Příloha č. 5 – Technická dokumentace

Technická dokumentace

V souladu s ustanovením § 45 a násl. zákona č. 137/2006 Sb., o veřejných zakázkách, ve znění pozdějších předpisů, zadavatel níže vymezuje charakteristiky a požadavky na služby jednotlivých samostatných částí, které jsou předmětem veřejné zakázky.

Níže vymezené charakteristiky a požadavky zadavatele na služby stejně jako hodnoty uvedené u těchto požadavků jsou zadavatelem stanoveny jako minimální přípustné. Uchazeči proto mohou nabídnout vyšší rozsah služeb a plnění a to ve vztahu k hodnocení dle stanovených hodnotících kritérií.

V textu zadání se používají pojmy výzkum a vývoj. V případě výzkumu se má vždy na mysli průmyslový výzkum, v případě vývoje jde vždy o experimentální vývoj.

Název projektu: Podpora výzkumu v bezpečnosti pro BTKlastr

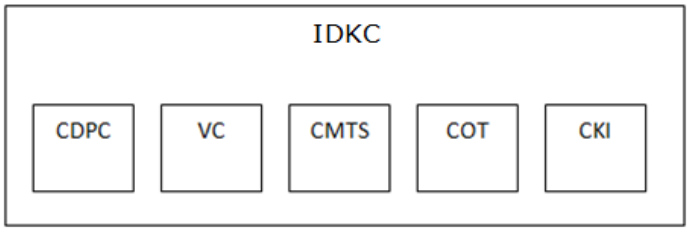
Předmětem projektu je IDKC (Integrované Dohledové a Krizové Centrum). Jde o integrační modulární systém, jehož účelem je integrace dílčích systémů tak, aby jejich ovládání bylo jednotné a umožňovalo by plnění funkcí dohledového poplachového centra, výcvikového centra, monitorování technologií i jejich ovládání, řešení EKI/KI a v budoucnu pak i dalších modulů.

Požaduje se provést průmyslový výzkum a experimentální vývoj a dodání funkčního řešení IDKC, který bude obsahovat definovaná a implementovaná základní rozhraní a funkčnosti specifikované dále tak, aby byl umožněn další rozvoj tohoto systému po jeho nabídnutí členům i nečlenům BTK.

Požadovaná architektura

Řešitel dodá systém IDKC jako softwarový modulární systém, který zajišťuje SW rozhraní a funkce k uvedeným základním částem:

- CDPC Centrální Dohledové Poplachové Centrum
- VC Výcvikové Centrum
- CMTS Centrum Monitorování Technologií a Servisu
- COT Centrum Ovládání Technologií (v základu bezpečnostních zámků)
- CKI Centrum kritické infrastruktury



Požadovaný způsob nasazení

Nasazení centrálního systému se předpokládá v serverovém technologickém centru ve virtuálním prostředí. Připojování dalších částí (jednotlivých modulů, zdrojů dat i klientských rozhraní) se požaduje přes řešitelem navržená dokumentovaná standardizovaná rozhraní.

Systém bude nasazován v následujících variantách

- Přímo u koncového uživatele jako zcela uzavřený systém. Vhodné pro velké subjekty.
- Přímo u koncového uživatele s napojením monitorování technologií CMTS na nadřazený systém (monitorování stavu hw a sw technologií, zálohování dat, vzdálená správa v případě problémů). V hodné pro velké a střední subjekty
- Provoz v centrálním technologickém centru BTK jako jeden systém s podporou pro min 500 samostatných subjektů/uživatelů při zachování plné funkčnosti. Sledování a monitorování stavu hw a sw technologií, komplexní údržba, záloha/obnova dat, provoz studené/teplé zálohy. Vše formou 24/365. V hodné pro střední a malé subjekty

Požadavky na použité technologie a komponenty

Použité technologie a všechny softwarové komponenty, z kterých bude systém po provedení výzkumu a vývoje sestaven a dodán nebo na kterých bude závislý, musí být dostupné a volně šiřitelné bez jakýchkoliv dalších poplatků za licence, atp. Jedinou výjimku tvoří použité mapové podklady.

Výzkum a vývoj IDKC se musí tedy zaměřit na operační systémy, databáze, aplikační servery a další softwarové komponenty, které mohou být dále šířeny bez dalších poplatků či licenčních nákladů.

Výkon a dostupnost

Systém musí být postaven na technologiích, které umožňují škálovatelnost výkonu systému a řešení vysoké dostupnosti pomocí clusteru aplikačních serverů.

Škálovatelností (scalability) výkonu se rozumí možnost přidat ke stávajícímu clusteru postupně jeden nebo více systémů, pokud celkové zatížení clusteru přesáhne jeho možnosti. Vysokou dostupností (high avalilability) se rozumí dostupnost služby i při výpadku některého z uzlů clusteru.

Dále se požaduje, aby dodaný systém umožňoval také vyvažování zátěže mezi uzly clusteru a její rozkládání (load balancing).

V dodávce díla IDKC musí být implementovány výše uvedené mechanismy clusteru.

Zálohování dat

Systém IDKC musí obsahovat v rámci řešení také systém zálohování a archivace dat včetně zpracovaných procesů pro obnovu těchto dat v případě havárie. Data musí být zálohována minimálně jednou denně za plného provozu systému bez jeho jakéhokoliv omezení výkonu či dostupnosti.

CDPC Centrální Dohledové Poplachové Centrum

V následujícím úvodu budou uvedeny obecné požadavky na výzkum a vývoj CDPC. Podrobná specifikace požadavků bude pak následovat pro jednotlivé moduly.

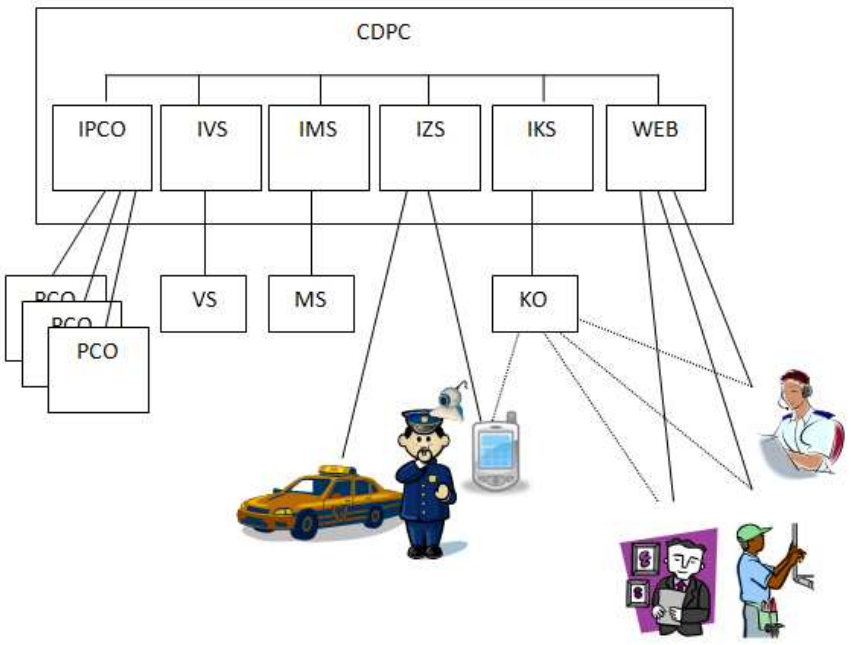
Úvod

Od modulu CDPC, který je jednou ze součástí IDKC, se požadují dodat v rámci jeho dodávky takové funkce, rozhraní a moduly, které umožní integraci:

- dílčích poplachových systémů (IPCO)
- video systémů (IVS)
- mapových systémů (IMS)
- systémů zásahových skupin (IZS)
- komunikačních systémů (IKS) různých komunikačních operátorů (KO)
- poskytování vybraných informací (WEB)

do jednoho celku s cílem

- jednotně ovládat tyto systémy
- řídit řešení poplachových událostí
- poskytovat vybrané informace zainteresovaným stranám jako jsou dispečeři, technici, členové zásahových skupin, majitelé objektů a další



V rámci integrace poplachových systémů se jedná o napojení systémů PCO (Pulty Centrální Ochrany) a jejich přijímačů zpráv. Použité protokoly přijímačů musí být standardní a požaduje se u nich

implementovaný protokol SurGard, který je jedním z nejrozšířenějších protokolů mezi přijímači zpráv a pulty centrální ochrany. V dodávky díla se požaduje napojit minimálně jeden typ PCO s minimálně jedním přijímačem zpráv a protokolem SurGard.

Integrace videosystémů v sobě zahrnuje výzkum a vývoj rozhraní, které bude sloužit pro připojování jednotlivých typů videosystémů, a připojení jednoho vybraného videosystému do CDPC.

Při řešení poplachových událostí se požadují po CDPC funkce inteligentního výběru příslušných zásahových skupin a online komunikaci s nimi. Požaduje se využít moderních komunikačních technologií k napojení online komunikačních terminálů, které budou využívat členové zásahových skupin pro navigaci při zásahu včetně získávání podrobných informací z CDPC pro zásah na daném objektu. Pro zkvalitnění dokumentace zásahu se požaduje dále vytvořit systém přenosu obrazu z personální kamery umístěné na zasahující osobě, jejíž obraz bude on-line přenášen do CDPC (přes modul integrace videosystémů), kde bude on-line používán dispečerem zásahu a archivován.

Dále se při řešení poplachových událostí dispečerem na CDPC požaduje videoverifikace poplachu, která spočívá v zobrazení posledních snímků videokamer na daném objektu s možností toto video předávat i zásahové skupině. Pro tyto účely bude určen a v dodaném modelu použit integrovaný videoserver.

V rámci požadavku na poskytování vybraných informací je požadováno vytvořit ukázkové vzorky koncových aplikací pro různé typy zainteresovaných osob. Jedná se zde o aplikace pro dispečery, manažery CDPC, techniky a montážníky v terénu, zásahové skupiny, manažery a majitele objektů a další. Zde se vždy preferuje aktivní webová aplikace s technologiemi AJAX, která bude optimalizována pro různá zařízení (monitor, tablet a smatrphone), nebo v případě nutnosti aplikace pro OS Android.

Podrobná specifikace požadavků CDPC

Dále bude uvedena podrobná specifikace požadavků k oblastem integrace, které byly uvedeny v úvodu. Budou specifikovány požadované parametry řešení.

Integrace poplachových systémů

Cílový modulární integrační systém IDKC, který se požaduje v rámci projektu vyvinout a dodat, musí v rámci svého modulu CDPC obsahovat navržené a implementované jednotné datové komunikační rozhraní, pomocí kterého se do tohoto systému dají integrovat jednotlivé typy poplachových systémů. Projekt se zaměřuje na poplachové systémy zakončené PCO (Pultem Centrální Ochrany), ale obecně lze pak integrovat do DCPC jakýkoli systém, který bude mít implementováno toto jednotné rozhraní.

Součástí dodávky je pak i realizace napojení minimálně jednoho vybraného typu PCO, do něhož řešitel naprogramuje své navržené jednotné datové rozhraní CDPC. Pomocí tohoto rozhraní bude CDPC komunikovat s PCO a jednotným způsobem zobrazovat a používat tato data v uživatelských obrazovkách CDPC (viz poskytování informací). Jednotné otevřené rozhraní PCO v CDPC musí umožňovat:

- **Přijímat a zpracovávat (odbavovat) vybrané poplachové události z tohoto PCO**. Odbavením se zde rozumí automatické založení akce, kterou pak dispečer řeší pomocí dalších modulů CDPC a jejich nástrojů. Načítá a zobrazuje podrobné informace o objektu z PCO, pomocí integrovaného systému videa verifikuje pomocí snímků z objektu daný poplach, pomocí integrovaného mapového systému a integrovaného systému zásahových skupin vysílá na objekt zásah, předává mu podrobné informace a koordinuje jej včetně jeho sledování na on-line videu. Jednotlivé kroky řešení zásahu jsou automaticky zaznamenávány včetně nahrávání hlasových komunikací integrovanými komunikačními systémy.
- **Získávat podrobná data o objektu v PCO**. Každý typ PCO má jiné struktury dat, ale pomocí implementace rozhraní s CDPC jsou tato data předávány v jednotné formě k jejich zobrazení. Součástí projektu je návrh takového rozhraní, které tato data umožní unifikovat a pracovat s nimi v CDPC jednotně na formulářích obrazovek dispečera a dalších uživatelů.
- **Vkládat nové objekty, editovat i mazat data objektu PCO a jeho konfigurace**. Požaduje se také, aby z obrazovek CDPC bylo možné data v PCO upravovat, vkládat i mazat. Jedná se pak zde jak o data administrativní jako jsou telefony a kontakty, tak i o data funkční - smyčky, sekce a další elementy objektu, převodní tabulky objektu a další. Funkční data budou na svých obrazovkách využívat
- **Získávat data událostí z archivu dat PCO**. Události, které jsou v rámci řešení poplachu i mimo něj zaznamenávány na samotném PCO, se požaduje přes rozhraní získávat k jejich použití v CDPC pro zobrazení událostí před poplachem nebo v sestavách dokumentace zásahu pro manažery CDPC.

Další požadavky na rozhraní CDPC:

- Návrh a realizace vnitřních rozhraní modulů i vnějších komunikačních rozhraní musí být **obecné, otevřené a rozšiřitelné** tak, aby šly integrovat různé datové struktury různých PCO a jednotně je pak v CDPC zobrazovat a používat
- Mezi poplachovým systémem PCO a CDPC se požaduje implementovat **šifrovaný kanál VPN**

Konkrétní požadavky pro výběr typu integrovaného PCO jsou:

- Musí být **dodán a integrován minimálně jeden typ PCO** (Pult Centrální Ochrany). Toto PCO musí být běžně prodávané PCO na trhu v ČR.
- Tento PCO musí komunikovat minimálně s **jedním typem přijímače protokolem SG-MLR2**
    - Tento přijímač musí přijímat minimálně **data z EZS typu** PARADOX ESPRIT , GALAXY HONEYWELL, MAXSYS
    - Tento přijímač musí přijímat minimálně **data z EPS typu** LITES MHU109, LITES MHU 110, ESSER 8000, 8007, 8008, Zettler Loop 500, Schrack Seconet – BMZ Integral
- PCO musí mít minimální **kapacitu** zpracování **10000** objektů, kterou je třeba doložit referenčním nasazením tohoto PCO v praxi
- PCO musí mít integrovánu datovou komunikaci se zásahovými vozy a umožňovat jejich navigaci na cíl. V zásahovém vozidle se předpokládá navigace podporující příjem příkazů (např. navigace Garmin)
- PCO musí umožňovat připojit obchůzkový systém a odbavovat jeho události

Ostatní požadavky na integrační modul CDPC:

- Kapacita připojených integrovaných PCO do CDPC je až **1000**, každé až **10000** objektů
- Modul CDPC musí být tedy dimenzován na odbavování a zpracování až **10 000 000** objektů
- Pro ověření této kapacity řešitel v rámci výzkumu a vývoje dodá testovací protokoly ze zátěžových testů

Integrace videosystémů

Integrace videa je klíčová pro splnění funkcí verifikace poplachů na objektech a také pro on-line video z personálních kamer členů zásahové jednotky. V rámci výzkumu je třeba analyzovat rozhraní a formáty současných kamerových systémů (sw a hw) a provést testy. Podle jejich výsledků pak navrhnout univerzální rozhraní k videosystémům, které pak bude použito ve vývoji a realizaci připojení těchto systémů.

Konkrétní požadavky na integraci videa jsou:

- Integrace video systémů (hw nebo sw přijímačů) s možnostmi ovládání (natáčení) kamer
- Návrh rozhraní, na které se budou jednotlivé videosystémy napojovat ovladači, které budou v rámci vývoje pro vybrané typy vyvinuty
- Praktická integrace (napojení) minimálně jednoho typu videopřijímače s podporou on-line videa od osobních kamer zásahových skupin
- Kapacita integrovaných videopřijímačů na CDPC je minimálně 1000, každý minimálně 255 kamer
- Integrovaná verifikace poplachu na CDPC (zobrazení posledních snímků videokamer na daném objektu s možností toto video předávat i zásahové skupině)

Integrace mapových systémů

Požaduje se do CDPC integrovat mapové systémy. Každý takový systém má své integrační API. Cílem projektu je v modulu integrace mapových systémů navrhnout rozhraní, se kterým budou jednotně pracovat moduly CDPC, které budou žádat spolupráci mapového systému a na toto rozhraní připojit jeden z vybraných mapových systémů.

Integrace zásahových skupin

Konkrétní požadavky na integraci zásahových skupin jsou:

- *Možnost výběru volných zásahových skupin v dispečerském rozhraní*
- *Přehled o aktuálních polohách zásahových skupin na mapovém podkladu (z integrovaného systému sledování mobilních objektů)*
- *Požaduje se podpora online komunikace s vybranou zásahovou skupinou (data, textově, hlasem) z dispečerského prostředí do terminálů zásahových skupin*
- *Požaduje se využít moderních komunikačních technologií k vytvoření online komunikačních terminálů, které budou využívat členové zásahových skupin*
- *V terminálech se požadují funkce*
    - *navigace při zásahu na předané polohy z CDPC*

- *předávání podrobných informací z CDPC pro zásah na daném objektu*
  - *textové informace, dokumentace objektu*
  - *grafika a fotografie*
  - *video z CDPC snímané z objektu*
- *komunikace s osobní kamerou, umístěnou na zasahující osobě do CDPC, a jeho odesílání do CDPC*
- *parametry snímaného obrazu minimálně 640x480 VGA 1snímek/s*

Integrace komunikačních systémů

Konkrétní požadavky na integraci komunikačních kanálů jsou:

- *Záznam logů všech textových komunikací DPDC*
- *Záznam hlasových komunikací (telefonních hovorů) DPDC*
- *Záznam video nahrávek DPDC*

Poskytování informací

Výsledkem výzkumu a vývoje modulu poskytování informací je vytvořit následující vzorové funkční obrazovky určené pro jednotlivé typy osob, které se systémem CDPC budou pracovat:

- Aplikace pro dispečera DPDC (řešení alarmů a zásahu)
  - Přístup s právy na vybrané skupiny objektů
  - Přehledová obrazovka alarmů
  - Detail parametrů napadeného objektu v jednotném formuláři
  - Funkce odbavování alarmu a změn stavu alarmu na objektu
  - Funkce komunikace se zásahovým vozem a jeho navigace na cíl
  - Funkce zobrazení videa z napadeného objektu (videoverifikace)
  - Funkce zobrazení on-line videa z personální kamery zasahující osoby
  - Funkce textové a hlasové komunikace se zasahující osobou
  - Funkce zobrazení logu komunikací s možností přehrání videa i hlasové komunikace

- *Aplikace pro technika DPDC (konfigurace objektů na PCO a jeho správa)*
- *Aplikace pro koncového zákazníka (majitele objektu) do smartphone*
  - *Zabezpečený přístup na data svých objektů (text, foto, video)*
  - *Možnost ovládání výstupů v těchto objektech*
- *Preferuje se webová aplikace, která bude optimalizována pro různá zařízení (monitor dispečera - dotykové ovládání, tablet a smatrphone), nebo aplikace pro Android*

VC Výcvikové centrum

Modul VC bude používán pro výuku a školení studentů a pracovníků v oblasti zabezpečovací techniky. Z implementačního pohledu půjde o modul CDPC vybavený simulátory jednotlivých koncových zařízení umožňující simulovat běžný provoz včetně generování běžných alarmových stavů. K těmto simulátorům musí být dodáno uživatelské rozhraní, které umožní vyučujícímu volit a generovat různé stavy včetně zpráv, odbavovaných v rámci CDPC.

Požadují se následující simulátory

- Simulátor EZS
- Simulátor EPS
- Simulátor videosystému

Data ze simulátorů musí být zpracována a následně archivována stejně, jako data z reálných zařízení.

Simulátory je možné nahradit připojením reálného zařízení. Toto zařízení však není součástí výběrového řízení a bude řešiteli zapůjčeno.

CMTS Centrum Monitorování Technologií a Servisu

Modul CMTS je určen pro monitorování hw a sw technologií v režimu 24/365.

Modul CMTS bude využíván jak pro monitorování všech dodaných modulů a komponent v rámci této dodávky, tak i externích hw a sw komponent. Obecně je požadován monitoring

- Dostupnosti serverů a zařízení
- Dostupnosti služeb na serverech a zařízeních
- Dostupnosti sítě a síťových prvků

Obecně musí být připojitelní jakékoliv zařízení podporující protokol SNMP, IPMI, JMX.

Forma uložení dat

Je preferováno uložení měřených dat do relační databáze. Uložená data musí být možné průběžně archivovat (denní záloha) a v případě potřeby obnovit ze záloh ostrá data. Pro tento účel musí být dodány nástroje pro zálohu a obnovu dat.

Oznamování událostí a vyhodnocování dat

Modul musí umožňovat uživatelskou definici událostí na základě matematických a logických operací s měřenými daty. Musí být možné zpracovávat data v čase, tzn. vyhodnocovat změny hodnot v průběhu měření (trendy). Pro zařízení stejného typu musí být možné vytvářet šablony. Součásti dodávky budou šablony pro následující systémy

- MS Windows Server, počínaje verzí 2008 a následujících
- MS Small Business Server, počínaje verzí 2007 a následujících
- MS Exchange Server, počínaje verzí 2007 a následujících
- MS Share Point Server, počínaje verzí 2010 a následujících
- MS Windows XP

- MS Windows Vista
- MS Windows 7
- MS Windows 8

Modul musí umožňovat oznámování událostí pomocí emailů a SMS. Pro každou událost musí být možné definovat způsob oznámení událostí a osoby, kterým má být informace zaslána. Informace o zaslání událostí musí být zpětně dohledatelné v rámci žurnálu modulu.

Prezentace dat

Jako klient se požaduje užití běžného internetového prohlížeče (Chrome, Internet Explorer, FireFox, atp.).

Aktuální stav sledovaných prostředků bude možno zobrazit přehledně formou dashboardu. Podrobnější informace bude možno zobrazit pomocí map, kde bude možno graficky zobrazit celou nebo část sledované infrastruktury a jejich hierarchii. Mapy bude možno tvořit pomocí nástroje, který musí být součásti dodávky.

Měřená data musí být možné zobrazovat graficky. Musí být možné vytvořit graf pro jednu měřenou veličinu a dále také pro několik měřených veličin najednou (min 10 veličin v jednom grafu). Grafy musí interaktivně umožňovat použití časového měřítka/lupy. Musí být možné zobrazit časový úsek min ½ rok (pro vyhodnocení trendů) a zároveň i časový úsek 1 hod (pro rozbor události).

Modul bezpečnostní zámek

Jde o sw modul, který zpracovává data z bezpečnostního zámku (je součástí interního výzkumu a vývoje). Bezpečnostní zámek mj. obsahuje komunikační část, která umožňuje výměnu dat mezi zámkem a nadřízeným systémem.

Popis bezpečnostního zámku

Popis vlastností bezpečnostního zámku je pouze informativní a umožňuje pochopit následující požadavky na sw modul. Není součásti tohoto výběrového řízení.

Bezpečnostní zámek je samostatné hw zařízení určené pro nasazení do hotelů a kancelářských komplexů. Obsahuje vlastní inteligenci, spolupracuje s identifikačními čipy a využívá komunikační rozhraní pro přenos dat na úrovni TCP/IP přenosů (z pohledu nadřízeného systému).

Bezpečnostní zámek obsahuje v interní paměti seznam oprávněných ID kódů, na jejichž základě se provádí otevření dveří. Použití neoprávněného ID kódu vyhodnocuje zámek jako pokus o neoprávněný vstup. Informace o oprávněném i neoprávněném vstupu přeposílá zámek asynchronně do nadřízeného systému. Není zaručeno, že informace je odeslána okamžitě po vzniku události.

Z pohledu konfigurace – nahrání oprávněných ID kódů, jsou možné dva přístupu. Nadřízený systém může posílat data přímo do bezpečnostního zámku (např. na popud obsluhy). Není však zaručeno, že je zámek schopen data přijmout - zámek může být z důvody snížení odběru odpojen od sítě. Po přihlášení do sítě se však zámek vždy automaticky zaregistruje do nadřazeného systému a ten pak může (konfigurační) data opětovně vyslat do zámku. Při odpojení od sítě zámek pošle informaci o odpojení. Není však zaručeno, že tato informace bude vždy odeslána.

Z pohledu koncové aplikace lze na zámek pohlížet jako na bezpečnostní prvek střežící oprávněný přístup do místnosti/objektu a v případě neoprávněného vstupu posílá okamžitě informaci do nadřazeného systému a zároveň jako informační prvek, kdy předává informace o příchodu osoby do místnosti se současnou identifikací osoby (přes ID kód). V poslední funkci jde o výkonový prvek, kdy na požadavek z nadřazeného systému otevře zámek a umožní vstup i bez autorizace.

Požadavky na Modul bezpečnostní zámek

Modul bezpečnostní zámek je součástí COT a je logicky rozdělen do následujících částí

Informační část Modulu řeší

- Způsob zadávání evidenci jednotlivých osob/zaměstnanců
- Přidělování ID kódů konkrétním osobám. Předpokládá se, že jedna osoba může mít větší počet ID kódů (až 250)
- ID kód může obsahovat až 24 znaků (byte)
- Přidělování přístupových práv k jednotlivým zámkům (jedna osoba může mít přístup k neomezenému počtu zámků)
- Přístupová práva jsou definována jako týdenní. Přístup je možné nastavit na libovolný den v týdnu, na každý den je možné nastavit i dobu přístupu
- Uložení informací o osobě a ID kódů v db
- Distribuci ID kódů do jednotlivých zámků
- Možnost rušení ID kódů v jednotlivých zámcích

- Distribuci časových týdenních přístupových práv do všech zámků, jejichž cfg parametry byly změněny
- Vyčtení časových týdenních přístupových práv ze všech nebo vybraných zámků a následné porovnání s údaji uložených v db
- Podpora výměny zámků (např. při poruše a následné výměně kus za kus). Po výměně musí dojít k automatickému nahrání všech cfg parametrů
- Definici master ID kódů. Každý zámek může podporovat až 32 master ID kódů. Jde pouze o logické označení ID kódů jak master (dále s touto informací pracuje pouze bezpečnostní zámek)
- Sestavy příchodů a odchodů evidovaných osob
- Evidence pracovní doby, denní, týdenní a měsíční

Střežící část Modulu řeší

- Vyhlášení poplachu při neoprávněném vstupu do místnosti (bez zadání ID kódu) – na základě obdržení konkrétní zprávy od zámku
- Vyhlášení poplachu při vstupu mimo vymezený den a čas – na základě obdržení konkrétní zprávy od zámku
- Rušení poplachu přiložením master ID kódů – na základě obdržení konkrétní zprávy od zámku
- Obecně bude k zámku přistupováno jako k bezpečnostnímu čidlu používaných ke střežení objektů (obsluha a sestavy jsou součásti řešení CDPC).

Výkonná část Modulu řeší

- Dálkové ovládání zámku (otevření dveří)
- Možnost ovládání pouze autorizovanou osobou
- Evidenci zaslání všech požadavků na otevření zámku. Eviduje se datum, čas, zámek a osoba, jenž povel vydala
- Výstupní sestavy s možností filtrace všech výstupních údajů evidence zaslání požadavků

CKI Centrum kritické infrastruktury

Jde o modul komplexního systému pro evidenci a informační podporu ochrany prvků kritické infrastruktury (KI) a evropské kritické infrastruktury (EKI).

Vytvořený nástroj podpoří proces tvorby plánů krizové připravenosti subjektu kritické infrastruktury, kde za nadstavbovou vlastnost systému lze považovat vytvoření evidenčního, analytického a plánovacího modulu a jejich propojenost na operační a integrační modul systému.

Hlavním cílem díla je zefektivnění plánovacího procesu ve vztahu k problematice ochrany kritické infrastruktury. Vytvoření díla umožní relevantnější a přehlednější zpracování plánů krizové připravenosti subjektu kritické infrastruktury a v konečném důsledku zjednodušení kontrolní činnosti gesčních orgánů.

Informační podpora ochrany kritické infrastruktury by měla přispět:

- **k optimalizaci plánovacího procesu** – zefektivní a zpřehlední tvorbu a evidenci plánů krizové připravenosti subjektu kritické infrastruktury,
- **zvýšení ochrany kritické infrastruktury** – zjednodušení a zefektivnění evidenčního, analytického a plánovacího procesu je považované za významnou optimalizaci ochrany kritické infrastruktury,
- **zefektivnění kontrolní činnosti** – jednotné prostředí zpracování plánů krizové připravenosti subjektů kritické infrastruktury umožní lepší komparaci a konfrontaci vybraných plánů s požadavky gesčních orgánů.

CKI je logicky členěn do následujících části

- Evidenční modul (EM) pro systém informační podpory ochrany kritické infrastruktury a evropské kritické infrastruktury,
- Analytický modul (AM) pro systém informační podpory ochrany kritické infrastruktury a evropské kritické infrastruktury,
- Plánovací modul (PM) pro systém informační podpory ochrany kritické infrastruktury a evropské kritické infrastruktury,
- Operační modul (OM) pro systém informační podpory ochrany kritické infrastruktury a evropské kritické infrastruktury,
- Integrační modul (IM)
-

Stručný popis jednotlivých dílčích modulů

Jednotlivé dílčí moduly jsou rozděleny do několika etap, ve kterých budou naplněny následující cíle:

- Tvorba EM systému prostřednictvím webové aplikace pro sběr dat a desktop aplikace pro správu a prezentaci evidence,
- Vytvoření AM za účelem analýzy rizik, analýzy dopadů, hodnocení zranitelnosti, katalogu příčin a seznamu opatření,
- Realizace PM ve vazbě na katalog opatření zpracovatele a katalog pro základní a operativní část plánu krizové připravenosti subjektu kritické infrastruktury,
- Vytvoření OM pro potřeby založení události, řešení události, realizaci opatření a jiných činností,
-

EM Evidenční modul

Evidenční modul systému by měl být primárně určen a fungovat jako databázový systém, který umožní editaci a evidenci relevantních dát ve vztahu k plánům krizové připravenosti subjektu kritické infrastruktury a to manuálně či formou příloh. V souvislosti s informačním naplněním tohoto modulu se bude jednat o naplnění těchto informačních potřeb:

a) Vymezení předmětu činnosti právnické nebo podnikající fyzické osoby a úkolů a opatření, které byly důvodem zpracování plánu krizové připravenosti

1) vymezení předmětu činnosti právnické nebo podnikající fyzické osoby ve vztahu k charakteru plněných opatření vyplývajících z krizového plánu,
2) identifikační údaje (název, sídlo, IČ) právnické nebo podnikající fyzické osoby,
3) přehled úkolů a opatření, které byly důvodem zpracování plánu krizové připravenosti včetně uvedení příslušného orgánu krizového řízení, který plnění úkolů a opatření požaduje,
4) seznam prvků kritické infrastruktury,
    i. V této části plánu krizové připravenosti subjektu kritické infrastruktury se uvede seznam prvků kritické infrastruktury včetně jejich identifikace (např. název, označení, lokalizace), jejichž je subjekt kritické infrastruktury provozovatelem.

b) Charakteristika krizového řízení

1) stručné vymezení organizačních částí právnické nebo podnikající fyzické osoby podílejících se na přípravě na krizové situace a jejich řešení,
2) předpokládané změny organizační struktury právnické nebo podnikající fyzické osoby nezbytné k zabezpečení činnosti za krizové situace a plnění opatření vyplývajících z krizového plánu,
3) definování orgánů vytvořených a aktivovaných za účelem řešení krizové situace a zabezpečení plnění opatření vyplývajících z krizového plánu a
4) vazby na příslušné orgány krizového řízení a krizové štáby, se kterými bude právnická nebo podnikající fyzická osoba spolupracovat při plnění opatření vyplývajících z krizového plánu.

AM Analytický modul

V rámci naplnění analytického modulu systému by mělo dojít k stanovení přehledu a hodnocení možných zdrojů rizik a analýzy ohrožení a jejich možný dopad na činnost právnické nebo podnikající fyzické osoby. Základní skutečnosti, které by měly být naplněny výzkumem:

1. Samotný proces analýzy rizik bude realizován na základě vybraných analytických metod.
2. V rámci analytického procesu budou za relevantní vstupy považovány:
    a) Katalog hrozeb,
    b) Katalog příčin,
    c) Seznam opatření,
3. Za požadované analytické procesy lze považovat:
    a) Analýzu dopadů,
    b) Analýzu zranitelností,
    c) Analýzu rizik,
4. Seznam opatření bude neupravenou databázi potenciálně využitelných opatření ve vztahu k vybraným systémům a subjektům.

PM Plánovací modul

Plánovací modul by měl umožnit relevantní naplnění požadovaných skutečností ve vztahu k naplnění operativní části plánu krizové připravenosti subjektu kritické infrastruktury. Z toho je zřejmé, že součásti této informační databázi bude:

a) Přehled opatření vyplývajících z krizového plánu příslušného orgánu krizového řízení a způsob zajištění jejich provedení

1) podrobný popis úkolů a opatření, které byly důvodem zpracování plánu krizové připravenosti,
2) vymezení konkrétních postupů realizace úkolů a opatření, které byly důvodem zpracování plánu krizové připravenosti a
3) definování předpokládaných požadavků na síly a prostředky pro realizaci úkolů a opatření, které byly důvodem zpracování plánu krizové připravenosti.
4) Stanovená opatření na ochranu prvku kritické infrastruktury
    i. V této části plánu krizové připravenosti subjektu kritické infrastruktury se uvede přehled opatření zaměřených na snížení rizika narušení funkce prvku kritické infrastruktury a dále postupy realizace těchto opatření za krizové situace.

b) Způsob zabezpečení akceschopnosti právnické nebo podnikající fyzické osoby pro zajištění provedení krizových opatření a ochrany činnosti právnické nebo podnikající fyzické osoby

1) popis systému fyzické ochrany právnické nebo podnikající fyzické osoby se zaměřením na fyzickou ostrahu, technickou ochranu a režimová opatření,
2) zabezpečení provedení změny organizační struktury právnické nebo podnikající fyzické osoby za krizové situace,

3) zabezpečení způsobu komunikace organizačních částí právnické nebo podnikající fyzické osoby za krizové situace a
4) definování odpovědných osob včetně uvedení pravomocí a způsobu jejich aktivace při plnění opatření vyplývajících z krizového plánu za krizové situace.

c) Postupy řešení krizových situací identifikovaných v analýze ohrožení

1) definování plánovaných opatření v působnosti právnické nebo podnikající fyzické osoby (včetně uvedení odpovědnosti za jejich provedení) realizovaných za účelem řešení krizové situace a
2) předpokládané požadavky na síly a prostředky nezbytné k řešení krizové situace u právnické nebo podnikající fyzické osoby.

d) Plán opatření hospodářské mobilizace u dodavatelů mobilizační dodávky

1) V této části plánu krizové připravenosti se v souladu s § 2 odst. 1 písm. f) zákona č. 241/2000 Sb., o hospodářských opatřeních pro krizové stavy a o změně některých souvisejících zákonů, uvede plán opatření hospodářské mobilizace. Zpracovatelem plánu opatření hospodářské mobilizace je v souladu s § 15 zákona č. 241/2000 Sb. pouze dodavatel mobilizační dodávky.

e) Přehled spojení na příslušné orgány krizového řízení

1) V přehledu spojení se uvede seznam telefonních kontaktů a elektronických adres na příslušné orgány krizového řízení a další subjekty podílející se na připravenosti na krizové situace a jejich řešení, případně na subjekty podílející se na zajištění opatření vyplývajících z krizového plánu za krizové situace. V případě kontaktních údajů na konkrétní osobu se uvedou údaje nezbytné pro identifikaci této osoby včetně vykonávané funkce a zařazení.
2) Pro jiný způsob spojení než ten, který je uveden v odstavci 1 (např. rádiové spojení, osobní spojky) se v této části plánu krizové připravenosti uvede také jeho popis a struktura.
3) V případě, že je přehled spojení na příslušné orgány krizového řízení a další subjekty podílející se na připravenosti na krizové situace a jejich řešení, případně na subjekty podílející se na zajištění opatření vyplývajících z krizového plánu za krizové situace uveden v jiné plánovací dokumentaci, uvede se v této části plánu krizové připravenosti pouze příslušný odkaz.

f) Přehled plánů zpracovávaných podle zvláštních právních předpisů využitelných při řešení krizových situací

Operační modul

Operační modul by měl primárně umožnit relevantní reakci na nežádoucí jev mající potenciální vliv na funkční kontinuitu systému kritické infrastruktury nebo evropské kritické infrastruktury. Lze proto předpokládat, že mezi základní požadavky lze stanovit:

1) Procesní realizaci založení události,
2) Proces řešení události ve vztahu k formulaci:
    a) Opatření,
    b) Činností,
3) Zajištění komunikačních úkolů.

Pol.	Typ VV	Popis položky	Specifikace	Etapa	Časová náročnost
CDPC a CMTS					
I-1	PV	Průmyslový výzkum zabývající se obecným popisem PCO	Formou průmyslového výzkumu je požadováno provést podrobný popis PCO, jeho vlastnosti a funkcí. Výsledek rozboru - Přehled dostupných systémů užívaných v ČR - Popis vlastností a funkcí PCO	I.	
I-2	PV	Průmyslový výzkum zaměřený na popis procesů zavedení BA, uživatele, objektu	Formou průmyslového výzkumu je požadováno provést podrobný popis procesu zavedení uživatele (např. BA, obecní úřad,…), subjektu a jeho monitorovacích prostředků. Výsledek rozboru - Údaje, které je nutné pro zavedení do systému získat od zákazníka a dále způsob, jakým způsobem (formou) informace po zákazníkovi požadovat. - Navrhované postupy pro zavádění těchto dat do systému, případně způsoby, jak tyto informace získat z jiných IS.	I.	
I-3	PV	Průmyslový výzkum zaměřený na popis procesů instalace zařízení u zákazníků	Formou průmyslového výzkumu je požadováno provést podrobný popis procesu instalace a nastavení koncových zařízení (ESZ, EPS, komunikátory) u zákazníka. Výsledek rozboru - Popis současného systému instalace u zákazníka, způsoby evidence - Návrh postupů instalace a konfigurace s ohledem na snížení nákladů na instalaci - Návrh způsobu evidence instalovaných zařízení	I.	
I-4	PV	Průmyslový výzkum zaměřený zjišťování kvality a poruchovosti	Formou průmyslového výzkumu je požadováno provést podrobný popis zjišťování kvality a poruchovosti výrobků a poskytovaných služeb. Výsledek rozboru - Popis (z pohledu kvality) kritických výrobků a konzumovaných služeb - Návrh pro zkvalitnění fce výrobků a služeb	I.	

		zařízení			
I-5	PV	Průmyslový výzkum zaměřený na návrh datového rozhraní	Formou průmyslového výzkumu je požadováno provést analýzu a návrh obecného datového rozhraní umožňující integraci - dílčích poplachových systémů (IPCO) - video systémů (IVS) - mapových systémů (IMS) - systémů zásahových skupin (IZS) - komunikačních systémů (IKS) různých komunikačních operátorů (KO) - poskytování vybraných informací (WEB) Cílem je návrh jednoho celku umožňující - jednotně ovládat tyto systémy - řídit řešení poplachových událostí - poskytovat vybrané informace zainteresovaným stranám jako jsou dispečeři, technici, členové zásahových skupin, majitelé objektů a další	I.	
I-6	PV	Průmyslový výzkum zaměřený na návrh datového rozhraní CDPC	Formou průmyslového výzkumu je požadováno provést analýzu a návrh jednotného datového komunikačního rozhraní, pomocí kterého se do tohoto systému dají integrovat jednotlivé typy poplachových systémů. Projekt se zaměřuje na poplachové systémy zakončené PCO, ale obecně lze pak integrovat do DCPC jakýkoli systém, který bude mít implementováno toto jednotné rozhraní. Jednotné otevřené rozhraní PCO v CDPC musí umožňovat - Přijímat a zpracovávat (odbavovat) vybrané poplachové události z tohoto PCO - Získávat podrobná data o objektu v PCO - Vkládat nové objekty, editovat i mazat data objektu PCO a jeho konfigurace - Získávat data událostí z archivu dat PCO - Rozšiřitelnost tak, aby šly integrovat různé datové struktury různých PCO a jednotně je pak v CDPC zobrazovat a používat - šifrovaný kanál VPN mezi poplachovým systémem PCO a CDPC Kapacitní požadavky na integrační modul CDPC: - Kapacita připojených integrovaných PCO do CDPC je až 1000, každé až 10000 objektů - Modul CDPC musí být tedy dimenzován na odbavování a zpracování až 10 000 000 objektů Návrh bude obsahovat	I.	

			- popis navrhovaného rozhraní - popis jednotlivých datových položek - informaci o předpokládané propustnosti navrhovaného rozhraní		
I-7	PV	Průmyslový výzkum zaměřený na návrh integrace videosystémů	Formou průmyslového výzkumu je požadováno provést analýzu a návrh integrace videosystémů. Požadavky na integraci videa - Integrace video systémů (hw nebo sw přijímačů) s možnostmi ovládání (natáčení) kamer - Návrh rozhraní, na které se budou jednotlivé videosystémy napojovat ovladači, které budou v rámci vývoje pro vybrané typy vyvinuty - Praktická integrace (napojení) minimálně jednoho typu videopřijímače s podporou on-line videa od osobních kamer zásahových skupin - Kapacita integrovaných videopřijímačů na CDPC je minimálně 1000, každý minimálně 255 kamer - Integrovaná verifikace poplachu na CDPC (zobrazení posledních snímků videokamer na daném objektu s možností toto video předávat i zásahové skupině) Návrh bude obsahovat - Popis formátů současných kamerových systémů (sw a hw) - Návrh rozhraní - Informaci o předpokládané propustnosti navrhovaného rozhraní	I.	
I-8	PV	Průmyslový výzkum zaměřený na návrh integrace mapových systémů	Formou průmyslového výzkumu je požadováno provést analýzu a návrh integrace existujících mapových systémů Návrh bude obsahovat - Popis vybraných rozhraní existujících mapových systémů - Popis navrhovaného rozhraní umožňujícího integraci map. systémů - Informaci o předpokládané propustnosti navrhovaného rozhraní	I.	
I-9	PV	Průmyslový výzkum zaměřený na návrh integrace zásahových skupin	Formou průmyslového výzkumu je požadováno provést analýzu a návrh integrace zásahových skupin. Rozhraní musí umožňovat - Možnost výběru volných zásahových skupin v dispečerském rozhraní - Přehled o aktuálních polohách zásahových skupin na mapovém podkladu (z integrovaného systému sledování mobilních objektů) - Požaduje se podpora online komunikace s vybranou zásahovou skupinou (data,	I.	

			textově, hlasem) z dispečerského prostředí do terminálů zásahových skupin - Požaduje se využít moderních komunikačních technologií k vytvoření online komunikačních terminálů, které budou využívat členové zásahových skupin - V terminálech se požadují funkce o navigace při zásahu na předané polohy z CDPC o předávání podrobných informací z CDPC pro zásah na daném objektu ▪ textové informace, dokumentace objektu ▪ grafika a fotografie ▪ video z CDPC snímané z objektu o komunikace s osobní kamerou, umístěnou na zasahující osobě do CDPC, a jeho odesílání do CDPC o parametry snímaného obrazu minimálně 640x480 VGA 1snímek/s Návrh bude obsahovat - Popis navrhovaného rozhraní umožňujícího integraci zásahových skupin - Informaci o předpokládané propustnosti navrhovaného rozhraní		
I-10	PV	Průmyslový výzkum zaměřený na návrh komunikačních systémů	Formou průmyslového výzkumu je požadováno provést analýzu a návrh integrace komunikačních systémů. Je požadováno zajistit záznam a uložení - Textových logů komunikací DPDC - Hlasových komunikací (telefonních hovorů) DPDC - Záznamu video nahrávek DPDC Návrh bude obsahovat - Popis navrhovaného rozhraní umožňujícího integraci komunikačních rozhraní - Informaci o předpokládané propustnosti navrhovaného rozhraní	I.	
I-11	PV	Průmyslový výzkum zaměřený na návrh modulu poskytování informací	Formou průmyslového výzkumu je požadováno provést analýzu a návrh integrace modulu poskytování informací Je požadována následující funkčnost - Aplikace pro dispečera DPDC (řešení alarmů a zásahu) o Přístup s právy na vybrané skupiny objektů o Přehledová obrazovka alarmů o Detail parametrů napadeného objektu v jednotném formuláři o Funkce odbavování alarmu a změn stavu alarmu na objektu	I.	

			o Funkce komunikace se zásahovým vozem a jeho navigace na cíl o Funkce zobrazení videa z napadeného objektu (videoverifikace) o Funkce zobrazení on-line videa z personální kamery zasahující osoby o Funkce textové a hlasové komunikace se zasahující osobou o Funkce zobrazení logu komunikací s možností přehrání videa i hlasové komunikace - Aplikace pro technika DPDC (konfigurace objektů na PCO a jeho správa) - Aplikace pro koncového zákazníka (majitele objektu) do smartphone o Zabezpečený přístup na data svých objektů (text, foto, video) o Možnost ovládání výstupů v těchto objektech - Preferuje se (webová) aplikace, která bude optimalizována pro různá zařízení (monitor dispečera – dotykové ovládání, tablet a smatrphone), nebo aplikace pro Android Návrh bude obsahovat - Popis navrhovaného rozhraní umožňujícího integraci modulu poskytování informací - Informaci o předpokládané propustnosti navrhovaného rozhraní		
I-12	PV	Průmyslový výzkum zaměřený na VC	Formou průmyslového výzkumu je požadováno provést návrh Výcvikového centra, způsobu simulace následujících zařízení - EZS - EPS - Videosystému	I.	
I-13	PV	Průmyslový výzkum zabývající se obecným popisem monit. systémů	Formou průmyslového výzkumu je požadováno provést podrobný popis PCO, jeho vlastnosti a funkcí. Výsledek rozboru - Popis dostupných monitorovacích systémů na trhu - Popis jejich vlastností a funkcí - Popis způsobu reportování incidentů a jejich zpravování	I.	
I-14	PV	Průmyslový výzkum zaměřený na vývoj CMTS	Formou průmyslového výzkumu je požadováno provést návrh vývoje a použití CMTS s podporou - Protokolů SNMP, IPMI, JMX - Uživatelských definici událostí na základě matematických a logických operací s měřenými daty	I.	

			- Časové rozlišitelností sledovaných veličin min. 1hod – ½ roku. - Předefinovaných šablon		
I-15	EV	Experimentální vývoj zaměřený na implementaci datového rozhraní	Formou experimentálního vývoje je požadováno provést implementaci obecného datového rozhraní navrženého dle úkolu I-5 Součástí implementace jsou i testy	II.	
I-16	EV	Experimentální vývoj zaměřený na implementaci datového rozhraní CDPC	Formou experimentálního vývoje je požadováno provést implementaci jednotného datového komunikačního rozhraní dle úkolu I-6 Součástí implementace jsou i testy	II.	
I-17	EV	Experimentální vývoj zaměřený na implementaci integrace videosystémů	Formou experimentálního vývoje je požadováno provést implementaci integrace videosystémů dle úkolu I-7. Součástí implementace jsou i testy	II.	
I-18	EV	Experimentální vývoj zaměřený implementaci integrace mapových systémů	Formou experimentálního vývoje je požadováno provést implementaci integrace existujících mapových systémů dle úkolu I-8 Součástí implementace jsou i testy	II.	
I-19	EV	Experimentální vývoj zaměřený na implementaci integrace zásahových	Formou experimentálního vývoje je požadováno provést analýzu a návrh integrace zásahových skupin dle úkolu I-9 Součástí implementace jsou i testy	II.	

		skupin			
I-20	EV	Experimentální vývoj zaměřený na implementaci komunikačních systémů	Formou experimentálního vývoje je požadováno provést implementaci integrace komunikačních systémů dle úkolu I-10 Součástí implementace jsou i testy	II.	
I-21	EV	Experimentální vývoj zaměřený na implementaci modulu poskytování informací	Formou experimentálního vývoje je požadováno provést implementaci integrace modulu poskytování informací dle úkolu I-11 Součástí implementace jsou i testy	II.	
I-22	EV	Experimentální vývoj zaměřený na implementaci VC	Formou experimentálního vývoje je požadováno implementaci Výcvikového centra, simulace následujících zařízení - EZS - EPS - Videosystému	II.	
I-23	EV	Experimentální vývoj zaměřený na implementaci CMTS	Formou experimentálního vývoje je požadováno provést implementaci CMTS s podporou - Protokolů SNMP, IPMI, JMX - Uživatelských definici událostí na základě matematických a logických operací s měřenými daty - Časové rozlišitelností sledovaných veličin min. 1hod – ½ roku. - Předefinovaných šablon	II.	
COT (bezpečnostní zámek)					
II-1	PV	Průmyslový výzkum zabývající se obecným popisem informačními	Formou průmyslového výzkumu je požadováno provést popis vlastností inteligentních zámků z hlediska zpracovávaných informací a informací zasílaných do nadřazených systémů, včetně případných norem a standardů používaných u inteligentních zámků. Výsledek rešerše bude použit pro následný návrh řešení	I.	

		vlastnostmi zámků			
II-2	PV	Průmyslový výzkum zaměřený na popis procesů evidence osobních údajů	Formou průmyslového výzkumu je požadováno provést podrobný popis způsobu získávání a evidence osobních údajů osob používající přístup k zámku nebo více zámkům. Především je nutné respektování v současnosti platné zákonné ustanovení o nakládání s osobními údaji. Výsledky rozboru budou použity pro následný návrh řešení	I.	
II-3	PV	Průmyslový výzkum zaměřený na návrh datového rozhraní	Formou průmyslového výzkumu je požadováno provést analýzu a návrh datového rozhraní umožňující integraci dat z bezpečnostního zámku do - Existujících docházkových systémů - Poplachových systémů (IPCO) - Poskytování vybraných informací (např. prostřednictvím webu)	I.	
II-4	PV	Průmyslový výzkum zaměřený na návrh Informační části modulu	Formou průmyslového výzkumu je požadováno provést analýzu a návrh Informační části modulu. Musí obsahovat - Způsob zadávání evidenci jednotlivých osob/zaměstnanců - Přidělování ID kódů konkrétním osobám. Předpokládá se, že jedna osoba může mít větší počet ID kódů (až 250) - Přidělování přístupových práv k jednotlivým bez. zámkům - Definice přístupová práva formou týdenního nastavování - Uložení informací o osobě a ID kódů v db - Distribuci ID kódů do jednotlivých zámků - Možnost rušení ID kódů v jednotlivých zámcích - Distribuci časových týdenních přístupových práv do všech zámků, jejichž cfg parametry byly změněny - Vyčtení časových týdenních přístupových práv ze všech nebo vybraných zámků a následné porovnání s údaji uložených v db - Podpora výměny zámků (např. při poruše a následné výměně kus za kus). Po výměně musí dojít k automatickému nahrání všech cfg parametrů - Definici master ID kódů. - Sestavy příchodů a odchodů evidovaných osob - Evidence pracovní doby, denní, týdenní a měsíční - Uživatelské rozhraní	I.	

II-5	PV	Průmyslový výzkum zaměřený na návrh Střežící části modulu	Formou průmyslového výzkumu je požadováno provést analýzu a návrh Informační části modulu. Musí obsahovat - Vyhlášení poplachu při neoprávněném vstupu do místnosti (bez zadání ID kódu) – na základě obdržení konkrétní zprávy od zámku - Vyhlášení poplachu při vstupu mimo vymezený den a čas – na základě obdržení konkrétní zprávy od zámku - Rušení poplachu přiložením master ID kódů – na základě obdržení konkrétní zprávy od zámku - Obecně bude k zámku přistupováno jako k bezpečnostnímu čidlu používaných ke střežení objektů (obsluha a sestavy jsou součásti řešení CDPC) - Uživatelské rozhraní	I.	
II-6	PV	Průmyslový výzkum zaměřený na návrh Výkonné části modulu	Formou průmyslového výzkumu je požadováno provést analýzu a návrh Informační části modulu. Musí obsahovat - Způsob dálkové ovládání zámku (otevření dveří) - Možnost dálkového ovládání zámku pouze autorizovanou osobou - Evidenci zaslání všech požadavků na otevření zámku. Eviduje se datum, čas, zámek a osoba, jenž povel vydala - Výstupní sestavy s možností filtrace všech výstupních údajů evidence zaslání požadavků - Uživatelské rozhraní	I.	
II-7	EV	Experimentální vývoj návrhu Informační části modulu	Formou experimentálního vývoje provést implementaci Informační části modulu bezpečnostního zámku dle úkolu II-4. Součástí implementace jsou i testy	II.	
II-8	EV	Experimentální vývoj zaměřený návrhu Střežící části modulu	Formou experimentálního vývoje provést implementaci Střežící části modulu bezpečnostního zámku dle úkolu II-5. Součástí implementace jsou i testy	II.	
II-9	EV	Experimentální vývoj návrhu Výkonné části modulu	Formou experimentálního vývoje provést implementaci Výkonné části modulu bezpečnostního zámku dle úkolu II-6. Součástí implementace jsou i testy	II.	

CKI					
III-1	PV	Průmyslový výzkum k tvorbě evidenčního modulu pro systém informační podpory ochrany KI a EKI	Evidenční modul systému by měl být primárně určen a fungovat jako databázový systém, který umožní editaci a evidenci relevantních dát ve vztahu k plánům krizové připravenosti subjektu kritické infrastruktury a to manuálně či formou příloh	I.	
III-2	PV	Průmyslový výzkum ve vztahu k tvorbě analytického modulu pro systém informační podpory ochrany KI a EKI	V rámci naplnění analytického modulu systému by mělo dojít k stanovení přehledu a hodnocení možných zdrojů rizik a analýzy ohrožení a jejich možný dopad na činnost právnické nebo podnikající fyzické osoby	I.	
III-3	PV	Průmyslový výzkum ve vztahu k tvorbě plánovacího modulu pro systém informační podpory ochrany KI a EKI	Plánovací modul by měl umožnit relevantní naplnění požadovaných skutečností ve vztahu k naplnění operativní části plánu krizové připravenosti subjektu kritické infrastruktury.	I.	
III-3.1	PV	Průmyslový výzkum ve vztahu k tvorbě plánovacího modulu pro	Výsledkem výzkumu bude: Přehled opatření vyplývajících z krizového plánu příslušného orgánu krizového řízení a způsob zajištění jejich provedení	I.	

		systém informační podpory ochrany KI a EKI			
III-3.2	PV	Průmyslový výzkum ve vztahu k tvorbě plánovacího modulu pro systém informační podpory ochrany KI a EKI	Výsledkem výzkumu bude: Způsobu zabezpečení akceschopnosti právnické nebo podnikající fyzické osoby pro zajištění a provedení krizových opatření a ochrany činnosti právnické nebo podnikající fyzické osoby	I.	
III-3.3	PV	Průmyslový výzkum ve vztahu k tvorbě plánovacího modulu pro systém informační podpory ochrany KI a EKI	Výsledkem výzkumu bude: Postupy řešení krizových situací identifikovaných v analýze ohrožení	I.	
III-3.4	PV	Průmyslový výzkum ve vztahu k tvorbě plánovacího modulu pro systém informační podpory ochrany KI a EKI	Výsledkem výzkumu bude: Plán opatření hospodářské mobilizace u dodavatelů mobilizační dodávky	I.	
III-3.5	PV	Průmyslový výzkum ve	Výsledkem výzkumu bude: Přehled spojení na příslušné orgány krizového řízení	I.	

		vztahu k tvorbě plánovacího modulu pro systém informační podpory ochrany KI a EKI			
III-3.6	PV	Průmyslový výzkum ve vztahu k tvorbě plánovacího modulu pro systém informační podpory ochrany KI a EKI	Výsledkem výzkumu bude: Přehled plánů zpracovávaných podle zvláštních právních předpisů využitelných při řešení krizových situací	I.	
III-4	PV	Průmyslový výzkum k tvorbě operačního modulu pro systém informační podpory ochrany KI a EKI	Operační modul by měl primárně umožnit relevantní reakci na nežádoucí jev mající potenciální vliv na funkční kontinuitu systému kritické infrastruktury nebo evropské kritické infrastruktury	I.	
III-5	EV	Experimentální vývoj k implementaci evidenčního modulu pro systém informační podpory ochrany KI a EKI	Experimentální vývoj by měl umožnit integraci a propojení jednotlivých modulů ve vztahu k naplnění požadavků ve vazbě na informační potřeby a podporu ochrany kritické infrastruktury a evropské kritické infrastruktury	II.	

III-6	EV	Experimentální vývoj k implementaci analytického modulu pro systém informační podpory ochrany KI a EKI	Experimentální vývoj analytického modulu by měl umožnit stanovení přehledu a hodnocení možných zdrojů rizik a analýzy ohrožení a jejich možný dopad na činnost právnické nebo podnikající fyzické osoby	II.	
III-7	EV	Experimentální vývoj k implementaci plánovacího modulu pro systém informační podpory ochrany KI a EKI	Experimentální vývoj plánovacího modulu by měl zajistit relevantní naplnění požadovaných skutečností ve vztahu k naplnění operativní části plánu krizové připravenosti subjektu kritické infrastruktury.	II.	
III-7.1	EV	Experimentální vývoj k implementaci plánovacího modulu pro systém informační podpory ochrany KI a EKI	Lze ve vztahu k struktuře plánovacího modulu požadovat: Aby součásti analytického modulu byli procesní bloky pro: a. Katalog opatření, b. Katalog zpracovatele, c. Katalog pro základní část plánu krizové připravenosti subjektu kritické infrastruktury, d. Katalog pro operativní část plánu krizové připravenosti subjektu kritické infrastruktury,	II.	
III-7.2	EV	Experimentální vývoj k implementaci plánovacího modulu pro systém	Lze ve vztahu k struktuře plánovacího modulu požadovat: Přímé propojení katalogu zpracovatele s evidenčním modulem systému,	II.	

		informační podpory ochrany KI a EKI			
III-7.3	EV	Experimentální vývoj k implementaci plánovacího modulu pro systém informační podpory ochrany KI a EKI	Lze ve vztahu k struktuře plánovacího modulu požadovat: Informační propojení a dotace katalogu pro základní část plánu krizové připravenosti subjektu kritické infrastruktury s modulární části katalogu zpracovatele, katalogu hrozeb a procesního bloku analýzy rizik	II.	
III-7.4	EV	Experimentální vývoj k implementaci plánovacího modulu pro systém informační podpory ochrany KI a EKI	Lze ve vztahu k struktuře plánovacího modulu požadovat: Aby katalog pro operativní část plánu krizové připravenosti subjektu kritické infrastruktury byl z pohledu vstupů propojen na katalog opatření a evidenční modul a umožní vkládat i: a. Plán opatření hospodářské mobilizace u dodavatelů mobilizační dodávky b. Přehled plánů zpracovávaných podle zvláštních právních předpisů využitelných při řešení krizových situací	II.	
III-7.5	EV	Experimentální vývoj k implementaci plánovacího modulu pro systém informační podpory ochrany KI a EKI	Lze ve vztahu k struktuře plánovacího modulu požadovat: Výstupy plánovacího modulu ve vztahu ke katalogu pro operativní část plánu krizové připravenosti subjektu kritické infrastruktury budou propojeny s operačním modulem	II.	
III-8	EV	Experimentální vývoj k implementaci	Experimentální vývoj operačního modulu by měl primárně umožnit relevantní reakci systému ve vztahu k nežádoucímu jevu mající degradační potenciální na funkční kontinuitu systému kritické infrastruktury nebo evropské kritické infrastruktury.	II.	

		operačního modulu pro systém informační podpory ochrany KI a EKI			
III-8.1	EV	Experimentální vývoj k implementaci operačního modulu pro systém informační podpory ochrany KI a EKI	Základní části operačního modulu budou: Procesní bloky pro: a. Založení události, b. Řešení události, opatření, činnosti, c. Komunikační úkoly	II.	
III-8.2	EV	Experimentální vývoj k implementaci operačního modulu pro systém informační podpory ochrany KI a EKI	Základní části operačního modulu budou: Systém umožňující propojení operačního modulu systému s integračním modulem systému a to v rámci funkčních bloků komunikační úkoly a integrace GPS a současně integrace DPPC a řešení události, opatření, činnosti	II.	
III-9	EV	Experimentální vývoj k implementaci integračního modulu pro systém informační podpory ochrany KI a EKI	Experimentální vývoj integračního modulu by měl vycházet z formulace příčin vzniku vybraných hrozeb, kde právě vybrané systémy PZTS, DPPC, GPS nebo GSM umožní generovat poplachové správy a tím sledovat vznik příčiny nežádoucího jevu. Pro potřeby relevantní reakce se předpokládá propojenost na operační modul systému.	II.	

III-9.1	EV	Experimentální vývoj k implementaci integračního modulu pro systém informační podpory ochrany KI a EKI	Požaduje se, aby součásti analytického modulu byly: Procesní bloky pro: a. Integraci 2D a 3D GIS, b. Integraci CCTV, c. Integraci DPPC, d. Integraci GPS.	II.	
III-9.2	EV	Experimentální vývoj k implementaci integračního modulu pro systém informační podpory ochrany KI a EKI	Požaduje se, aby součásti analytického modulu byla: Propojenost analytického modulu s integračním modulem prostřednictvím funkčního bloků katalog příčin	II.	