

Příloha č. 1 – Rámcový popis předmětu plnění

OBSAH:

Funkční požadavky	2
User Management a Asset Management	2
Event management, business logika.....	3
Video management a detekce	4
Interaktivní přehledová mapa.....	5
Ostatní požadavky na dodané software řešení.....	6
Požadavky na implementaci	6
Zprovoznění IDP	6
Testovací a ověřovací provoz IDP	7
Testované funkcionality:	7
Školení uživatelů	7
Migrace monitoringu užšího centra města.....	8
Migrace kamerových streamů	8
Migrace dat a jejich vizualizace.....	8
Požadavky na implementaci	8

Integrační datová platforma (IDP)

Cílem projektu je vytvoření vizualizační, procesní a datové integrační platformy podporující rozvoj digitálních služeb, založených na sběru a zpracování dat z různých průmyslových a IT systémů města a městských organizací (dále jen Integrační datová platforma, nebo IDP).

IDP bude představovat serverový informační systém, jehož vlastníkem bude město Český Krumlov a se kterým budou pracovat i další městem zřízené a založené organizace. Provoz a správu IDP budou zajišťovat IT pracovníci města Český Krumlov.

IDP bude plnit úlohu nadřazeného systému umožňujícího datovou a procesní integraci různých i autonomních systémů. Přinese nástroje pro sběr, správu a zpracování dat a událostí z napojených systémů a zajistí komplexní přehled o aktuální situaci napříč městskými infrastrukturami. Nabídne nástroje pro zefektivnění operačních postupů a řešení mimořádných situací v různých oblastech a organizacích.

IDP zajistí možnost aktivně pracovat s informacemi v souvislostech a využívat je při automatizaci procesů napříč jednotlivými autonomními systémy, pomocí předem připravených scénářů a průběžného vyhodnocování odchylek od běžného stavu v reálném čase.

IDP bude zobrazovat relevantní informace z více systémů přehledně na jednom místě. Pro názorné pochopení souvislostí umožní interpretovat i prostorová data a většinu souvisejících informací v mapových nebo jiných grafických podkladech.

Systém IDP bude implementován na nově vytvořené infrastruktuře, umístěné v serverovně v prostorách Městské policie na autobusovém nádraží, která bude vybavena pro provoz IDP a připojena k metropolitní optické síti.

SW řešení pro IDP musí být tvořeno backend (IDP server) a frontend (IDP klient) částmi, kde frontend část musí být realizována formou desktop či webové aplikace a musí mít jednotné uživatelské rozhraní, ve kterém budou pracovat veškerí koncoví uživatelé, bez nutnosti přepínání mezi více různými a nejednotnými SW aplikacemi / klienty.

IDP server bude instalován v serverovně umístěné v prostorách Městské policie na autobusovém nádraží. Přístup k IDP bude možný min. na třech pracovištích, které budou využívat IDP klienty (Městská policie, Městský úřad, Českokrumlovský rozvojový fond, spol. s r.o.). Počet pracovišť se v budoucnu může rozšiřovat, proto musí IDP server umožnit budoucí napojení dalších IDP klientů.

IDP server musí do budoucna umožnit také integraci dalších technologií nad rámec tohoto zadání, jako jsou informační systémy města, parkovací systémy, kamerové systémy, aplikace využívané v rámci řízení dopravy, dohledové systémy Služeb Města Český Krumlov, systémy IoT a další.

Funkční požadavky

User Management a Asset Management

IDP budou využívat uživatelé z různých organizací, k různým činnostem. Musí proto nabídnout možnost pokročilého nastavení uživatelských práv, přístupů ke zdrojům připojeným k IDP, nebo nastavení rozsahu a způsobu zobrazovaných dat (individuální pohledy pro uživatele, nebo jinak definované skupiny uživatelů). Cílem IDP je poskytnout jednotné, uživatelsky přehledné a přívětivé rozhraní pro správu integrovaných prvků a systémů z jednoho místa pomocí klávesnice a jedné myši. Včetně dispečerských nástrojů, které zajistí lepší přehled díky možnosti využívat více monitorů, nebo případně budoucí centralizaci formou centrálního dispečinku.

Uživatelé budou pracovat s velkým počtem připojených prvků a systémů, průmyslových a IoT zařízení, kamerových prvků, s ITS technologiemi, informačními panely a dalšími koncovými prvky. K tomu je nutné, aby systém umožňoval správu těchto připojených zařízení, správu technických informací o zařízeních, kontrolu nad vzdálenými zařízeními (ovládání kamer, předávání kamer na základě definovaných oprávnění), správu geoinformací (poloha, pohyb, změna stavu), a real-time zobrazení stavových informací.

- Musí umožňovat současnou práci min. 3 uživatelů s aktivním přístupem (plná funkcionalita) a min. dalších 10 pracovníků s pasivním přístupem (konzumace reportů, vlastní dashboardy, bez potřeby administrátorských práv na změnu systémového nastavení). Je-li tato funkcionalita licencována, musí být licence součástí dodávky.
- Přístup uživatelů do IDP (autorizace) musí být založen na volně definovaných oddělených rolích s možností přidělování práv v rámci role podle zdrojů dat, skupiny zařízení apod. Typ přístupu je definován interně v dodávaném SW řešení

- Autentizace uživatelů musí probíhat pomocí integrace s Microsoft Active Directory a musí umožňovat přihlašování pomocí lokálních účtů (v případě nedostupnosti Microsoft Active Directory).
- Definice oprávnění jednotlivých uživatelů IDP na základě příslušnosti do předem nadefinovaných skupin/rolí.
- Systém bude umožňovat audit chování uživatelů a mechanismus zamezení neautorizovaných změn v konfiguraci SW řešení.
- Musí umožnit evidenci informací o připojených zařízeních a systémech, včetně zobrazení real-time informací,
- Musí umožnit zobrazení profilu daného připojeného zařízení nebo systému a filtrování reportu za daný prvek, systém.

Event management, business logika

Je požadováno, aby byla IDP navržena jako systém využívající událostmi řízenou architekturu a využívala principu vytváření, detekce, zpracování a reakcí na události. Každá integrovaná technologie v rámci tohoto zadání, ale i do budoucna bude z pohledu IDP zdrojem dat a událostí, které systém zpracovává. Informace přijaté z integrovaných technologií budou kategorizovány, ukládány a poté předávány k dalšímu zpracování. IDP proto musí nabízet nástroje, které umožní vytvářet logické postupy a automatizovat procesy, jako je například Rule Engine, nebo workflow, které dokáží zpracovat události a informace vstupující do systému podle přednastavených pravidel a podmínek. Tyto nástroje musí být součástí IDP a přístupné pro uživatele prostřednictvím IDP klienta ve formě drag and drop rozhraní umožňujícího Low-Code development ze strany zadavatele.

Díky tomu bude IDP moci vizualizovat aktuální stav, nebo automaticky reagovat na příchozí události prostřednictvím přednastavených akcí. K řešení konkrétních událostí bude možné využít přesně definované pracovní postupy (workflow). Pracovní postupy budou definovat možné stavy pro každý typ události a proces, kterým lze takové události řešit. Historii přijatých událostí, uživatelských akcí a realizovaných procesů bude možné dále analyzovat a vyhodnotit prostřednictvím logů, vizualizačních a reportovacích nástrojů.

Jako minimum pro zajištění těchto funkcí jsou požadovány následující prvky event management prostředí:

- Událost
- Alarm
- Reakce
- Rule engine
- Workflow

Zadavatel plánuje využívat IDP jako řídicí středisko pro řešení různých situací podle požadavků uživatele. Musí proto umožnit automatizované spouštění akcí (např. automatické natočení kamery, otevření závory, řízení osvětlení, odeslání zpráv, automatická akce v systémech třetích stran a podobně).

Funkční požadavky:

- Umožní sběr událostí z integrovaných systémů prostřednictvím REST API
- Pro potřeby dalšího zpracování a ukládání přijatých událostí umožní definovat strukturu každé události jako objektu.

- Musí podporovat možnost ukládání a správy událostí ve vlastní interní databázi
- Musí podporovat možnost sběru, ukládání a zpracování systémových událostí
- Musí podporovat vytváření jednotlivých workflow pro automatizované procesy. Jedná se o tvorbu workflow skrze grafické (low-code) rozhraní, definici způsobu vyhodnocení jednotlivých událostí a nadefinování následných akcí.
- Umožní pozastavení vyhodnocování jednotlivých událostí na předem stanovenou dobu, po které se workflow opět automaticky zapne – využití pro potlačení alarmů např. po dobu dopravní nehody.
- Umožní definování spuštění workflow závislosti na pracovní době v jednotlivých dnech.
- Musí zajistit eskalaci jednotlivých událostí na základě nadefinovaných workflow na dispečerské pracoviště v podobě alarmu.
- Musí obsahovat integrovaný (low-code) nástroj pro řízení práce s alarmy (incident management).
- Musí zaznamenávat vlastní auditní logy a auditní záznamy všech aktivit.
- Musí umožňovat agregaci událostí do jednoho identifikovaného incidentu, pokud se události vážou k témuž incidentu.
- Musí umožnit objednateli vytvářet reporty minimálně ve formátech PDF, CSV.
- Musí umožňovat automatické spuštění definovaných reportů (měsíčně, týdně, denně, nebo v definovaném čase), jejich ukládání na síťové úložiště nebo zasílání e-mailem přímo ze systému.
- Musí umožňovat na jakoukoliv událost navázat automatickou akci/reakci, např.:
 - Spuštění automatizovaného procesu
 - Notifikaci přes mail s možností definovat pravidla pro zasílání na různé adresy podle kritičnosti, zdroje apod.
 - Spuštění externího skriptu
- Veškerá uživatelská konfigurace, definice událostí, zdrojů dat, definice pravidel, tvorba reportů. musí probíhat z grafického rozhraní IDP klienta, bez nutnosti zásahu do programového kódu.
- Všechny potřebné SW komponenty musí být součástí dodaného systému, včetně případné databáze a potřebných licencí.
- Všechny požadované funkce systému se musí spravovat s prostřednictvím jedné společné řídicí konzole, která je přístupná přes webové rozhraní nebo klienta pro OS MS Windows 10.
- Veškeré uživatelské nastavení a vlastní práce se systémem se musí provádět na jednom místě z jedné společné konzole nehledě na daný modul.

Video management a detekce

IDP musí poskytnout interní modulární video management systém (VMS), který bude využíván pro potřeby provozovatelů kamerových systémů, které se využívají především pro monitoring budov, parkovišť, nebo dopravy. Jeho úlohou bude centralizace těchto systémů, jejich jednotná správa a následné sdílení. Zároveň musí umožnit napojení kamerových streamů ze stávajícího VMS systému Městské policie (VMS zn. AVIGILON). Je proto požadováno jak interní VMS, tak možnost budoucí integrace VMS třetích stran.

V budoucnu je pravděpodobné využití i dalších detekčních platforem pro detekci SPZ v rámci plánovaného zábránového systému, prediktivní analýzy v rámci optimalizace využití systému BusStop, analýzy dopravních proudů pro potřeby plánovaného inteligentní řízení dopravy a podobně.

- V rámci video managementu a detekce musí IDP umožnit následující funkce:
 - Připojení kamerových streamů

- Nahrávání kamerových streamů
- Možnost připojení více video záznamových serverů
- Hardwarově akcelerované dekódování videa
- Export záznamu
- Nastavení délky záznamu na záznamovém serveru
- Nastavení délky záznamu na kamerách
- Podpora různých exportních formátů videa
- Podpora záložních záznamových serverů
- Vestavěná detekce pohybu v obraze
- Archivace na síťové úložiště
- Podpora kodeků: H.261, H.263, H.264, H.265, MPEG1, MPEG2, MPEG4, MJPEG, Theora, VP8, VP9, a dalších
- Musí umožnit připojení jednotlivých kamer do systému. Během implementace bude Objednatel pracovat s omezeným počtem kamer a tento počet bude průběžně navyšovat.
- Musí zajistit zpětné přehrání obrazového záznamu kamer.
- Musí umožnit integraci nástrojů pro off-line a on-line video analýzy. Podporu připojení a integraci video analytického SW třetích stran pro následující události:
 - Detekce pohybu a polohy osob
 - Detekce zón – narušení
 - Parkování – informace o obsazenosti
 - Počty příjezdů/odjezdů
 - Změny směru
 - Typy dopravních prostředků – identifikace typu vozidla pro statistické účely
 - Rozpoznávání a čtení registračních značek vozidel, akce/reakce na základě přečtené registrační značky vozidla
 - Doba stání
 - Průjezd opačným směrem
- Nastavení kamerových a situačních pohledů pro jednotlivé uživatele nebo role.
- Musí obsahovat funkci zobrazení nejbližších pohledů z kamer automaticky z místa kde byl vyhlášen alarm nebo jiná nadefinovaná událost, anebo ruční výběrem místa.

Interaktivní přehledová mapa

Interaktivní přehledová mapa má umožnit sledovat stav, polohu a real-time informace o velkém počtu technologických prvků. Za tímto účelem dynamicky vytvářet mapy a diagramy, které poskytují dobrý přehled o aktuální situaci. Systém bude podporovat práci ve více mapových vrstvách, umět pracovat s vektory, datovými body, online dlaždicemi nebo mapami. Musí umožnit práci nad mapovými vrstvami z GIS města Český Krumlov.

Systém bude umožňovat

- Jednotný mapový a vizuální systém
- Práce nad základní mapou města
- Možnost zakreslení umístění jednotlivých prvků (kamery, čidla, zařízení) a ostatních zdrojů systému
- Zobrazení informací o jednotlivých zdrojích – základní údaje

- Indikace stavu funkčnosti jednotlivých zařízení
- Zobrazení údajů/dat jednotlivých zdrojů (obrazové záznamy z kamer v reálném čase, hodnoty senzorů, provozní stavy technického vybavení atd.)
- Možnost zakreslení dosahu/viditelnosti jednotlivých kamer
- Identifikace jednotlivých eventů v reálném čase s notifikací pro dispečera
- Je požadována podpora mapových a GIS podkladů ve standardu ESRI ArcGIS

Ostatní požadavky na dodané software řešení

- Dodané aplikační prostředí je a bude min. 2 roky podporováno ze strany výrobců (např. verze PHP, Python, Java, Postgres a další použité technologie dle konkrétního řešení).
- Pravidelné bezpečnostní aktualizace aplikačního prostředí nebo kódu nejméně každé 3 měsíce.
- IDP server nebude používat nepodporované a zastaralé produkty a protokoly.
- Pro instalaci IDP klienta je požadována podpora operačního systému Windows 10
- Pro instalaci IDP serveru je požadována podpora OS Windows server (předposlední a aktuální verze v době dodání SW řešení) a podpora OS Linux Ubuntu 20.04 LTS Server (x86_64) a novější
- Je požadována možnost instalace ve virtuálním prostředí s online migrací v prostředí VMware vSphere

Požadavky na implementaci

Zprovoznění IDP

Zprovozněním aplikace se rozumí:

- Dodání instalačních souborů a instalační dokumentace
- Instalace a konfigurace IDP serveru a IDP klientů na připravenou infrastrukturu
- Konfigurace aplikace dle požadovaného stavu
- Integrace SW třetích stran dle požadovaného stavu
- Školení uživatelů
- Provedení bezpečnostních testů aplikace
- Provedení komplexních testů dle testovacích scénářů
- Provedení zátěžového testu

Dodavatel po úspěšném zprovoznění SW řešení dodá objednateli jako součást předmětu plnění podrobnou dokumentaci dodávaného systému, včetně kompletního popisu, nastavení a konfigurace daného řešení tak, aby jej bylo možné nadále provozovat a udržovat.

Objednatel požaduje dodání dokumentace v českém jazyce a v následující logické struktuře:

- provozní dokumentace
- administrátorská příručka
- instalační manuál
- uživatelská dokumentace (uživatelský manuál)
- Dokumentace API

Dokumentace musí kromě obecné práce se systémem obsahovat i specifické informace o konkrétní implementaci a konfiguraci řešení nasazené u objednatele. Dodavatel bude v rámci podpory provozu IDP

aktualizovat dokumentaci formou zasílání změnových zpráv tak, aby objednatel měl průběžně k dispozici aktuální dokumentaci k aplikaci, jež v danou dobu užívá.

Testovací a ověřovací provoz IDP

Testovací a ověřovací provoz bude zahájen objednatelem na základě celkového zprovoznění systému. Délka testovacího provozu objednatelem je stanovena na minimálně 30 kalendářních dnů. Testovací provoz slouží k ověření bezchybného chodu systému v reálném provozu. Testovací provoz obsahuje provedení komplexních testů dle testovacích scénářů objednatele. Objednatel a dodavatel o průběhu testování vyhotoví testovací protokol.

Testované funkcionality:

- Vytvoření uživatele – ověření přes active directory, lokální ověření
- Nastavení uživatelské role
- Načítání objektů z GIS města ve vrstvách
- Připojení kamerového vstupu
- Připojení nekamerového vstupu
- Připojení čidla
- Zobrazení zdrojů v GIS vrstvě
- Vytvoření nového workflow, pozastavení workflow na stanovenou dobu
- Přehrání obrazového záznamu kamer MKDS
- Eskalace událostí na základě workflow
- Test spuštění automatických reakcí
 - Spuštění automatizovaného procesu
 - Notifikaci přes mail s možností definovat pravidla pro zasílání na různé adresy podle kritičnosti, zdroje apod.
 - Spuštění externího skriptu
- Indikace stavu funkčnosti jednotlivých zařízení v aplikaci
- Zobrazení údajů/dat jednotlivých zdrojů (obrazové záznamy z kamer v reálném čase, hodnoty senzorů.)
- Kontrola záznamů auditních logů a auditních záznamů
- Vytvoření 4 reportů
- Test automatického spouštění reportů

Testování se bude provádět na 3 kamerových vstupech po dobu testovacího provozu. Cílem je ověření bezproblémového běhu aplikace.

Ode dne ukončení testování objednatelem je dodavatel povinen nejpozději do 20 kalendářních dnů odstranit veškeré závady zjištěné v průběhu testování a uvedené v testovacím protokolu.

Školení uživatelů

- Dodavatel provede školení uživatelů a administrátorů.
- Úvodní školení administrátorů pro max. 3 osoby v prostorách Objednatele v délce 8 hodin.
- Úvodní školení operátorů pro maximálně 5 osob v prostorách Objednatele v délce 8 hodin.

Migrace monitoringu užšího centra města

Monitoring užšího centra města bude i nadále zajištěn prostřednictvím stávající detekční platformy CertiConVis, která zůstane v původním umístění beze změn. Detekční systém bude s IDP serverem propojen prostřednictvím API rozhraní, díky čemuž budou do IDP serveru ukládány detekované události a data.

VMS služba IDP bude centrálním bodem, do kterého budou postupně napojeny i ostatní kamerové systémy města a městských organizací. Zajistí centralizaci záznamů a detekovaných dat na jednom místě a řízení přístupu kompetentních organizací k těmto datům. Výjimkou budou kamerové streamy městského kamerového dohledového systému městské policie (dále jen MKDS). Městská policie provozuje vlastní VMS systém, který zůstane zcela nezávislý. V případě, že bude monitorovací systém chtít využívat streamy MKDS, budou do VMS služby IDP předávány z VMS Městské policie.

Migrace kamerových streamů

Dodavatel zajistí napojení kamerových streamů využívaných k monitoringu centra do IDP serveru následujícím způsobem:

- V případě streamů přebíraných z kamer MKDS zajistí předání prostřednictvím propojení VMS Městské policie s VMS službou IDP serveru a následné předání streamů z IDP serveru do analytického serveru systému CertiConVis.
- V ostatních případech zajistí přímé napojení kamerových streamů do VMS služby IDP serveru a následné předání streamů IDP serveru do analytického serveru systému CertiConVis

Konkrétně se bude jednat o video streamy z následujících kamerových bodů:

- Horní ulice - kamera umístěná na budově městského divadla.
- Linecká ulice - kamera umístěná na ZŠ Linecká.
- Ulice Latrán - kamera umístěná na objektu ve vlastnictví ČKRF (součást MKDS).
- pod Plášťovým mostem – detekční kamera, která je součástí (součást MKDS).

Migrace dat a jejich vizualizace

Po migraci kamerových streamů dojde k propojení IDP serveru s analytickým serverem prostřednictvím API. IDP server bude nakonfigurován tak aby přebíral a ukládal výsledky detekce jako události do vlastní databáze. Následně bude v rámci IDP serveru vytvořen dashboard pro monitoring centra, v rámci kterého budou výsledky detekce vizualizovány.

Zadavatel požaduje, aby byla v rámci dashoardu řešena i historická data.

Požadavky na implementaci

Město Český Krumlov zajistí všechny potřebné konfigurace v rámci přenosových tras a datových sítí tak, aby byly uvedené datové streamy dostupné v nové lokalitě centrálního datového sálu v budově autobusového nádraží.

Dodavatel následně zajistí následující implementační činnosti:

- Napojení a konfiguraci kamerových streamů do IDP serveru

- Napojení a konfigurace video streamů z IDP serveru do detekční platformy CertiConVis
- Sběr událostí z CertiConVis do IDP prostřednictvím API
- Konfigurace dashboardu IDP pro monitoring centra v rozsahu stávající vizualizace.
- Dodání instalačních souborů a instalační dokumentace
- Školení operátorů pro maximálně 5 osob v prostorách Objednatele v délce 8 hodin.
- Provedení bezpečnostních testů aplikace
- Provedení komplexních testů dle testovacích scénářů. Objednatel a dodavatel o průběhu testování vyhotoví testovací protokol.
- Provedení zátěžového testu

Testování se bude provádět na všech kamerových vstupech po dobu testovacího provozu. Cílem je ověření bezproblémového běhu aplikace.

Ode dne ukončení testování objednatel je dodavatel povinen nejpozději do 20 kalendářních dnů odstranit veškeré závady zjištěné v průběhu testování a uvedené v testovacím protokolu.