby, které vjíždějí do areálu.

3.7. Systém pro kontrolu dat e-identity dle Přílohy č. 2

Systém kontroly dat e-identity bude zajišťovat ověřování identity osob na základě elektronických identifikátorů, jako jsou čipové karty, biometrické údaje nebo mobilní aplikace. Tento systém bude integrován s EKV a dalšími bezpečnostními systémy pro zajištění komplexní správy přístupů.

- Čtečky e-identity: Instalace čteček pro elektronické identifikátory u vstupů do budov, včetně čipových karet a biometrických čteček.
- Centrální databáze uživatelů: Systém bude propojen s centrální databází, která bude obsahovat údaje o uživateli, včetně jejich přístupových práv a identifikátorů.
- Ověřovací proces: Systém provede ověření e-identity při každém vstupu, umožní nebo odepře přístup podle přidělených oprávnění a zaznamená událost v centrálním systému.
- Integrace s EKV a LPR: Systém e-identity bude propojen s EKV a LPR, což zajistí, že přístup k vozidlům a osobám bude synchronizován a bezpečně řízen.

3.8. Stavební úpravy technické místnosti dle Přílohy č. 2

- Návrh nezbytných stavebních úprav technických místností v každé z budov v jednotlivých areálech, zahrnující specifikace pro zajištění klimatizace, elektroinstalací, požárního zabezpečení a bezpečnostních systémů pro přístup.

3.9. Napojení na dohledové a poplachové přijímací centrum (DPPC) u každého jednotlivého areálu dle Přílohy č. 2

- Navrhnout a specifikovat systém napojení na DPPC, který umožní nepřetržité monitorování stavu zabezpečovacích a požárních systémů, přenos poplachových informací a rychlou reakci na incidenty. To zahrnuje propojení systémů PZTS, EPS a případně VSS s DPPC.
- Propojení na dohledová centra budou realizována na PČR a HZS místně příslušnými pro okamžitý výjezd bezpečnostních složek při spuštění poplachů v dané lokalitě.

3.10. Vyvedení výstupů na centralizované místo v lokalitě Hlučín dle Přílohy č. 2

- Návrh zabezpečené komunikační infrastruktury umožňující přenos dat a centrální monitorování všech systémů na vzdálené centralizované místo v lokalitě Hlučín.

3.11. Funkční požadavky na bezpečnostní systém pracující s objemovou detekcí se zobrazením na 3D mapě a jeho uživatelské rozhraní u každého jednotlivého areálu dle Přílohy č. 2

- schopnost zajistit komplexní střežení zakázaného pásma ve střežených objektech (perimetru), včetně střežení v bezprostřední blízkosti zakázaného pásma uvnitř střežených objektů (tzv. „předpoplach“), tj. vytyčená zóna o šířce individuálně nastavitelných metrů;
- schopnost zajištění plášťové ochrany určených budov, a to včetně oken, popř. dalších prostor, jejichž stavebně technické ohraničení je z hlediska bezpečnosti vyhodnoceno jako rizikové (střechy, vycházkové dvory apod.);
- schopnost zajištění komplexního střežení venkovních prostor každého jednotlivého areálu (dvory, parkoviště, prostory mezi budovami);
- autonomnost systému, tzn. poběží výhradně na vnitřním serveru bez možnosti přímého zásahu a přístupu z vnějšku (včetně servisu);
- systém musí být schopný efektivně fungovat v nepříznivých povětrnostních podmínkách jako jsou běžné sněžení, déšť nebo mlha. Detekční technologie systému by měla být navržena tak, aby minimalizovala vliv povětrnostních podmínek, a zároveň rozpoznávala extrémní situace (např. velmi hustá mlha, intenzivní déšť či sněžení). Za standardních povětrnostních podmínek, jako je běžné sněžení a déšť, bude systém nadále spolehlivě monitorovat daný prostor, i když může dojít k určitému snížení dosahu detekce. V případě extrémních meteorologických podmínek bude systém stále poskytovat informace o střeženém prostoru, avšak s omezenou kvalitou detekce. Systém by měl být schopen upozornit operátora na výskyt těchto extrémních podmínek a přizpůsobit detekční algoritmy, aby omezil šumy způsobené počasím;
- hlavní zobrazení a ovládání koncových prvků bezpečnostního systému bude vyvedeno na DPPC na centralizované místo v lokalitě Hlučín;

- druhé zobrazení a ovládání koncových prvků bezpečnostního systému s nižší úrovní přístupu bude vyvedeno na DPPC nižší úrovně v každém jednotlivém areálu.
- možnost individuálního (nezávislého) nastavení jednotlivých částí střežícího systému, ve smyslu jeho aktivace, resp. deaktivace ze strany jeho obsluhy;
- systém bude zabezpečen pro případ výpadku napájení záložním zdrojem (řádově 15 minut), s následným připojením na náhradní zdroj energie z důvodu nepřetržité funkčnosti i v případě výpadku elektrického proudu;
- možnost min. 7denního zálohování veškerých dat systému na úložišti v každém jednotlivém areálu, pro případ zpětné analýzy;
- ukládání a shromažďování dat o vzniklých závadách systému, které budou moci být dále využity při řešení servisních úkonů;
- možnost rozšíření systému o další prvky;
- vytvoření uživatelských účtů pro přihlášení více klientů;
- uživatelsky jednoduchý a variabilní ovládací systém, jehož součástí bude graficky přívětivé uživatelské prostředí ve formě 3D mapových podkladů střeženého objektu;
- neprodlená akustická i vizuální aktivace poplachu a vyrozumění DPPC v každém jednotlivém areálu a na centralizovaném místě v lokalitě Hlučín o neoprávněném pohybu osoby v určeném prostoru;
- automatické natáčení případných PTZ otočných kamer na pohybující se „narušitele“;
- v případě technicky kompatibilních otočných kamer instalovaných ve stávajícím zabezpečovacím systému organizace (VSS) možnost jejich využití bez nutnosti instalace nových kamer;
- funkce „přátelské osoby“;
- celý systém musí být v českém jazyce včetně dokumentace a příruček;
- po zprovoznění systému zajištění proškolení zaměstnanců a příslušníků Záchraného útvaru HZS ČR ovládáním a základním nastavením systému;
- u každého jednotlivého areálu musí být možnost jednosměrného vyvedení signalizace narušení na PCO (DPPC) PČR a HZS (pomocí stávajícího systému zabezpečení nebo po vlastní lince);

4. Legislativní požadavky

Příprava legislativní dokumentace: Zahrnout přípravu všech potřebných dokumentů a povolení, která jsou nezbytná pro legislativní akceptaci projektu vč. řádného a schváleného provozu jednotlivých technologií. To zahrnuje případné stavební povolení, a dále souhlasy s instalací technologií, certifikace a další právní náležitosti potřebné pro řádný provoz.

5. Finanční rozpočet

Zpracování finančního rozpočtu: Na základě projektové dokumentace vytvořit podrobný rozpočet, který bude zahrnovat všechny aspekty realizace projektu, od nákladů na materiál a instalaci po případné legislativní poplatky.

6. Závěr

Tento projekt poskytuje komplexní řešení pro ochranu jednotlivých areálů skladů, integruje různé bezpečnostní systémy a technologie do jednoho centrálně spravovaného celku. Projektant musí zajistit, aby všechny komponenty byly kompatibilní a plně integrované s centrálním monitorovacím systémem, s důrazem na bezpečnost, spolehlivost a škálovatelnost řešení. Tímto způsobem bude dosaženo maximální úrovně ochrany každého jednotlivého areálu, zaměstnanců a majetku.

Projektant je povinen zajistit, aby všechny technické návrhy byly provedeny v souladu s aktuálními normami a legislativními požadavky, a aby výsledný projekt splňoval veškeré požadavky zadavatele na funkčnost, bezpečnost a efektivitu, včetně napojení na pulty centralizované ochrany pro zajištění nepřetržitého monitorování a bezpečnosti.

Je možné využít i stávající technologie a rozvody v jednotlivých dislokovaných areálech v případě, že 100 % bez vad naplňují cíle projektu.