VILNIAUS RAJONO SAVIVALDYBĖS ADMINISTRACIJA
VAIZDO STEBĖJIMO SISTEMOS PLĖTROS, ĮRENGIMO, PRIEŽIŪROS, DUOMENŲ PERDAVIMO IR APDOROJIMO GALIMYBIŲ STUDIJA
Vilnius, 2026 m.

---

1. ĮVADAS IR PASLAUGOS PASIŪLYMO AIŠKINAMASIS RAŠTAS

1.1. Studijos tikslas ir uždaviniai

Šios galimybių studijos tikslas – nuodugniai įvertinti Vilniaus rajono savivaldybės administracijos (toliau – Užsakovas arba **VRSA**) esamą vaizdo stebėjimo infrastruktūrą bei poreikius ir suprojektuoti centralizuotą, saugią bei keičiamo mastelio (angl. *scalable*) IP vaizdo stebėjimo sistemą. Studijoje numatomas perėjimas nuo šiuo metu veikiančio fragmentuoto ir decentralizuoto modelio prie centralizuoto valdymo modelio, apimant modernizavimo ir plėtros etapus 2026–2029 m., procesų svarbą pritaikant dirbtinį intelektą ir resursų automatizavimui, sąnaudų mažinimui, efektyviam užduočių atlikimui, duomenų analizavimui.

Pagrindiniai studijos uždaviniai:

- Nustatyti techninius ir funkcinius reikalavimus kameroms, programinei įrangai bei uždarojo duomenų perdavimo tinklo architektūrai.
- Suprojektuoti fizinės infrastruktūros (serverių, saugyklų (duomenų archyvo), kompiuterinių darbo vietų) poreikį *„on-premise“* modelio pagrindu.
- Apibrėžti uždaro duomenų perdavimo tinklo architektūrą, ryšio įrangą ir sistemos integracijų apimtį
- Išspręsti lauko kamerų, montuojamų ne ant pastatų, el. maitinimo inžinerinius iššūkius, pritaikant tvarias alternatyvas.
- Užtikrinti atitiktį BDAR (GDPR) reglamentui ir NIS2 kibernetinio saugumo direktyvoms. Įvertinti prieigos kontrolės, duomenų apsaugos ir kibernetinio saugumo priemones bei dokumentų poreikį pagal taikytinus reikalavimus.
- Įvertinti esamą VRSA infrastruktūrą, stebėjimo vietas ir plėtros poreikį, remiantis pateiktais dokumentais bei faktiniais infrastruktūros duomenimis.
- Apibrėžti projektavimo, įrengimo, konfigūravimo, bandymų, dokumentavimo ir priežiūros reikalavimus.
- Parengti 23 seniūnijų atnaujinimo ir plėtros planą, apimantį esamas 110 kamerų ir naujai planuojamas 220 kamerų (iš viso 330 kamerų), bei pateikti rinkos analize pagrįstą preliminarų biudžetą etapais (žingsniais).

1.2. Metodologija ir pradinės sąlygos

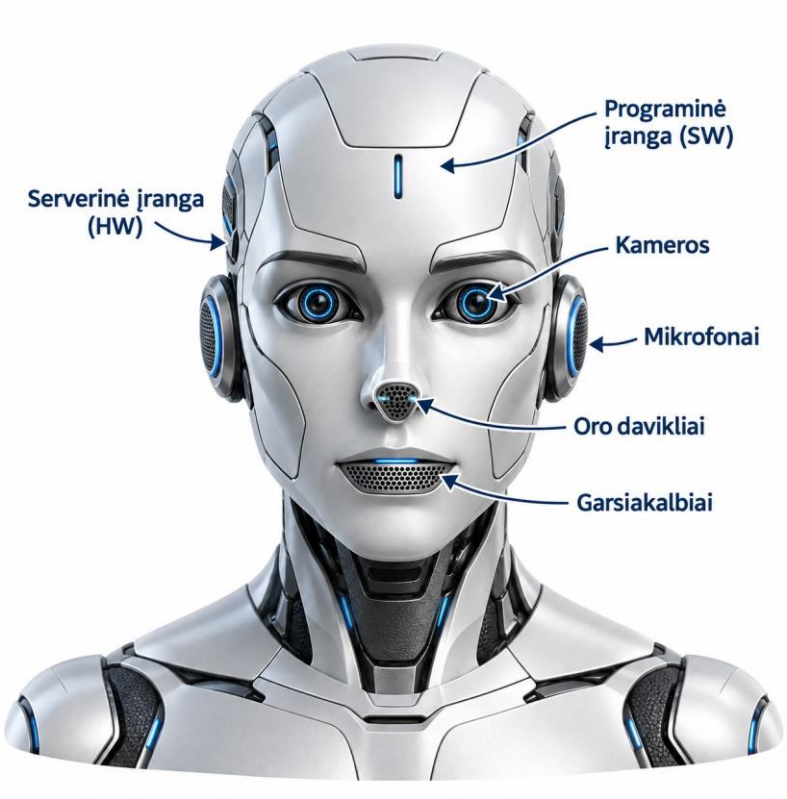
Studija parengta vadovaujantis CVP IS priemonėmis vykusiais pirkimais 2025 ir 2026 metais, IT gerosiomis praktikomis, technologinėmis tendencijomis, dirbtinio intelekto taikymu, Lietuvos Nacionalinio kibernetinio saugumo centro rekomendacijomis, įvertinant kylančias grėsmes ir iššūkius dėl dirbtinio intelekto (DI), taip pat kibernetines grėsmes iš nedraugiškų šalių, bei šių dienų poreikiais:

1. Architektūra: 100% *on-premise*. Visi serveriai, saugyklos (diskų telkiniai) ir valdymo mazgai įrengiami specialiai skirtoje serverinėje arba serverinei keliamus reikalavimus atitinkančiose techninėse patalpose.
2. Duomenų saugojimas: Vaizdo įrašų saugojimo trukmė – 30 dienų, užtikrinant nepertraukiamą 24/7 įrašymą visoms sistemai priklausančioms kameroms.
3. Valdymas ir stebėjimas: Planuojamos dvi (2) nutolusios operatorių darbo vietos su vaizdo siena bei **trys (3)** viešosios tvarkos darbuotojų kompiuterinės darbo vietos savivaldybėje.
4. Duomenų perdavimas. Uždara tinklo struktūra, naudojant vidinę (LAN) IP adresaciją, siekiant maksimalaus saugumo ir privatumo užtikrinimo, išvengiant jautrių duomenų praradimo ar sugadinimo, bei užtikrinant aukštą duomenų perdavimo pasiekiamumą.
5. ANPR funkcionalumas: Automatinis transporto priemonių valstybinių numerių atpažinimas diegiamas policijos ir savivaldybės tiksliai atrinktose vietose (26 lokacijose).
6. Dirbtinio intelekto (DI) (angl. Artificial intelligence (AI)) funkcionalumas, kur sistemos dalių funkcijas vaizdžiai paaiškina 1 paveiksle pateikta robotizuoto žmogaus ir techninių komponentų analogija. Tai aiškinamoji iliustracija, o faktinė sistemos architektūra

nustatoma pagal studijos projektinius sprendinius ir Užsakovo poreikius.

1 pav.

Vaizdo stebėjimo sistemos dalių funkcinė analogija



Pastaba: Robotizuoto žmogaus atvaizdas naudojamas tik sistemos dalių funkcinei analogijai. Iliustracijoje parodyti mikrofonai, oro davikliai ir garsiakalbiai nėra papildomi privalomi komponentai; jų poreikis nustatomas pagal Užsakovo poreikius.

2. ESAMOS BŪKLĖS ĮVERTINIMAS IR CENTRALIZACIJOS KONCEPCIJA

Šiuo metu VRSA teritorijoje (23 seniūnijose) veikia apie 110 vaizdo stebėjimo kamerų. Atlikus apžiūrą ir techninį auditą, nustatyta itin didelė technologinė fragmentacija, kelianti riziką duomenų saugumui ir operatyviam valdymui:

- Stand-alone buitinės kameros: Esamų kamerų dalis seniūnijose yra autonominiai (*stand-alone*) plataus vartojimo prekių ženklų įrenginiai (pvz., Imou, Reolink). Šios kameros vaizdą įrašo tik lokaliai (į vidines MicroSD korteles), veikia per viešuosius mobilius arba atvirus belaidžius tinklus, neturi centralizuoto valdymo ir neatitinka institucinių saugumo standartų.
- Seniūnijų pastatų kameros: Ant seniūnijų administracinių pastatų yra sumontuotos profesionalesnės įvairių (pvz., Dahua, Hikvision) kiniečių gamintojų kameros. Jos vaizdo srautus siunčia į lokalius vaizdo įrašymo įrenginius (NVR) – po vieną (1) įrašymo įrenginį kiekvienoje iš 23 seniūnijų. Vaizdas prieinamas tik fiziškai nuvykus į vietą arba per nesaugias išorines P2P programėles.

Decentralizuotas variantas	**Privalumai**	**Apribojimai ir vertinimas**
Decentralizuotų NVR išlaikymas	Vietinis įrašymas mažina WAN priklausomybę.	Sudėtingesnis bendras valdymas, auditas ir paieška. Kaip pagrindinis projekto modelis neatitinka centralizacijos reikalavimo.

Perėjimo prie centralizuoto modelio koncepcija:
Visi esami sprendimai palaipsniui eliminuojami arba perkeliami į vieningą tinklo struktūrą. Seniūnijų pastatų kameros (pvz. Dahua, Hikvision) integruojamos į bendrą tinklą per RTSP/ONVIF protokolus, o pasenę lokalių NVR įrašymo įrenginiai ir buitinės kameros (Imou/Reolink) pakeičiamos naujomis, jungiant į centralizuotą Vaizdo valdymo programinę įrangą (VMS). Pagrindinis vaizdo srautas per uždarą duomenų perdavimo tinklą nukreipiamas į centrinę serverinę, kur užtikrinamas 30 dienų archyvas, vieningas teisių valdymas ir funkcionalumas.

Centralizuotas variantas	**Privalumai**	**Apribojimai ir vertinimas**
Centralizuota MAS ir SAS architektūra	Vieninga sąsaja, paieška, teisių valdymas, priežiūra ir archyvas.	Būtini pakankami ryšio kanalai, centrinio mazgo apsauga (prisijungimas prie VMS sistemos per 2FA) ir greitesnės gedimų atkūrimo procedūros.

Centralizuotas variantas	Privalumai	Apribojimai ir vertinimas
Centralizuotas valdymas su vietiniu buferiavimu	Išsaugo centralizacijos naudą ir padeda kompensuoti laikinas ryšio pertraukas.	Automatinis vietinių įrašų tęstinumas/atkūrimas turi būti suderinamas su pasirinkta VMS sistema ir patikrintas sistemos bandymais arba gerąja IT praktika.

2.1. Esamos būklės įvertinimas ir identifikuotos problemos (Decentralizuotas modelis)

Šiuo metu Vilniaus rajono savivaldybės teritorijoje veikianti vaizdo stebėjimo infrastruktūra (apie 110 esamų kamerų) yra vystoma decentralizuotu principu. Kameros buvo įsigyjamos ir įrengiamos atskirais etapais, skirtingų seniūnijų užsakymais, naudojant lokalius, tarpusavyje nesusietus įrašymo įrenginius (NVR) arba autonomines kameras su vietinėmis atminties kortelėmis.

Atlikus esamos būklės auditą, identifikuoti šie kritiniai trūkumai, kurie daro dabartinį modelį netinkamu tolesnei plėtrai iki 330 kamerų apimties:

1. Technologinis fragmentavimas ir nesuderinamumas: Savivaldybėje naudojama skirtingų gamintojų įranga (nuo profesionalių sistemų iki žemos klasės buitinių kinietiškų kamerų). Tai neleidžia sukurti vientisos stebėjimo aplinkos. Operatoriai privalo naudoti kelias skirtingas programines sąsajas, o tai drastiškai sulėtina reakcijos laiką incidentų metu.
2. Duomenų praradimo rizika ir rezervavimo trūkumas: Lokalieji įrašymo įrenginiai (NVR) seniūnijose naudoja bazinius diskų masyvus be pariteto apsaugos. Sugedus fiziniam diskui arba įvykus elektros sutrikimui seniūnijos pastate, vaizdo archyvas dažnu atveju visiškai prarandamas. RAID apsaugo tik duomenis vieno serverio viduje (nuo kietojo disko gedimo). Rezerviniai sprendimai esamoje architektūroje neegzistuoja, tiek nėra naudojamas RAID (angl. Redundant Array of Independent Disks) nuo kietojo disko gedimo, tiek nėra sistemos persijungimo, dingus vaizdo perdavimui.
3. Kibernetinio saugumo spragos (NIS2 neatitiktis): a) decentralizuoti įrenginiai seniūnijose neturi centralizuoto ugniasienių valdymo; b) autorizuota gamyklinė aparatinė programinė įranga (*firmware*) nėra sistemingai atnaujinama; c) duomenų perdavimui nenaudojami saugūs šifravimo protokolai (RTSPS/HTTPS/TLS); d) lokalieji įrenginiai neturi centralizuoto naudotojų teisių valdymo ir nekeičiamo audito žurnalo (*Tamper-proof Audit Trail*), kas tiesiogiai pažeidžia ES NIS2 direktyvos reikalavimus, taikomus ypatingos svarbos regioninei infrastruktūrai.
4. DI analitikos ir paieškos nebuvimas: esami įrenginiai turi ribotas analitikos pritaikymo galimybes. Dėl centralizuotos duomenų bazės nebuvimo, neįmanoma atlikti globalios objektų ar transporto priemonių valstybinių numerių (ANPR) paieškos visoje savivaldybėje. Jei lokaliai fiksuojamas valstybinis numeris, norint atsekti transporto

priemonės judėjimą, operatoriai turėtų rankiniu būdu jungtis prie kiekvienos seniūnijos NVR atskirai ir vizualiai peržiūrėti valandų trukmės įrašus.

5. Pralaidumo asimetrija ir rinkoje esančių planų (ryšio paslaugų) apribojimai: Remiantis savivaldybės nutolusių padalinių esamų administracinių ryšio kanalų analize ir Lietuvos rinkoje taikomais standartiniais asimetrinio LTE 4G ryšio paslaugų prieigų planais, nutolusių taškų išeinančio srauto pralaidumas (angl. *upload speed*) standartiškai yra kintamas ir techniškai apribotas iki ~5–10 Mbps diapazono. Kadangi esamas ~110 kamerų modelis buvo orientuotas į lokalų vaizdo įrašymą seniūnijų įrenginiuose (NVR), istoriškai nebuvo inžinerinio poreikio užsakyti didesnio pralaidumo LTE 5G arba šviesolaidinio ryšio paslaugų planų. Centralizuotam naujų 5MP, 8MP arba 32MP kamerų srautų perdavimui realiame laike šis esamas pralaidumas yra kritiškai svarbus, o tai įrodo būtinybę kurti naują, dedikuotą duomenų perdavimo infrastruktūrą, skirtą tik vaizdo duomenų perdavimui, naudojant vidinius tinklo IP adresus (LAN IP).
6. Loginių segmentų (VLAN) nebuvimas: Esamoje fragmentuotoje struktūroje vietinės vaizdo kameros seniūnijose dažnu atveju veikia tame pačiame loginiame tinklo segmente, kuriame dirba administracijos darbuotojų kompiuteriai ir serveriai. Tai gali sukelti nuolatinę tinklo perkrovų riziką ir drastiškai sumažina bendrą savivaldybės IT infrastruktūros saugumą.
7. Nepatikimi VPN šifravimo sprendimai: Duomenų perdavimui tarp kai kurių nutolusių administracinių taškų naudojami viešaisiais tinklais paremti sprendimai (IPsec VPN ir pan.) arba pasenę techninės įrangos virtualūs privatūs tinklai (VPN) be dedikuoto (licencijuoto) saugaus belaidžio duomenų perdavimo. Didėjant kamerų skaičiui iki 330 vienetų, bandymas naudoti esamus seniūnijų galinius įrenginius (pvz. maršrutizatorius) sukeltų jų centrinių procesorių (CPU) perkrovas dėl masinio duomenų šifravimo krūvio ir duomenų srauto.

2.2. Centralizuoto modelio koncepcijos pagrindimas

Siekdama eliminuoti esamos būklės trūkumus, Galimybių studija numato pereiti prie Korporatyvinio lygio centralizuotos VMS architektūros (Master/Satellite modelio), kurioje visi 330 kamerų srautai, metaduomenys ir valdymo teisės yra konsoliduojami viename virtualiame arba fiziniame savivaldybės serverių mazge.

CENTRALIZUOTO MODELIO PRIVALUMAI
1. Unifikuotas valdymas ► Viena sąsaja visoms 330 kamerų ir AI
2. Didelis patikimumas ► ne mažesnė nei RAID 5 arba 6 diskų telkiniui (masyvui) saugykla, plius „N+1 serveris“rezervas vaizdo archyvo plėtimui ir vaizdo srauto įrašymui

3. NIS2 Atitiktis ► Nekeičiamas SQL audito žurnalas, nežemiau kaip TLS 1.2 šifravimo versija
4. Operatyvi paieška ► Bendra visas kameras apimanti analitika/ANPR paieška per labai trumpą laiką. T.y. gebanti atlikti pilną ir/arba dalinę ANPR paiešką pagal pasirenkamus laukus aktualiose ir/arba archyvinėse duomenų bazėse, nurodant: (a) pilną transporto priemonės numerį; (b) ne pilną transporto priemonės numerį; (c) valstybę, kurioje registruota transporto priemonė; (d) transporto priemonės spalvą; (e) transporto priemonės tipą; (f) vaizdo kameros identifikacinį požymį; (g) vaizdo kameros vietą; (h) vaizdo kameros kryptį; (i) datos ir laiko pasirenkamus intervalus; (j) atpažintus numerius (l) neatpažintus numerius.

2.2.1. Inžinerinis ir operacinis centralizacijos naudos pagrindimas

- Vieninga valdymo ir stebėjimo sąsaja (Unified Management): Centralizuotas VMS modelis sujungia visų 23 seniūnijų kamerų srautus į vieną sistemos aplinką. Operatoriai realiu laiku mato visą VRSA rajono situaciją interaktyviuose žemėlapiuose (GIS), o aliarmo signalai (pvz., perimetro kirtimas, ieškomo automobilio numerio fiksavimas) akimirksniu iššoka viename ekrane, nepriklausomai nuo to, kurioje seniūnijoje kamera yra fiziškai sumontuota.
- Centralizuotas resursų efektyvumas ir ne mažesnis nei RAID 5 našumas: Vietoj 23 atskirų silpnų įrenginių seniūnijose, sukuriamas vienas galingas, įrašymo serverių segmentas centriniame mazge. Srautų rašymas į centralizuotą paskirstytą diskų masyvą su tolygiai išmėtytais pariteto duomenimis, užtikrinantį subalansuotą atsitiktinio skaitymo ir rašymo spartą, kuri būtų būtina vienu metu maksimaliai priimant 2.4625 Gbps srautą iš 330vnt. IP kamerų.
- „N+1“ lygio sisteminis atsparumas: Centralizuotame modelyje įdiegtas fizinis rezervinis įrašymo serveris nuolat stebi aktyvių įrašymo serverių būseną. Jei vienas iš pagrindinių įrašymo serverių patiria aparatinį gedimą, rezervinis serveris perima nurodytą kamerų srautų įrašymą. Toks patikimumo lygis decentralizuotame modelyje reikalautų pirkti po rezervinį įrenginį kiekvienai seniūnijai, kas būtų ekonomiškai neatsakinga.
- Metaduomenų paieška: Centralizuota „Microsoft SQL Server“ duomenų bazė, veikianti pagal *„Per Core“* modelį, realiu laiku priima ir indeksuoja visų kamerų siunčiamus DI metaduomenis (pvz. objektus, objektų atributus ar ANPR duomenis). Tai leidžia operatoriams arba policijos pareigūnams atlikti kelių sekundžių arba minučių trukmės paiešką visoje VRSA savivaldybės teritorijoje pagal specifinius filtrus (pvz., „raudonos spalvos automobilis“ arba „asmuo su juoda apranga“), kas decentralizuotoje sistemoje techniškai neįmanoma.
- Kibernetinio saugumo ir privatumo kontrolė: Centralizuotas modelis leidžia IT administratoriams viename taške suvaldyti naudotojų teises integruojant sistemą su

Active Directory (LDAP), aktyvuoti daugiaveiksmį autentifikavimą (MFA) arba dviejų faktorių autentifikavimą (2FA) bei užtikrinti, kad privatumo zonų maskavimas būtų pritaikytas tiesiogiai srautams, apsaugant gyventojų teises. Nekeičiamas SQL audito žurnalas fiksuoja kiekvieną operatoriaus paspaudimą ir vaizdo eksportą, pilnai tenkindamas NIS2 teisinį reglamentavimą bei įvykių atsekamumą.

2.3. Decentralizuoto modelio išlaikymo rizikų analizė

Siekdami objektyviai įvertinti technologinės plėtros alternatyvas, žemiau pateikiame struktūrizuotą rizikų analizę, kuri identifikuoja grėsmes savivaldybės vaizdo stebėjimo sistemos tęstinumui, duomenų saugumui ir teisinei atitikčiai, jei 330 kamerų plėtra būtų vykdoma paliekant esamą decentralizuotą modelį.

Rizikos vertinamos pagal standartinę vertinimo skalę, kur Tikimybė ir Poveikis skirstomi skalėje nuo 1 (žema) iki 5 (aukščiausia), o galutinis Rizikos lygis nustatomas juos sudauginus (Rizika = Tikimybė × Poveikis):

- 1–6: Žema rizika (priimtina, stebima).
- 8–12: Vidutinė rizika (reikalauja valdymo priemonių).
- 15–25: Aukšta / Kritinė rizika (nepriimtina, būtini neatidėliotini architektūriniai pakeitimai).

Lentelė Nr. 1: Rizikų vertinimas išlaikant decentralizuotą sistemos modelį

Rizikos ID	Rizikos sritis ir aprašymas	Tikimybė (1-5)	Poveikis (1-5)	Galutinis lygis (1-25)	Teisinis, finansinis ir inžinerinis rizikos pasekmių vertinimas
RSK-TEIS-01	Teisinė neatitiktis NIS2 direktyvai ir LR Kibernetinio saugumo įstatymui. *Decentralizuota sistema neužtikrina centralizuoto audito žurnalo ir srautų šifravimo.*	5	5	25 (Kritinė)	Nuo 2024 m. pabaigos įsigaliojusi NIS2 direktyva numato asmeninę vadovų atsakomybę ir finansines baudas iki 7 mln. EUR arba 1,4% globalios apyvartos už ypatingos svarbos infrastruktūros saugumo neužtikrinimą. Šifruotų RTSPS srautų ir nekeičiamo (*Tamper-*

					proof) SQL audito žurnalo nebuvimas decentralizuotame modelyje gali būti teisinių sankcijų taikymo audito metu pasekmė.
RSK-KIB-02	Sisteminiai kibernetiniai incidentai ir duomenų nutekinimas. *Seniūnijose esantys NVR įrenginiai neturi centralizuoto ugniasienių valdymo, saugaus programinio kodo atnaujinimo, patikimos ir skaitmeniniu parašu pasirašytos gamintojo programinės įrangos.*	4	4	16 (Aukšta)	Decentralizuoti lauko mazgai ir įrašymo įrenginiai tampa lengvu taikiniu automatizuotoms kenkėjiškų programų (angl. *botnets / malware*) atakoms. Užgrobus vieną iš įrenginių, užpuolikai gali gauti prieigą prie kitų savivaldybės tinkle esančių įrenginių, suklastoti arba nutekinti vaizdo įrašus, sukeldami masinį BDAR pažeidimą ir reputacinę krizę.
RSK-FIN-03	Neproporcingas operacinių kaštų (OPEX) augimas. *23 atskirų serverinių/NVR mazgų fizinė priežiūra, diskų keitimas ir licencijų administravimas.*	4	3	12 (Vidutinė)	Ekonominis neefektyvumas. Sugedus įrangai, techninis personalas privalo fiziškai vykti į atitinkamą seniūniją. Augant kamerų skaičiui iki 330, decentralizuotos sistemos SLA palaikymo ir

					eksploatacijos kaštai per 4 metus viršytų centralizuoto serverio įrengimo kaštus dėl nuolatinių transporto, amortizacijos ir licencijų atnaujinimo išlaidų.
RSK-INŽ-04	Duomenų praradimas dėl aparatinės dalies gedimų. *Lokalių diskų masyvų pažeidimai seniūnijose nesant diskų arba serverio rezervavimo.*	4	4	16 (Aukšta)	Funkcinis praradimas. Kadangi seniūnijų NVR nenaudoja pažangios RAID architektūros vieno fizinio disko gedimas vietiniame įrenginyje dažnu atveju reiškia viso to taško 30 dienų archyvo praradimą. Rezervinio „N+1“ serverio nebuvimas reiškia, kad sugedus seniūnijos NVR, stebėjimas tame regione visiškai sustoja iki fizinio įrangos pakeitimo.
RSK-OPER-05	Kritinis operacinio darbo efektyvumo nuosmukis. *Policijos ir savivaldybės operatorių nesugebėjimas operatyviai vykdyti bendros paieškos incidentų metu.*	5	3	15 (Aukšta)	Jei vaizdo analitikos metaduomenys ar transporto numerių (ANPR) duomenys nesaugomi vieningoje SQL duomenų bazėje, nusikaltimo tyrimo metu operatorius privalo rankiniu būdu atlikti 23 atskiras užklausas į skirtingus įrenginius. Paieška,

					kuri centralizuotame modelyje trunka trumpai, čia užsitęsia iki kelių valandų ar net parų, prarandant operatyvinį pranašumą karštais pėdsakais arba įvykių atsekamumą.

2.4 Išvados dėl rizikų valdymo

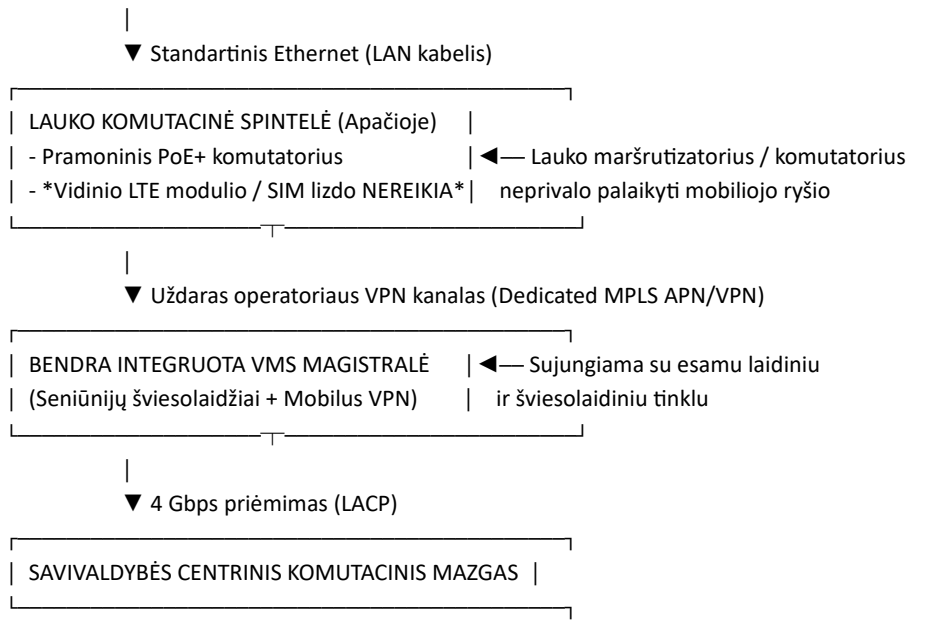
Identifikuotų rizikų analizė aiškiai įrodo, kad decentralizuoto modelio išlaikymas arba bandymas jį plėsti iki 330 kamerų generuoja nepriimtiną rizikos lygį (balai nuo 16 iki 25). Vienintelė efektyvi, tarptautiniais IT standartais pripažinta rizikos mažinimo priemonė – visiškas esamos architektūros transformavimas į centralizuotą Master/Satellite modelį, kuris:

- Sumažina teisinę ir kibernetinę riziką (RSK-TEIS-01, RSK-KIB-02) iki žemo, priimtino lygio, naudojant nežemesnį TLS 1.2 šifravimą ir nekeičiamą SQL audito žurnalą.
- Eliminuoja duomenų praradimo grėsmę (RSK-INŽ-04) per centralizuotą RAID diskų masyvą ir rezervinį „N+1“ perjungimą.
- Užtikrina investicijų grąžą ir operatyvumą bei efektyvumą (RSK-FIN-03, RSK-OPER-05) per bendrą metaduomenų paiešką vieningoje VMS sistemoje.

Perėjimas nuo esamo decentralizuoto modelio prie centralizuotos *Master/Satellite* VMS architektūros yra vienintelis techniškai ir ekonomiškai pagrįstas sprendimas. Jis ne tik išsprendžia esamos fragmentuotos įrangos nesuderinamumo problemas, bet ir sukuria saugią, lengvai plečiamą, duomenų analitika grįstą platformą, paruoštą integravimui su Lietuvos policija bei kitomis operatyvinėmis tarnybomis ir institucijomis.

2.4.1 Centralizuoto tinklo pralaidumo modeliavimas ir hibridinė integracija (Laidinis (šviesolaidinis) + uždaras tinklas MPLS APN/VPN ir nežemiau kaip 5G Mobilusis ryšys)
Perėjimas prie centralizuoto modelio reikalauja suprojektuoti visiškai izoliuotą, patikimo pralaidumo duomenų perdavimo tinklą. Remiantis atliktais inžineriniais skaičiavimais, bendras grynasis vaizdo srautas iš 330 pramoninių kamerų sudaro 2 757,5 Mbps (apie 2,76 Gbps), o

įvertinus TCP/IP protokolų virš sąnaudas bei 20% saugumo rezervą momentiniams šuoliams, centrinis mazgas privalėtų priimti 3 639,9 Mbps (apvalinama iki 4 Gbps) nuolatinį įeinantį srautą. Siekiant užtikrinti 100% duomenų saugumą, patikimumą ir NIS2 atitiktį taškuose, kur nutiesti fizinį šviesolaidį yra ekonomiškai ar techniškai neįmanoma, pirkimo techninėje specifikacijoje įtvirtinama uždaro tinklo hibridinė prieigų strategija - laidinė/šviesolaidinė prieiga ir mobiliojo ryšio nežemiau kaip 5G su išoriniais maršrutizatoriais ir/arba antenomis:



1. Išorinių 5G lauko įrenginių naudojimas: Nutolusiuose taškuose mobiliojo ryšio tiekėjai signalo priėmimui privalo naudoti aukštos klasės išorinius pramoninius lauko įrenginius, integruotus viename korpuse su kryptinėmis antenomis (angl. *CPE - Customer Premises Equipment*). Šie įrenginiai montuojami aukštai ant atramų ar pastatų fasadų, užtikrinant maksimalų mobiliojo ryšio signalo stiprumą, kryptinį jautrumą ir stabilumą net ir rajono vietovėse su silpna geografine aprėptimi.
2. Lauko įrangos supaprastinimas spintelėse: Kadangi išorinis lauko įrenginys (*CPE*) pats atlieka mobiliojo ryšio (LTE / 5G) signalo priėmimą, moduliavimą ir dekodavimą išorėje, vaizdo duomenys į lauko komutacinę spintelę yra nuleidžiami standartiniu laidiniu lauko UTP 5 cat. Ethernet (RJ45) arba optiniu kabeliu. Dėl šios priežasties lauko maršrutizatoriai ir komutatoriai, esantys pačioje spintelėje, neprivalo palaikyti LTE / mobiliojo ryšio funkcijų ir turėti vidinių SIM kortelių lizdų. Tai leidžia naudoti

standartizuotus pramoninius L2/L3 komutatorius, supaprastina jų administravimą ir visiškai pašalina riziką dėl SIM kortelių pažeidimo ar fizinės vagystės iš spintelės.

3. Uždaro privataus tinklo integracija: Ryšio tiekėjas per šiuos išorinius įrenginius privalo sukurti visiškai izoliuotą, projektui skirtą uždarą MPLS technologijos (pagrįstą žiedine topologija) APN/VPN tinklą, naudojant dedikuotą prieigos tašką kamerai (-oms) (dedicated MPLS APN/VPN 5G). Šis mobilusis segmentas magistraliniame lygmenyje (L3 lygmens *routingas / MPLS*) yra tiesiogiai integruojamas ir sujungiamas su bendru laidiniu bei šviesolaidiniu seniūnijų bei VRSA centriniu tinklu, suformuojant vieningą, šifruotą ir saugią vaizdo stebėjimo tinklo erdvę.
4. Visiška loginė izoliacija ir centrinė komutacija: tiek iš mobiliojo ryšio įrenginių, tiek iš fizinių šviesolaidžių ateinantys srautai sujungiami į bendrą VMS vaizdo VLAN segmentą, kuris yra visiškai izoliuotas nuo VRSA savivaldybės vidinio tinklo. Centriniame serverių mazge integruotas srautas priimamas per magistralinius komutatorius su 10 Gbps SFP+ sąsajomis, veikiančiomis LACP režimu.

Lentelė Nr. 12: Techniniai ir funkciniai reikalavimai tinklo įrangai ir ryšio paslaugoms

Reikalavimo ID	Tinklo / Ryšio komponentas	Minimalūs techniniai ir funkciniai reikalavimai tinklo įrangai ir paslaugoms
REQ-NET-01	Centrinis magistralinis komutatorius (Core Switch)	Pramoninis L3 lygio valdomas komutatorius. Ne mažiau kaip 8x 10G SFP+ lizdai, ne mažiau kaip 24x 1G/2.5G RJ45 prievadai. Komutacinė galia (*Switching capacity*) ne mažesnė kaip 128 Gbps. Pilnas IEEE 802.1Q (VLAN), LACP (802.3ad) bei IGMP v2/v3 Snooping (Multicast vaizdo srautų valdymui) palaikymas. Du karštojo keitimo (*Hot-Swap*) maitinimo šaltiniai.
REQ-NET-02	Uždaro 4G/5G ryšio paslauga ir lauko įrenginiai (Operatoriaus užduotis)	Privalomas uždaro tinklo (dedicated MPLS APN/VPN) sukonfigūravimas be išėjimo į viešąjį internetą. Ryšio priėmimui nutolusiuose taškuose tiekėjas turi naudoti pramoninius išorinius 5G lauko įrenginius (*CPE*), palaikančius 5G naujausius 3GPP standartus, su ne žemesne kaip IP55 apsaugos klase ir darbine temperatūra nuo -30 °C iki +50 °C. Tiekėjas privalo užtikrinti garantuotą minimalų išeinantį pralaidumą (*CIR*), atitinkantį kamerų tipų poreikius.
REQ-NET-03	Pramoniniai lauko komutatoriai kamerų	Pramoniniai L2/L3 komutatoriai, montuojami lauko spintose. Vidinio LTE modulio ar SIM lizdo palaikymas nėra privalomas, o duomenis iš išorinio 5G įrenginio priima per

	mazguose (Edge Switches)	standartinį RJ45 Ethernet prievadą. Darbinė temperatūra nuo -30 °C iki +50 °C. Apsauga nuo viršįtampių ir žaibo (min. 6kV). Ne mažiau kaip 4x PoE+ (802.3at) prievadai kamerų maitinimui (bendras PoE biudžetas min. 60W) bei bent 1x 1G SFP optinis arba Ethernet lizdas magistraliniam ryšiui.

Toks architektūrinis sprendimas yra ypač naudingas savivaldybei, nes nuima naštą nuo lauko spintelėse esančios įrangos. Išoriniai įrenginai (*CPE*) visiškai išsprendžia mobiliojo ryšio signalo slopinimo problemą, kuri dažnai kyla bandant antenas montuoti metalinių spintelių viduje, o pačioje spintelėje naudojami standartiniai pramoniniai PoE komutatoriai tampa pigesni, lengviau pakeičiami gedimo atveju ir reikalauja mažiau priežiūros. Visi srautai lieka izoliuoti ir apsaugoti uždarame operatoriaus tinklo VPN cikle.

2.5. ESAMOS ELEKTROS ENERGIJOS INFRASTRUKTŪROS REVIZIJA IR MAITINIMO SPRENDINIŲ INŽINERINIS PAGRINDIMAS

2.5.1. Kritinės problemos identifikavimas ir esamos būklės apribojimai

Atlikus planuojamų 330 vaizdo stebėjimo kamerų taškų geografinį auditą 23-jose Vilniaus rajono seniūnijose, nustatyta kritinė infrastruktūros problema – didžiojoje dalyje operatyviai svarbių vietų (kryžminėse sankryžose, kelių įvažiavimuose, viešosiose erdvėse) nėra nuolatinio, 24/7 veikiančio elektros energijos maitinimo šaltinio.

Dauguma parinktų taškų yra nutolę nuo savivaldybės ar seniūnijų administracinių pastatų, o artimiausia fizinė infrastruktūra yra gatvių apšvietimo atramos arba valstybinės elektros skirstomųjų tinklų linijos. Esamos būklės elektros infrastruktūros apribojimai skirstomi į tris esmines grupes:

1. Gatvių apšvietimo tinklo ciklišKumas: Dalis kamerų techniškai gali būti montuojamos ant gatvių apšvietimo atramų, tačiau šiose linijose elektros įtampa yra tiekiama tik tamsiu paros metu (įjungus gatvių apšvietimą). Dieną linijose įtampa visiškai atjungiama, todėl pramoninės 5MP/8MP/32MP lauko kameros, reikalaujančios nuolatinio 24/7 maitinimo, negali funkcionuoti be papildomų buferinių sprendimų.
2. Technologinis ir finansinis prisijungimo prie skirstomųjų tinklų (ESO) sudėtingumas: Taškuose, kur nėra jokios esamos infrastruktūros, naujo fizinio elektros įvado projektavimas, techninių sąlygų gavimas iš skirstomųjų tinklų operatoriaus, kabelių klojimas po žeme ir skaitiklių spintų statyba reikalauja didelių laiko sąnaudų (nuo 6 iki 12 mėnesių vienam taškui) ir neproporcingai didelių kapitalinių investicijų (CAPEX).
3. Visiškas energetinis izoliuotumas nutolusiuose kelių mazguose: Rajoninių kelių sankryžose ir miškingose vietovėse, kurios yra kritiškai svarbios transporto priemonių

numerių atpažinimui (Tipas B / ANPR), fizinių kabelinių elektros linijų tiesimas yra techniškai neįmanomas dėl saugomų zonų arba kraštovaizdžio apribojimų.

2.5.2. Hibridinių elektros maitinimo sprendinių inžinerinis pagrindimas

Siekiant išspręsti elektros energijos trūkumo problemą ir užtikrinti nepertraukiamą vaizdo stebėjimo sistemos bei išorinių 5G ryšio įrenginių veikimą, Galimybių studijoje suprojektuoti ir ekonomiškai pagrįsti trys (3) alternatyvūs hibridiniai maitinimo scenarijai. Jie leidžia lanksčiai pritaikyti sprendimą kiekvienam iš 330 taškų, priklausomai nuo lokalios situacijos:

Scenarijus A: Akumuliatoriniai buferiniai blokai gatvių apšvietimo linijose

- Inžinerinis sprendinys: Taškuose, kur kameros montuojamos ant apšvietimo atramų, lauko komutacinėse spintose įrengiami specializuoti pramoniniai buferiniai maitinimo šaltiniai su didelės talpos LiFePO4 (Ličio geležies fosfato) akumuliatorių baterijomis.
- Veikimo principas: Tamsiu paros metu, kai gatvių apšvietimas įjungtas, sistema ne tik maitina kameras bei ryšio įrangą, bet ir maksimaliu greičiu įkrauna integruotas baterijas. Dienos metu, kai apšvietimo linija išjungiama, sistema automatiškai, per kelias milisekundes perjungia maitinimą iš baterijų masyvo. Akumuliatorių talpa privalo būti apskaičiuota taip, kad užtikrintų autonominį įrangos veikimą ne mažiau kaip 19 valandų atšiauriausiomis žiemos sąlygomis.

Scenarijus B: Centralizuotas fizinis prisijungimas prie skirstomųjų tinklų linijų

- Inžinerinis sprendinys: Taškuose, kur vaizdo stebėjimo mazgai atlieka didelę reikšmę (pvz., kelių susikirtimai su dideliu eismo intensyvumu, kur diegiamos didelės galios Tipas C greitaeigės PTZ ir Tipas B ANPR kameros), ir baterijų sistemų naudoti neįmanoma dėl didelio suminio energijos poreikio arba kaštų.
- Veikimo principas: Šiose vietose projektuojamas standartinis fizinis prijungimas prie skirstomųjų tinklų operatoriaus žemos įtampos linijų. Pirkimo sąlygose numatoma, kad Tiekėjas privalo parengti el. projektus, suderinti sąlygas, įrengti lauko apskaitos-paskirstymo spintas su elektros skaitikliais arba automatiniais jungikliais bei atlikti fizinius kabeliavimo darbus iki kamerų atramų.

Scenarijus C: Autonominiai hibridiniai atsinaujinančios energijos mazgai

- Inžinerinis sprendinys: Visiškai izoliuotuose taškuose (rajoniniuose keliuose, pamiškėse) projektuojamos autonominės hibridinės gamybos stotys, montuojamos tiesiogiai ant kameros atramos.
- Veikimo principas: Elektros energijos gamybai naudojamas hibridinis modelis, susidedantis iš monokristalinių saulės modulių (min. 400W galios) ir mikro vėjo generatoriaus (min. 300W galios), pritaikyto žemiems startiniams vėjo greičiams. Sugeneruota energija kaupiama lauko sąlygoms sertifikuotame LiFePO4 baterijų konteineryje su išmaniuoju MPPT valdikliu. Vėjo generatoriaus įtraukimas yra privalomas, kadangi Lietuvoje žiemos mėnesiais saulės generacija nukrenta iki kritinės

ribos, o vėjo aktyvumas šiuo periodu yra didžiausias, taip užtikrinant nepertraukiamą vaizdo perdavimą ištisus metus.

Lentelė Nr. 13: Techniniai reikalavimai maitinimo infrastruktūros komponentams

Reikalavimo ID	Komponento pavadinimas	Minimalūs techniniai ir funkciniai reikalavimai maitinimo įrangai
REQ-PWR-01	Pramoninė buferinė baterijų sistema (Scenarijus A)	Integruotas lauko sąlygoms pritaikytas UPS valdiklis su LiFePO4 baterijų moduliu. Talpa ne mažesnė kaip 100Ah prie 12VDC įtampos. Darbinė temperatūra nuo -20 °C iki +50 °C. Baterijų valdymo sistema (BMS) privalo turėti apsaugą nuo giliojo iškrovimo, perkrovimo ir perkaitimo. Minimalus ciklų skaičius iki 80% talpos likučio – 2000 ciklų.
REQ-PWR-02	Lauko apskaitos ir paskirstymo spintos (Scenarijus B)	Antivandalinė lauko spinta su ne žemesne kaip IP65 apsaugos klase ir mechaniniu užraktu. Įrengta dedikuota vieta skirstomųjų tinklų operatoriaus skaitikliui arba automatiniam jungikliui, integruota DIN bėgelių sistema, automatiniai jungikliai (MCB), nuotėkio relės (RCD) bei pramoninė B+C klasės viršįtampių apsauga (SPD), skirta apsaugoti kamerų elektroniką nuo tinklo įtampos šuolių ir žaibo iškrovų.
REQ-PWR-03	Autonominis hibridinis maitinimo komplektas (Scenarijus C)	Saulės modulis: Monokristalinis, min. 440W, efektyvumas ne mažesnis kaip 21%, su IK08 mechaniniu atsparumu smūgiams. Vėjo generatorius: Vertikalios arba horizontalios ašies, max. startinis vėjo greitis ne didesnis kaip 2.0 m/s, nominali galia min. 300W prie 11 m/s. MPPT valdiklis su integruotu RS485 ir SNMP komunikacijos protokolu, skirtu baterijos būsenos (SoC) nuotoliniam stebėjimui per VMS sveikatos modulį.

Inžinerinė išvada pirkimo specifikacijai:
Šis detalus trijų scenarijų išskyrimas techninėse sąlygose apsaugo savivaldybę nuo situacijos, kai laimėjęs tiekėjas atsisako vykdyti darbus paaiškėjus, kad numatytose vietose nėra elektros įvadų. Griežtas LiFePO4 baterijų ir hibridinės saulės/vėjo generacijos reikalavimas užtikrina, kad sistema funkcionuos 24/7 režimu be vaizdo praradimo, o visi projektavimo ir ESO sąlygų derinimo kaštai iš anksto gula ant Tiekėjo pečių pagal nurodytus biudžeto normatyvus, o Užsakovas turi iš ESO išimti prisijungimo sąlygas.

3. TECHNINIAI IR FUNKCINIAI REIKALAVIMAI KAMEROMS

3.1. Kamerų techniniai poreikiai (11 privalomų parametrų vertinimas)
Visi vaizdo stebėjimo sistemos plėtrai naudojami įrenginiai privalo būti pramoninio lygio (*Enterprise-grade*), pritaikyti nepertraukiamam 24/7 (day/night) veikimui Lietuvos klimato sąlygomis . Siekiant užtikrinti vienodą pasiūlymų vertinimą, kiekvienam iš penkių (5) nustatytų kamerų tipų taikoma ši 11-os esminių techninių parametrų matrica:
3.1.1. Tipas A: Didelės raiškos 4-ių jutiklių viename korpuse panoraminė lauko kamera (Multisensor PTRZ)

- 1. Raiška: Ne mažiau kaip 32MP bendra efektyvi raiška, kurią suformuoja keturi (4) nepriklausomi jutikliai, kiekvienas po 8MP (3840x2160).
- 2. Sensoriaus dydis: Ne mažesnis kaip 1/1.8” progresyvaus nuskaitymo (Progressive Scan) CMOS kiekvienam iš 4 jutiklių.
- 3. Matymo kampas: Kiekvieno jutiklio horizontalus matymo kampas reguliuojamas nuo min. 50° iki max. 95° (bendras sistemos dengiamas kampas – iki 360° be aklųjų zonų).
- 4. Naktinio matymo funkcionalumas: Išmanusis automatinis mechaninis IR-cut filtras (ICR), skirtas persijungimui tarp dieninio (spalvoto) ir naktinio (nespalvoto) režimų.
- 5. Apšvietimo parametrai: Integruotas kintamo intensyvumo adaptyvus IR pašvietimas visiškoje tamsoje (0 Liuksų) ne mažesniu kaip 30 metrų atstumu. Minimalus jautrumas šviesai spalvotame režime: 0.2 Lux .
- 6. Užrakto greitis (Shutter Speed): Automatinis arba rankinis elektroninis užraktas, veikiantis diapazone nuo 1/4 s iki 1/30 000 s.
- 7. Kadrų skaičius per sekundę (FPS): Ne mažiau kaip 15 fps (realus laikas) prie maksimalios 32MP raiškos, užtikrinantis sklandų judančių objektų fiksavimą.
- 8. Palaikomi vaizdo kodekai ir formatai: Aparatinis H.265, H.264 (High/Main Profile) ir MJPEG profilių palaikymas.
- 9. Atsparumo aplinkos poveikiui klasė: Ne žemesnė kaip IP66 (sandarumas) ir IK10 (mechaninis atsparumas vandalizmui).
- 10. Veikimo temperatūros intervalas: Stabilus veikimas ir paleidimas esant temperatūrai nuo -30 °C iki +50 °C.
- 11. Vidinės atminties poreikis: Integruotas MicroSD/SDHC/SDXC lizdas, palaikantis ne mažesnę kaip 512 GB pramoninę atminties kortelę vietiniam įrašų dubliavimui (Edge Storage).

3.1.2. Tipas B: Specializuota transporto numerių atpažinimo (ANPR) ir konteksto kamera

- 1. Raiška: Hibridinė sistema (du jutikliai viename korpuse): Ne mažiau kaip 5MP OCR jutikliui ir 8MP kontekstiniam CMOS jutikliui.

- 2. Sensoriaus dydis: ANPR jutiklis: 2/3” OCR sensor (apsauga nuo vaizdo liejimosi); Kontekstinis jutiklis: 8 Megapixel (4K) color CMOS.
- 3. Matymo kampas: Reguliuojamas motorizuotu objektyvu (12-40mm), horizontalus kampas nuo 11° iki 36°, skirtas tikslingam eismo juostų padengimui iki 40m atstumu.
- 4. Naktinio matymo funkcionalumas: Specializuotas naktinis OCR režimas su sinchronizuotu impulsiniu pašvietimu ir aplinkos šviesos atspindžių (pvz., priekinių žibintų) filtravimu.
- 5. Apšvietimo parametrai: Integruotas kryptingas IR apšvietimas iki 40 metrų transporto numerių atspindžiams fiksuoti.
- 6. Užrakto greitis (Shutter Speed): Greitaeigis užraktas, pritaikytas transporto srautui.
- 7. Kadrų skaičius per sekundę (FPS): ne mažiau kaip 50 fps ANPR jutikliui (skirtas transporto greičiui ≥250 km/h ir nuskaitymo patikimumui ≥99,5%) ir ne mažiau kaip 15 fps (realus laikas) prie maksimalios 8MP raiškos kontekstiniam jutikliui.
- 8. Palaikomi vaizdo kodekai ir formatai: H.265, H.264 ir tiesioginis nesuspaustų JPEG / BMP tranzito nuotraukų generavimas OCR serveriui.
- 9. Atsparumo aplinkos poveikiui klasė: Ne žemesnė kaip IP66 ir IK10 apsauga.
- 10. Veikimo temperatūros intervalas: Nuo -30 °C iki +50°C .
- 11. Vidinės atminties poreikis: Integruota ne mažesnė kaip 16 GB SD vidinė pramoninė atmintis duomenų bazių saugojimui.

3.1.3. Tipas C: Greitaeigė valdoma lauko kamera (PTZ)

- 1. Raiška: Tikrasis 8MP (3840x2160) vaizdas su ne mažiau 20x optinio artinimo ir skaitmeninis ne mažiau 12x artinimo arba 5MP (2560 x 1920) su ne mažiau 30x optinio artinimo ir skaitmeninis ne mažiau 12x artinimo.
- 2. Sensoriaus dydis: Ne mažesnis kaip 1/2.8” progresyvaus nuskaitymo (Progressive Scan) CMOS.
- 3. Kameros sukimosi greičio diapazonas horizontalioje plokštumoje ne prasčiau nei 0.04°/s - 300°/s
- 4. Naktinio matymo funkcionalumas: Automatinis naktinis režimas, sinchronizuotas su optinio artinimo mechanizmu (apšvietimo kampas siaurėja artinant vaizdą).
- 5. Apšvietimo parametrai: IR pašvietimas, veikiantis iki 150 metrų visiškoje tamsoje.
- 6. Užrakto greitis (Shutter Speed): Nuo 1/4s iki 1/30 000s.
- 7. Kadrų skaičius per sekundę (FPS): Ne mažiau kaip 15 fps prie 8MP raiškos arba ne mažiau kaip 25 fps prie 5MP raiškos.
- 8. Palaikomi vaizdo kodekai: H.265, H.264, MJPEG.
- 9. Atsparumo aplinkos poveikiui klasė: IP66 ir IK10.
- 10. Veikimo temperatūros intervalas: Nuo -30 °C iki +50 °C.
- 11. Vidinės atminties poreikis: Lizdas MicroSD kortelei ≥ 512GB talpos.

3.1.4. Tipai D ir E: 8MP (4K) Kupolinė (Dome) ir Cilindrinė (Bullet) lauko kameros

- 1. Raiška: Ne mažiau kaip 8MP (3840x2160) raiška.
- 2. Sensoriaus dydis: Ne mažesnis kaip 1/1.8” progresyvaus nuskaitymo (Progressive Scan) CMOS jutikliui.
- 3. Matymo kampas: Horizontalus kampas nuo 50° iki 95° (motorizuotas varifokalinis objektyvas).
- 4. Naktinio matymo funkcionalumas: Mechaninis ICR filtras su automatiniu perjungimu.
- 5. Apšvietimo parametrai: Tipo D (Kupolinė) – iki 50m adaptyvus IR; Tipo E (Cilindrinė) – iki 50m adaptyvus IR.
- 6. Užrakto greitis (Shutter Speed): Nuo 1/4 s iki 1/30 000 s.
- 7. Kadrų skaičius per sekundę (FPS): Ne mažiau kaip 15 fps prie 8MP.
- 8. Palaikomi vaizdo kodekai: H.265, H.264, MJPEG.
- 9. Atsparumo aplinkos poveikiui klasė: IP66/IP67 sandarumas ir IK10 apsauga nuo smūgių.
- 10. Veikimo temperatūros intervalas: Nuo -30 °C iki +50 °C .
- 11. Vidinės atminties poreikis: Palaikoma MicroSD kortelė iki 512 GB.

Kamerų minimalūs parametrai lentelė:

Tipas	**Paskirtis**	**Minimalūs parametrai**
A vaizdo	Multisensor (visakryptė)	Viename korpuse 4 jutikliai × 8 MP CMOS; bendra ≥32 MP; PTR; kiekvienas jutiklis ≥1/1.8"; motorizuotas varifokalinis objektyvas; H kampas 50–95°; iki 360°; IR ≥30 m; ≥15 fps prie maksimalios raiškos; H.265/H.264/MJPEG; IP66; IK10; -30…+50 °C; ≥512 GB vidinė atmintis.
B ANPR	ANPR/OCR + kontekstas (numerių nuskaitymo kamera)	Viename korpuse 2 jutikliai: ≥5 MP OCR, + ≥8 MP CMOS; iki 200 km/h ir 2 kelio juostos (juostos plotis ≥3,75 m), nuskaitymo patikimumas 99,5% prie ≥250 km/h, 12–40 mm motorizuotas varifokalinis objektyvas; H kampas 11–36°; IR ≥40 m; ≥50 fps ANPR ir ≥15 fps kontekstas; IP66/IK10; -30…+50 °C; ≥16 GB vidinė atmintis.

Tipas	Paskirtis	Minimalūs parametrai
C vaizdo	PTZ (valdoma)	Viename korpuse 1 jutiklis: ≥8 MP (3840×2160) su ≥20× optinio ir ≥12× skaitmeninio arba 5 MP (2560 x 1920) su ≥30× optinio ir ≥12× skaitmeninio; ≥1/2.8" CMOS; ≥ IR iki 150 m; ≥15 fps prie maksimalios raiškos; H.265/H.264/MJPEG; IP66/IK10; -30…+50 °C; ≥512 GB vidinė atmintis.
D vaizdo	Dome (kupolinė)	Viename korpuse 1 jutiklis: ≥8 MP; ≥1/1.8" CMOS; motorizuotas varifokalinis objektyvas, H 50–95°; ICR; adaptyvus IR iki 50 m; ≥15 fps prie maksimalios raiškos; H.265/H.264/MJPEG; IP66/IK10; -30…+50 °C; ≥512 GB vidinė atmintis.
E vaizdo	Bullet	Viename korpuse 1 jutiklis: ≥8 MP; ≥1/1.8" CMOS; motorizuotas varifokalinis objektyvas, H 50–95°; ICR; adaptyvus IR iki 50 m; ≥15 fps prie maksimalios raiškos; H.265/H.264/MJPEG; IP66/IP67; IK10; -30…+50 °C; ≥512 GB vidinė atmintis.

3.2. Kamerų funkciniai reikalavimai (6 privalomų sričių vertinimas)
Visi kamerų tipai privalo gamykliškai ir aparatiškai palaikyti šias 6 esmines funkcines grupes, išskyrus „B“ tipą:

1. Suderinamumas su standartais ir protokolais (įskaitant ONVIF): Kameros turi turėti galiojančius ONVIF Profile S (vaizdo perdavimui) ir Profile T (pažangiam H.265 srautų ir analitikos perdavimui) sertifikatus. Palaikomi tinklo protokolai: IPv4/IPv6, HTTP, HTTPS, TLS 1.2, RTSP, RTP, TCP, UDP, DHCP, NTP, IGMP (Multicast).
2. Kibernetinio saugumo funkcijos: Užtikrinamas saugaus įkrovimo patikra (Secure Boot). Ir gamintojo autorizuota kameros programinė įranga (Signed Firmware).
3. Privatumo zonų maskavimas (Privacy Masking): Galimybė vaizdo scenoje sukonfigūruoti ne mažiau kaip 5 nepriklausomas privatumo zonas (angl. *privacy masks*), kurios visiškai užtušuojamos/blokuojamos (pvz., privatūs gyventojų langai, kiemai), kad operatoriai jų nematytų, o įrašas tose zonose nebūtų vykdomas.
4. Vaizdo analitika kamerose (Edge AI) neapkraunant centrinio VMS serverio. Privalomas funkcijų rinkinys: virtualios linijos kirtimas, įsibrovimas į zoną, neteisėtas objekto palikimas arba dingimas iš zonos, vaizdo sabotažo (angl. *tamper detection* – kameros nusukimo, uždengimo, fokusavimo praradimo) identifikavimas. Objektų klasifikavimas ir

atributų nustatymas: realiu laiku klasifikuoja objektus į dvi pagrindines grupes: Žmonės ir Transporto priemonės. Sistema privalo nustatyti šiuos atributus ir perduoti juos kaip metaduomenis į VMS: drabužių spalva (viršutinė/apatinė dalis), kepurės buvimas; transporto priemonių tipas (lengvasis, sunkvežimis, autobusas, motociklas, dviratis), transporto priemonių tipų spalva ir kryptis.

5. Vaizdo suspaudimo ir duomenų srauto valdymo funkcijos: Integruota išmanioji srauto valdymo technologija (pvz., kintamo pralaidumo algoritmai), kuri dinamiškai analizuoja vaizdo sceną: kai scenoje judėjimo nėra, bitų srautas (*bitrate*) galimai sumažinamas iki 50–70%, o aptikus judesį, akimirksniu grąžinama maksimali kokybė, optimizuojant tinklo ir diskų saugyklos poreikį.
6. Aplinkos apsaugos kriterijų taikymo aspektai: Kamerų gamyboje privalo būti nenaudojamos pavojingos medžiagos (atitiktis RoHS direktyvai). Įrenginiai privalo turėti energijos efektyvumo valdymą, palaikyti energijos taupymo režimus per PoE (IEEE 802.3af/at), o pakuotės medžiagos turi būti perdirbamos, atitinkant savivaldybės žaliųjų pirkimų reikalavimus.

„B“ tipo kameros: privalo gamykliškai ir aparatiškai palaikyti šias 6 esmines funkcines grupes:

1. Suderinamumas su standartais ir protokolais (įskaitant ONVIF): Kameros turi turėti galiojančius ONVIF Profile S (vaizdo perdavimui). Palaikomi tinklo protokolai: IPv4/IPv6, HTTP, HTTPS, TLS 1.2, RTSP, RTP, TCP, UDP, DHCP, NTP, IGMP.
2. Kibernetinio saugumo funkcijos: Užtikrinamas saugaus įkrovimo patikra (Secure Boot). Gamintojo autorizuota kameros programinė įranga (Signed Firmware).
3. Išmanusis suliejimas (Blurring): automatiškai atpažinus transporto priemonę, turi būti visi kiti aplinkiniai subjektai (pėstieji, dviratininkai, aplinkinių namų langai ar objektai už eismo juostos ribų) automatiškai suliejami pačiame vaizde.
4. Vaizdo analitika kamerose (Edge AI) neapkraunant centrinio VMS serverio. Privalomas funkcijų rinkinys: atpažinti transporto priemonių valstybinį numerį, nemažiau nei dvejose eismo juostose (kai eismo juostos plotis nemažiau kaip 3,75 metro) bet kuriuo paros metu ir judant transporto priemonei iki 250 km/h greičiu; vykdyti numerių atpažinimo tikslumą ne mažesnei nei 99,5% iš visų tinkamai užfiksuotų transporto priemonių numerių; įvertinti judančios transporto priemonės greitį; atpažinti prieš eismą važiuojančias transporto priemones; atpažinti sustojusias transporto priemones; integruoti su trečiųjų šalių vaizdo stebėjimo sistemomis; valdyti (baltuosius/juoduosius) sąrašus, su nepriklausomu veiksmu kiekvienam sąrašui; atpažinti transporto priemonių pavojingų krovinių vežimo ADR lenteles (Kemler numeriai); siųsti IP pranešimus (HTTP post formatu arba lygiaverčiu) į ne mažiau kaip 2 skirtingus serverius (virtualias mašinas) Užsakovo ir Policijos.Objektų klasifikavimas ir atributų nustatymas: atpažintas transporto priemonės valstybinis numeris, kryptis, markė, modelis, tipas (klasė), spalva, laikas ir vietos koordinatė.

5. Vaizdo suspaudimo ir duomenų srauto valdymo funkcijos: Integruota išmanioji srauto valdymo technologija (pvz., kintamo pralaidumo algoritmai), kuri dinamiškai analizuoja vaizdo sceną: kai scenoje judėjimo nėra, bitų srautas (*bitrate*) sumažinamas iki 50–70%, o aptikus judesį, akimirksniu grąžinama maksimali kokybė, optimizuojant tinklo ir diskų saugyklos poreikį.
6. Aplinkos apsaugos kriterijų taikymo aspektai: Kamerų gamyboje privalo būti nenaudojamos pavojingos medžiagos (atitiktis RoHS direktyvai). Įrenginiai privalo turėti energijos efektyvumo valdymą, palaikyti energijos taupymo režimus per PoE (IEEE 802.3af/at), o pakuotės medžiagos turi būti perdirbamos, atitinkant savivaldybės žaliųjų pirkimų reikalavimus.

3.3. VAIZDO STEBĖJIMO, ĮRAŠYMO IR VALDYMO PROGRAMINĖS ĮRANGOS (VMS) TECHNINIAI IR FUNKCINIAI REIKALAVIMAI

3.3.1. VMS Techniniai parametrai

VMS programinė įranga privalo atitikti šiuos bazinius techninius parametrus:

1. Palaikomų kamerų gamintojų skaičius: ne mažiau kaip 50 unikalių pasaulinių gamintojų gamyklinių (angl. *native*) API tvarkyklių palaikymas.
2. Įrašymo serverių / įrenginių skaičius: Architektūra privalo gebėti centralizuotai valdyti ir sinchronizuoti iki 300 nepriklausomų įrašymo mazgų (SAS serverių).
3. Palaikomų kamerų skaičius: Sistemos programinis branduolys privalo turėti mastelio licencijavimą iki 2000 IP kamerų, pradiniame etape pilnai apdorojant 330 kamerų srautus.
4. Darbo vietų skaičius: Palaikomas neribotas operatorių paskyrų skaičius, pradiniame etape licencijuojant dvi (2) stacionarias operatoriaus darbo vietas ir tris (3) stacionarias darbo vietas viešosios tvarkos specialistams.
5. Palaikomų operacinių sistemų skaičius: suderinamumas su ne mažiau kaip 3 operacinių sistemų šeimomis (Windows Server/Linux – serveriams; Windows 11 – operatoriams; iOS/Android – nuotolinei prieigai pagal poreikį).
6. Duomenų bazės suderinamumas: Integruotas pramoninis suderinamumas su Microsoft SQL Server Express/Standard/Enterprise (64-bit), naudojant p*er „Core“* modelį arba „VM“ modelį.

3.3.2. VMS Funkciniai reikalavimai (12 esminių funkcijų išplėtojimas)

VMS platforma privalo gamykliškai užtikrinti ir palaikyti šį funkcinį paketą, kuris būtų įtrauktas į viešojo pirkimo specifikaciją kaip atmetimo kriterijai:

Komentuota [1]: STRUKTŪRA: antraštėje 12 funkcijų, tačiau išplėtotame sąraše 11; suvestinėje 11 ID ir praleistas VMS-05.

1. Suderinamumas su standartais ir protokolais (įskaitant ONVIF): VMS privalo turėti oficialų, profilių gamintojo patvirtintą suderinamumą su ONVIF Profile S, G ir T standartais. Programinė įranga privalo palaikyti saugų duomenų perdavimą tinkle naudojant HTTPS, TLS 1.2, RTSPS (RTSP over TLS) bei multicast srautų valdymą per IGMP v2/v3 protokolus.
2. Vaizdo įrašymas ir saugojimas: VMS privalo užtikrinti nepertraukiamą 24/7 vaizdo srautų priėmimą ir tiesioginį rašymą į ne mažesnį kaip RAID 5 diskų masyvą. Sistema turi palaikyti skirtingus įrašymo režimus: nuolatinį, pagal grafiką (tvarkaraštį), pagal kameros AI analitikos aliarmo signalą arba pagal vaizdo pokytį (judesio detekciją). Minimalus vaizdo saugojimo terminas – 30 dienų, su automatiniu seniausių duomenų perrašymo (angl. first-in, first-out - FIFO) mechanizmu.
3. Naudotojų teisių valdymas ir saugumo funkcijos: Teisių valdymas privalo būti pagrįstas vaidmenimis (RBAC). VMS turi užtikrinti integraciją su savivaldybės centralizuota katalogų tarnyba per saugų LDAP (Active Directory) protokolą, palaikyti daugiaveiksnį autentifikavimą (MFA) arba dviejų faktorių autentifikavimą (2FA) ir turėti nekeičiamą audito žurnalą (Tamper-proof Audit Trail), kuriame fiksuojamas kiekvienas operatoriaus veiksmas (prisijungimas, vaizdo peržiūra, archyvo eksportas), o šių įrašų negali ištrinti ar koreguoti joks naudotojas.
4. Išmanioji paieška (Smart Search / Meta Search): VMS privalo turėti pažangų paieškos variklį, gebantį vykdyti momentinę paiešką archyve pagal IP kamerų sugeneruotus AI metaduomenis (objektų atributus). Operatorius privalo turėti galimybę filtruoti įrašus pagal asmens charakteristikas (žmogus, drabužių spalva, objektas) arba transporto priemonės savybes (markė, modelis, klasė (tipas), spalva), gaunant paieškos rezultatus iš pasirinktų IP kamerų vienu metu.
5. Dinaminis privatumo zonų ir veidų maskavimas (Dynamic Privacy Masking): Programinė įranga privalo užtikrinti galimybę tiesiogiai vaizdo sraute ir peržiūros metu užmaskuoti (užtušuoti juodais arba neryškiais pikseliais) privatumo zonas. VMS privalo palaikyti tiek statinį maskavimą (privačių namų langų paslėpimas), tiek dinaminį maskavimą peržiūros metu, kuris realiu laiku seka ir automatiškai maskuoja judančių praeivių veidus ar pašalinių automobilių valstybinius numerius operatoriaus ekrane. Pagrindiniame vaizdo archyve (RAID 5 arba RAID 6 masyve) turi būti išsaugomas originalus, nemaskuotas vaizdas, siekiant išlaikyti teismo ekspertizės įrodomąją vertę. Teisė peržiūrėti ir eksportuoti originalų, nemaskuotą vaizdą turi būti ribojama pagal vaidmenis (RBAC) ir prieinama tik autorizuotiems administratoriams.
6. Momentinė vaizdo peržiūra (Instant Playback & Alarm Pop-up): Stebėjimo lange operatoriui paspaudus vieną mygtuką, VMS privalo leisti atsukti ir peržiūrėti tos kameros paskutinių 1–15 minučių įrašą tame pačiame lange, nenutraukiant tiesioginės transliacijos. Fiksavus kritinį įvykį (pvz., automobilio pažeidėjo numerį), sistemoje turi

suveikti aliarmo iššokantis langas (Alarm Pop-up), kuris automatiškai nukreipia operatoriaus dėmesį į incidento kamerą.

7. Žiniatinklio (WEB) funkcionalumas: VMS privalo turėti integruotą, saugų (HTTPS) Web serverį, leidžiantį autorizuotiems savivaldybės ar seniūnijų darbuotojams prisijungti prie sistemos per standartines interneto naršykles (be papildomų programų ar įskiepių diegimo). WEB sąsaja privalo leisti stebėti tiesioginį vaizdą, atlikti archyvo paiešką ir eksportuoti vaizdo medžiagą, ribojant prieigą tik prie konkrečiai seniūnijai priskirtų kamerų.
8. Aukštas prieinamumas ir „Failover“ funkcionalumas: VMS privalo palaikyti „N+1“ prieinamumo klasterizaciją. Centralizuotame modelyje esantis rezervinis įrašymo serveris privalo nuolat stebėti aktyvių įrašymo serverių būseną. Jei vienas iš pagrindinių įrašymo serverių patiria aparatinį gedimą, rezervinis serveris perimtų nurodytą kamerų srautų įrašymą.
9. Centralizuota vaizdo analitika: Programinė įranga privalo gebėti priimti, interpretuoti ir struktūrizuoti analitinius signalus, ateinančius iš kamerų procesorių (Edge AI), taip pat turėti vidinius serverinius algoritmus, skirtus sudėtingesnėms operacijoms: srautų skaičiavimui, judėjimo tankio žemėlapių (Heatmaps) generavimui viešosiose erdvėse bei garso anomalijų (šūvio, stiklo dūžio) vizualizavimui aliarmo žurnale.
10. Transporto priemonių valstybinių numerių (ANPR) atvaizdavimas: VMS privalo turėti dedikuotą sąsajos modulį arba posistemę, kuris realiu laiku iš specializuotų ANPR kamerų priima atpažintus valstybinius numerius, MMCR duomenis (markę, modelį, spalvą) ir momentines tranzito nuotraukas. Šie duomenys turi būti vizualiai atvaizduojami operatoriaus ekrane specialiame eismo srauto žurnale (angl. ANPR Live Roll), su galimybe akimirksniu patikrinti numerį „juoduosiuose sąrašuose“ ir generuoti perspėjimus ir siųsti įspėjamąjį pranešimą SMS žinute, pranešimo tekste nurodant valstybinį numerį.
11. Transporto priemonių valstybinių numerių (ANPR) paieška: Atlikti pilną ir/arba dalinę transporto priemonių numerių paiešką pagal pasirenkamus laukus (kriterijus arba požymius) aktualiose ir/arba archyvinėse duomenų bazėse, nurodant: (a) pilną transporto priemonės numerį; (b) ne pilną transporto priemonės numerį; (c) valstybę, kurioje registruota transporto priemonė; (d) transporto priemonės spalvą; (e) transporto priemonės tipą; (f) vaizdo kameros identifikacinį požymį; (g) vaizdo kameros vietą; (h) vaizdo kameros kryptį; (i) datos ir laiko pasirenkamus intervalus; (j) atpažintus numerius (l) neatpažintus numerius. Paieškos operatoriaus sąsaja turi būti suderinama su paplitusiomis interneto (pvz.: Internet Explorer, MS Edge, Google Chrome, Mozilla Firefox (arba lygiavertėm)) naršyklėmis.
12. Kamerų atvaizdavimas savivaldybės žemėlapyje (Interaktyvūs GIS žemėlapiai): VMS operatoriaus sąsaja privalo turėti integruotą interaktyvų 2D/3D žemėlapių modulį (palaikantį OpenStreetMap, ArcGIS arba Google Maps). Žemėlapyje privalo būti

geografiškai išdėstytos visos **VRSA** 23 seniūnijų kameros su jų realia būsena (veikia, atjungta, aliarmas). Žemėlapyje turi matytis kamerų apžvalgos kampų kryptys ir spinduliai, o operatorius privalo turėti galimybę paleisti tiesioginį vaizdą dukart paspaudęs ant kameros piktogramos žemėlapyje.

13. Vaizdo perdavimas iš darbo vietų ir vaizdo sienų valdymas: Programinė įranga privalo užtikrinti operatoriams galimybę keistis vaizdo srautais tarp darbo vietų (angl. Video Push). Pavyzdžiui, pirmasis operatorius, aptikęs incidentą savo ekrane, privalo turėti galimybę vienu pelės paspaudimu nukreipti tą srautą į antrojo operatoriaus ekraną arba į centralizuotą **VRSA** vaizdo sieną (Video Wall), užtikrinant sklandų komandinį situacijų valdymą.

VMS funkcijų minimalūs reikalavimai lentelė

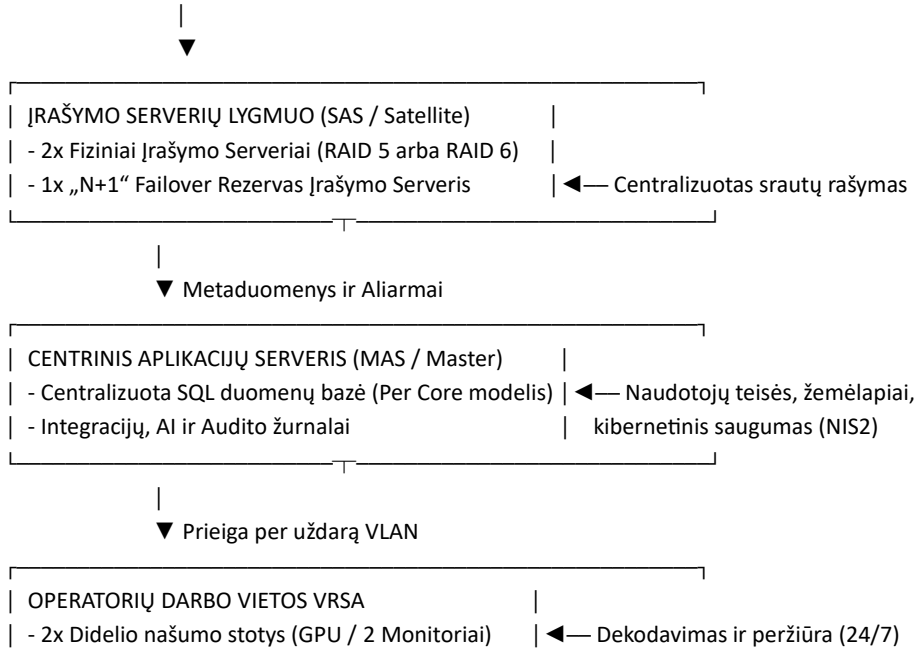
ID	Funkcija	Minimalus reikalavimas
VMS-01	Kamerų palaikymas	Sistema turi užtikrinti ne mažiau kaip 330 IP kamerų eksploatavimą pradiniame etape. Sistema turi būti techniškai plečiama bent iki 2 000 IP kamerų nekeičiant architektūros branduolio ir pagrindinės programinės įrangos. Užsakovas neįsipareigoja įsigyti licencijų daugiau kaip 330 kamerų pradiniame etape.
VMS-02	Gamintojų palaikymas	Ne mažiau kaip 50 pasaulinių gamintojų native API / tvarkyklių arba lygiavertis atviras integravimo mechanizmas.
VMS-03	Įrašymas	24/7, pagal grafiką, pagal AI aliarmą ir judesį; FIFO perrašymas.
VMS-04	Archyvas	Ne trumpiau kaip 30 dienų; originalios raiškos įrašymas pagal techninį projektą.
VMS-06	RBAC	Vaidmenimis grįstas teisių valdymas, integracija su AD per LDAP, MFA administravimo sąsajoms.
VMS-07	Auditas	Nekeičiamas / nuo administratoriaus manipuliavimo apsaugotas audito žurnalas.
VMS-08	Analitika	Edge AI metaduomenų priėmimas ir serverinė analitika; srautų skaičiavimas, heatmap ir aliarmų valdymas.
VMS-09	ANPR	ANPR Live Roll, numerių ir t/p paieška (dalinė arba pilna), juodųjų sąrašų perspėjimai, tranzito nuotraukos ir metaduomenys.

ID	Funkcija	Minimalus reikalavimas
VMS-10	GIS	Interaktyvus 2D/3D žemėlapis; 23 seniūnijų kameros, būsena, kryptis / aprėptis ir tiesioginio vaizdo paleidimas.
VMS-11	Video Push	Vieno operatoriaus vaizdo srauto perdavimas kitai darbo vietai / Video Wall.
VMS-12	Eksportas	Vaizdo ir metaduomenų eksportas; ANPR XML/JSON eksportas; Eksportuojamo vaizdo suliejimo funkcija.

4. VAIZDO VALDYMO PROGRAMINĖS ĮRANGOS IR SERVERIŲ INFRASTRUKTŪROS REIKALAVIMAI

4.1. Centralizuotos VMS architektūros koncepcija

Siekdamas užtikrinti patikimą 330 kamerų valdymą, Užsakovas diegia korporatyvinio lygio centralizuotą Vaizdo valdymo programinę įrangą (VMS), kuri naudoja Master/Satellite (MAS/SAS) paskirstytųjų serverių architektūrą. Šis modelis leidžia atskirti sistemos administravimą, duomenų bazių valdymą ir tiesioginį vaizdo srautų įrašymą į skirtingus fizinius ar virtualius vienetus, užtikrinant maksimalų sistemos naudingumą ir stabilumą.



Sistemos minimalūs reikalavimai lentelė:

ID	Reikalavimas	Minimalus reikalavimas
GEN-01	Sistemos mastas	Ne mažiau kaip 330 IP kamerų palaikymas pradiniame sprendime.
GEN-02	Architektūra	On-premise, centralizuota Master/Satellite (MAS/SAS) architektūra ar lygiavertis architektūrinis sprendimas.
GEN-03	Vaizdo saugojimas	24/7 įrašymas ir ne trumpesnis kaip 30 parų archyvas.
GEN-04	Tinklas	Atskiras, logiškai izoliuotas VMS vaizdo tinklas; centrinis projektinis įeinantis srautas – ne mažiau kaip 4 Gbps.
GEN-05	Saugumas	TLS/HTTPS, RBAC (vaidmenimis grįstas prieigos teisių valdymas), LDAP/AD (SSO – vartotojo slaptažodį administruoja domeno kontrolerio (DC) administratorius), MFA, nekeičiamas audito žurnalas („Security audit“), saugus įkrovimas („Secure Boot“)/ saugumo modulis („TPM“) pagal taikymą.
GEN-06	Prieinamumas	RAID1 OS ir RAID 5 arba 6 vaizdo duomenų telkiniui, automatinis duomenų bazių kopijų darymas, dubliuoti maitinimo šaltiniai.
GEN-07	ANPR	Specializuotas ANPR funkcionalumas 26 lokacijose, su metaduomenų ir nuotraukų apdorojimu.
GEN-08	SLA	24/7/365 incidentų registravimas, monitoringas ir reagavimas pagal 1–3 kritiškumo lygius.
GEN-09	Nuosavybė	Įranga, dokumentacija, konfigūracijos ir pagal sutartį perduodamos licencijos priklauso Užsakovui pagal sutarties sąlygas.
GEN-10	Plečiamumas	Sistema turi būti techniškai paruošta tolesnei IP kamerų plėtrai, nekeičiant architektūros branduolio.

VMS ir centrinio mazgo lentelė

Komponentas	Minimalus reikalavimas
MAS / Master	1 centrinis aplikacijų ir duomenų bazės serveris; VMS valdymas, metaduomenys, integracijos, auditas.
SAS / Satellite	Ne mažiau kaip 2 aktyvūs fiziniai vaizdo įrašymo serveriai ne mažiau kaip 1000Mbps vaizdo srauto įrašymo našumo per serverį ir 1 rezervinis vaizdo įrašymo serveris.
Prieinamumo priemonės	RAID1 OS, RAID5 arba RAID6 vaizdo duomenims, automatinės DB kopijos ir dubliuoti maitinimo šaltiniai.
Saugykla	RAID 5 arba 6 duomenų telkinys / lygiavertė programiškai valdoma gedimų tolerancijos architektūra.
SQL	Atskira NVMe/SSD RAID 1 arba techniškai lygiavertė sistema sisteminei DB ir metaduomenims.
Operatoriai	2 (dvi) didelio našumo darbo vietos; GPU dekodavimas; ne mažiau kaip dviejų monitorių palaikymas kiekvienoje.
Tinklas	Centrinis L3 magistralinis tinklas su 10G SFP+ uplink ir VLAN/LACP/IGMP funkcijomis.

Serveriai ir duomenų archyvas lentelė

ID	Komponentas	Minimalus reikalavimas
SRV-01	MAS	1 fizinis arba lygiavertis dedikuotas serveris; Windows Server 2022/2025 64-bit suderinamumas; VMS ir SQL funkcijos.
SRV-02	SAS	2 aktyvūs fiziniai įrašymo serveriai ir 1 rezervinis įrašymo serveris; vaizdo srautai įrašomi atskirai nuo MAS.
SRV-04	Saugyklos architektūra	RAID 5 arba RAID 6 / lygiavertė SDS gedimų tolerancijos architektūra; paskirstytas rašymas.
SRV-05	SQL saugykla	Atskiras NVMe/SSD RAID 1 arba lygiavertis masyvas sisteminei SQL DB, teisėms, laiko žymoms, aliarmams ir AI metaduomenims.

ID	Komponentas	Minimalus reikalavimas
SRV-06	Diskų talpa	Ne mažiau kaip 400 TB bendros fizinės diskų talpos; studijoje modeliuojama 20 TB Enterprise diskų pagrindu.
SRV-07	Hot-Spare	Kiekviename aktyviame SAS – ne mažiau kaip 1 aktyvus Hot-Spare; automatinis rebuild.
SRV-08	Įeinantis srautas	Nepertraukiamas įrašymas be frame dropping esant projektiniam ≥4 Gbps įeinančiam srautui.
SRV-09	TPM	TPM 2.0 arba lygiavertė aparatinė saugos priemonė.
SRV-10	Monitoringas	SNMP / sisteminės būklės monitoringas, diskų, temperatūros, maitinimo, tinklo ir VMS sveikatos stebėjimas.

4.2. VMS duomenų perdavimo reikalavimai

1. VMS duomenų perdavimo tinkle (perduodant informaciją tiek iš vaizdo perdavimo kamerų į centrą, tiek centre, tiek operatoriaus kompiuterinę darbo vietą) informacija (vaizdas, garsas, duomenys) turi būti perduodama TCP/IP protokolu, nenaudojant nesaugių analoginių perdavimo sistemų naudoti negalima.
2. Visas VMS duomenų perdavimo tinklas (WAN) ir jo dalys turi būti suprojektuotos ir įrengtos laikantis hierarchinės struktūros ir turi atitikti IT gerosios praktikos rekomendacijas dėl OSI ir TCP/IP standartinių modelių, o IP protokolas turi būti laikomas pagrindiniu maršrutizavimo protokolu. VMS duomenų perdavimas turi būti vykdomas atskirame, izoliuotame loginiame arba fiziniame tinkle, neturinčiame tiesioginės prieigos prie viešųjų interneto tinklų, remiantis Nacionalinio kibernetinio saugumo centro viešai paskelbtomis rekomendacijomis, ir tinklas turi būti loginiu arba fiziniu būdu atskirtas nuo kitų Tiekėjo ir paslaugų ir nuo viešųjų (interneto) tinklų arba jų VPN tunelių. Visas VMS duomenų perdavimo turi būti vykdomas, laikantis duomenų perdavimo izoliacijos ir saugumo, o uždaro tinklo technologija turi būti neblogesnė nei BGP/MPLS, remiantis ITU komiteto dokumentu G.8110.1, TIA ir IETF standartais bei rekomendacijomis, pateikiamomis https://www.itu.int/rec/T-REC G.8110.1/en), kur duomenų perduodamas būtų paremtas žiedine topologija kiekviename taške, naudojant po vieną tinkle išskirtą IP adresų bloką (angl. subnet) kiekvienam taško sujungimui.
3. Jungiantis prie VMS duomenų perdavimo tinklo turi būti užtikrinta, kad būtų įdiegta ir naudojama nemažiau kaip 2FA autentifikacija prisijungimams prie sistemos, t.y

jungiantis su 2FA turi būti naudojamas naudotojo vardas, slaptažodis ir laikinas kodas, kuris turi būti generuojamas mobiliajame telefone.

4.2. VMS techniniai ir programinės įrangos reikalavimai

Sistemos programinė įranga turi užtikrinti visišką suderinamumą su šiomis operacinėmis sistemomis ir duomenų bazių valdymo varikliais:

1. Aplikacijų serverio (MAS) aplinka: Privalomas suderinamumas su Microsoft Windows Server 2022/2025 (64-bit) korporatyvine versija.
2. Duomenų bazės palaikymas: VMS privalo naudoti pramoninę duomenų bazę Microsoft SQL Server 2022/2025 Express/Standard arba Enterprise (64-bit). Duomenų bazė naudojama išskirtinai sisteminei konfigūracijai, naudotojų teisėms, laiko žymoms, aliarmo įvykiams ir AI analitikos metaduomenims saugoti.
3. Kliento programinė įranga (Unified Client): Dedikuota centralizuota valdymo programa, veikianti Windows 11 (64-bit) aplinkoje. Ji privalo palaikyti hibridinę vaizdo ir prieigos kontrolės įvykių unifikaciją (angl. *Unified Management*) bei aparatinį vaizdo dekodavimą naudojant operatoriaus darbo vietos GPU resursus.
4. Nuotolinis stebėjimas (Web & Mobile): VMS privalo turėti vidinę, saugią (HTTPS) žiniatinklio sąsają (*Web Client*) sistemos administravimui ir sveikatos stebėjimui (*Enterprise Health Monitoring*).
5. Mastelio galimybės (Scalability): Licencinė sistema neturi riboti įrašymo įrenginių (angl. *recorders*) skaičiaus plėtros. Centrinis aplikacijų serveris privalo gebėti apdoroti iki 300 nepriklausomų įrašymo mazgų (SAS) vienoje sistemoje, o aliarmų aktyvumas turi siekti ne mažiau kaip 64 įvykius per sekundę.

4.2.1. Centralizuotos duomenų bazės „Microsoft SQL Server“ licencijavimo modelio pagrindimas

Sistemoje bus naudojama Microsoft SQL Server Standard versija, kuri yra visiškai pakankama 330 kamerų sistemos konfigūracijai ir įvykių žurnalams saugoti. Šiam projektui specifikacijose įtvirtinamas „Per Core“ (Branduolių) licencijavimo modelis (4 branduolių paketas). Šis pasirinkimas yra pagrįstas ne ekstremalaus našumo poreikiu, o šiomis teisinėmis-licencinėmis bei NIS2 atitikties sąlygomis:

- Griežta „Microsoft“ tankinimo (angl. *Multiplexing*) taisyklė: Pagal oficialias „Microsoft“ licencijavimo gaires, jei naudojamas alternatyvus „Server + CAL“ modelis, Užsakovas privalo pirkti prieigos licenciją (CAL) kiekvienam įrenginiui ar naudotojui, kuris tiesiogiai arba netiesiogiai siunčia ar gauna duomenis iš SQL serverio. Kadangi prie VMS (ir netiesiogiai prie SQL konfigūracijos) nuolat jungiasi 2 pagrindiniai įrašymo serveriai, 1 rezervinis serveris, 2 operatorių darbo vietos, o svarbiausia – išorinės LKPB, IRD ir „Regitros“ API sąsajos, „Server + CAL“ modelis teisiškai reikalautų pirkti šimtus CAL

licencijų visiems šių institucijų galiniams įrenginiams. „Per Core“ modelis šį teisinį apribojimą visiškai panaikina – naudotojų ir įrenginių skaičius tampa neribotas.

- NIS2 audito žurnalo ir aliarmo įvykių indeksavimas: Nors pats vaizdo srautas rašomas tiesiai į pramoninį RAID 5 arba RAID6 masyvą (ne į SQL), visi dirbtinio intelekto analitikos metaduomenys (valstybiniai numeriai, automobilių markės, žmonių atributai) ir NIS2 reikalaujamas nekeičiamas naudotojų audito žurnalo įrašas įkeliamas į SQL duomenų bazės lenteles. 4 branduolių „SQL Standard“ licencija yra optimali, kad užtikrintų stabilų šių tekstinių įvykių indeksavimą realiame laike, nesukeliant sistemos strigimų piko valandomis, kai transporto ANPR kameros vienu metu fiksuoja šimtus tranzitų respublikiniuose keliuose.
- Aukšto prieinamumo ir rezervavimo palaikymas: Pasirinkus licencijavimą pagal branduolius ir turint aktyvų programinės įrangos palaikymą (*Software Assurance*), Užsakovas įgyja teisę nemokamai paleisti pasyvųjį SQL serverį rezervavimo tikslais (*Passive Failover Instance*), kas leidžia pilnai užtikrinti centrinio aplikacijų serverio (MAS) dubliavimą be papildomų DBVS licencijų pirkimo.

4.3. Serverių struktūra ir našumo skaičiavimai (330 kamerų kiekiui)

Siekiant užtikrinti techninėse specifikacijose numatytą 100% *on-premise* modelį, nepertraukiamą 24/7 įrašymą ir 30 dienų trukmę, serverių infrastruktūra skirstoma į tris dedikuotus segmentus.

4.3.1. Centrinis aplikacijų ir duomenų bazės serveris (MAS)

Šis serveris vykdo visos sistemos logikos, naudotojų autentifikavimo, audito žurnalų ir integracijų valdymą. Jis tiesioginio vaizdo srauto neįrašinėja, todėl jo konfigūracija orientuota į greitą SQL užklausų apdorojimą.

- Procesorius (CPU): Ne mažiau kaip 1x Intel Xeon E-2236 (6 branduoliai, 12 gijų, 3.4 GHz) arba naujesnės kartos Intel Xeon Silver / AMD EPYC.
- Operatyvioji atmintis (RAM): Ne mažiau kaip 32 GB ECC DDR4/DDR5 RAM.
- Sisteminė saugykla (OS & DB): 2x 400 GB Enterprise SAS (15 000 RPM) arba pramoniniai NVMe SSD, sukonfigūruoti RAID 1 (Mirror) režimu, užtikrinant operacinės sistemos ir SQL duomenų bazės greitaveiką bei izoliaciją nuo pagrindinio vaizdo archyvo.

4.3.2. Įrašymo serverių segmentas (SAS / Video Edge Recorders)

Atsižvelgiant į tai, kad bendras 330 pramoninių kamerų srautas su visomis tinklo protokolo viršsąnaudomis ir saugumo rezervu sudaro 3,64 Gbps nuolatinį projektinį pralaidumą, šis krūvis paskirstomas per du (2) identiškus didelio našumo įrašymo serverius, bei vieną (1) rezervinį serverį (N+1).

- Kamerų paskirstymas: Kiekvienam aktyviam serveriui tenka apie 165 kameras (srautus) (~0.82 Gbps grynojo vaizdo srauto per serverį). Vaizdo srautai siunčiami tiesiai į serverių diskų posistemę, o ne į duomenų bazę, t.y. serverio našumas nemažiau kaip 1Gbps.

- Procesorius (CPU) vienam serveriui: 2x Intel Xeon Silver arba AMD EPYC (iš viso ne mažiau 12 branduolių viename serveryje), skirti masiniam srautų priėmimui ir AI metaduomenų indeksavimui.
- Operatyvioji atmintis (RAM): Ne mažiau kaip 32 GB ECC RAM viename serveryje.
- Tinklo sąsaja: Kiekvienas įrašymo serveris privalo turėti nemažiau kaip 2x 1 Gbps ir 2x 2,5 Gbps tinklo plokštes, sujungtas LACP režimu (angl. *Link Aggregation*), užtikrinant pralaidumo rezervą ir tinklo linijų dubliavimą priimant srautus iš šviesolaidinių bei uždarų GSM LTE (CPE įrenginių) tinklų.

4.3.3. Diskų posistemės architektūros modeliavimas ir programiškai valdomos saugyklos (SDS) pagrindimas

Siekdamas užtikrinti stabilų ir nepertraukiamą 330 pramoninių kamerų generuojamo galimo maksimalaus 3,64 Gbps projektinio piko pralaidumo priėmimą realiame laike, Užsakovas priima klasikinę aparatinės RAID (įskaitant RAID 5 arba RAID6) architektūrą, kai failai supjaustomi į mažus blokus ir paskirstomi per visus masyvo diskus. Toks sprendimas sistemai leidžia skaityti duomenis iš kelių diskų vienu metu ir veikti greitai.

1. Vaizdo srautų suspaudimo nustatymai ir dinaminis srauto valdymas

Vaizdo srautų pralaidumo skaičiavimui taikomas išmanusis kintamo bitų srauto (angl. *Variable Bitrate* – VBR) režimas su griežtai apribota maksimalia riba (*Cap VBR*). Pastovaus bitų srauto CBR (angl. *Constant Bitrate*) režimas atmetamas kaip ekonomiškai neefektyvus, nes kai scenoje judėjimo nėra, jis eikvotų disko vietą statinėse naktinėse scenose.

Siekiant užtikrinti maksimalų H.265 kodeko efektyvumą, techninėje specifikacijoje įtvirtinami šie gamykliniai kamerų nustatymai:

- GOP (*Group of Pictures*) struktūra: vertinama didesnė GOP = 50 (prie 25 fps tai reiškia, kad pilnas kadras (*I-frame*) siunčiamas kas 2 sekundes, o tarp jų siunčiami tik pakitimų metaduomenys (*P-frames*)). Tai sumažina statinių scenų svorį iki 40%.
- Išmanusis srauto valdymas: Aktyvuojami gamykliniai dinaminiai VMS algoritmai (dinaminis GOP kintamumas ir triukšmų filtravimas), kurie realiu laiku reaguoja į scenos pokyčius, optimizuodami disko vietą.

Kadangi 330 kamerų tinklas apima skirtingo intensyvumo lokacijas, saugyklos poreikis modeliuojamas per tris inžinerinius scenarijus (Optimistinis: 8MP = 3,5 Mbps / 32MP = 15 Mbps; Nominalus: 8MP = 5,5 Mbps / 32MP = 24 Mbps; Blogiausio atvejo: 8MP = 8,0 Mbps / 32MP = 32 Mbps).

Lentelė Nr. 4.1: Dinaminio saugyklos poreikio modeliavimo suvestinė

Kameros tipas ir kiekybinė apimtis	Optimistinis srautas (Mbps)	Nominalus srautas (Mbps)	Blogiausio atvejo srautas (Mbps)

8MP kameros (295 vnt.)	3,5 Mbps	5,5 Mbps	8,0 Mbps
32MP kameros (35 vnt.)	15,0 Mbps	24,0 Mbps	32,0 Mbps
Suminis grynojo vaizdo srautas	1 552,50 Mbps	2 462,50 Mbps	3 480,00 Mbps
Paros archyvo talpa (Grynoji)	16,77 TB / parą	26,60 TB / parą	37,58 TB / parą
30 dienų archyvo poreikis (Naudingas)	503,01 TB	797,85 TB	1 127,52 TB
30 dienų archyvo poreikis (Naudingas), naudojant išmaniąją vaizdo kodavimo ir suspaudimo technologiją	251,55 TB	398,93 TB	563,76 TB

Naudojant išmaniąją vaizdo kodavimo ir suspaudimo technologiją. Ji realiuoju laiku analizuoja stebėjimo kameros vaizdą ir vidutiniškai 50% ar daugiau sumažina tinklo pralaidumo (bandwidth) bei disko vietos poreikį, visiškai neprarasdama svarbių detalių – tokiu atveju 30 dienų poreikiui reikalingą talpos vieta būtų 1,2TB per kameros srautą, kas bendroje apimtyje sudarytų ~396TB

2. Fizinės talpos suvedimas

Norint nominaliame scenarijuje 30 dienų poreikiui reikalingą bendrąjį naudingąjį talpą (~400 TB) paversti fizine įranga, naudojamos išorinės pramoninės diskų lentynos, užpildytos 20 TB nominalo Enterprise diskais. Sistemos patikimumas ir apsauga nuo duomenų praradimo suvaldoma hibridiniu būdu:

- Erasure Coding (N+M) lygmuo: VMS programinė įranga paskirsto vaizdo duomenų blokus ir klaidų taisymo pariteto metaduomenis tolygiai per visus diskus (taikant pramoninę *Software-Defined Storage* 20+4 arba analogišką schemą). Tai visiškai panaikina vieno disko perkrovos riziką, nes rašymo ir skaitymo IOPS apkrova pasiskirsto po visą masyvą, užtikrindama stabilų 0,82 Gbps piko srauto užrašymą be kadrų praradimo.
- Fizinis diskų skaičius: Vienam serveriui tenkančiam plotui padengti nominaliame scenarijuje būtų naudojama 12 diskų. Įvertinus klaidų taisymo kodavimo (*Erasure Coding*) rezervą (atitinkantį 1 disko talpą) bei 1 aktyvų „Hot-Spare“ diską, viename serveryje montuojami 12 fiziniai diskai po 20 TB. Bendra sistemos fizinė naudinga talpa išlieka optimali – ~400 TB.
- Aplikacinis redundantiškumas (Apsaugos skydas): Sugedus didesniam diskų skaičiui nei numato klaidų taisymo kodas, prarandama tik maža dalis archyvo segmentų konkrečiame diske, o bendras sistemos veikimas nesustoja. Visišką veiklos tęstinumą užtikrina aktyvus „RAID5 arba RAI6“rezervas. Strateginės vaizdo kameros (pvz., kelių ANPR) VMS lygiu turi galimybę atlikti dubliuotą įrašymą (*Dual Recording*) į abu nepriklausomus SAS serverius vienu metu.

- Sistemos elgsena Blogiausio atvejo scenarijuje: Jei ekstremalios sąlygos (pūga/triukšmas) tęstųsi visas 30 dienų nepertraukiamai, talpos poreikis galimai išaugtų iki 600 TB. Sukonfigūruotas bendras 400 TB grynos naudingos talpos masyvas (20 diskų × 20 TB) iš dviejų serverių užtikrintų, kad piko metu saugomas archyvas automatiškai laikinai sutrumpėtų iki 23,95 dienos (~24 dienų). Tai yra visiškai priimtina pramoninė rizika, kadangi ekstremalūs aplinkos triukšmai gamtoje niekada netrunka 30 parų iš eilės.

4.3.4. Technologinių alternatyvų analizė ir ekonominis diskų masyvo parinkimo pagrindimas

Siekiant užtikrinti maksimalų Vilniaus rajono savivaldybės biudžeto lėšų panaudojimo efektyvumą ir neperžengti preliminariame biudžete numatytų investicijų ribų, buvo atlikta vaizdo archyvo saugojimo technologinių alternatyvų analizė. Kadangi vaizdo stebėjimo sistemoms LR teisės aktai bei NIS2 direktyva draudžia toleruoti masinį duomenų praradimą (kas eliminuoja absoliučiai pigiausią, tačiau jokios gedimų tolerancijos neturintį RAID 0 modelį), žemiau pateikiamas ekonominis ir inžinerinis pramoninių diskų masyvų modelių palyginimas

Ekonominis saugyklų efektyvumo palyginimo lentelė

Architektūros lygis	Talpos efektyvumas	Pariteto / nuostolio diskai	Finansinis vertinimas ir kaštų įtaka projektui	Tinkamumas Vilniaus r. projektui / Inžinerinė išvada
Klasikinis RAID 5	~95% (Aukštas)	1 disko gedimas	Geriausias kainos ir talpos santykis. Reikalauja pirkti papildomus pariteto diskus, bendrą sistemos fizinės talpos poreikį išpučiant iki 400 TB.	Pasirinktas modelis. Užtikrina maksimalią greitaveiką programiniu lygmeniu (SDS). Dviejų diskų gedimo tolerancija aparatiniame lygmenyje o bendra fizinė talpa išlaikoma ties optimalia 400 TB riba.
Klasikinis RAID 6	~92% (Vidutinis)	2 diskų gedimas	Pabrangina sistemą. Reikalauja pirkti papildomus pariteto diskus, bendrą sistemos fizinės talpos poreikį išpučiant iki 400 TB.	Svarstytinas kaip ekonomiškai mažiau efektyvus. Dviejų diskų gedimo tolerancija aparatiniame lygmenyje o bendra fizinė talpa išlaikoma ties optimalia 400 TB riba.

Klasikinis RAID 10	50% (Labai žemas)	Pusė visų diskų talpos	Kritiškai brangus. Reikalauja 100% duomenų dubliavimo (veidrodinio atspindžio), todėl projekto kaina diskų saugyklai padidėtų mažiausiai 70 000 – 80 000 EUR.	Atmestas. Neproporcingas lėšų švaistymas, nesukuriantis papildomos pridėtinės vertės vaizdo srautų įrašymui.
Klasikinis RAID 2	Netaikoma	7 diskai per serverį	Finansiškai ir techniškai neįmanomas. Komerciškai neegzistuojantis modelis. Reikalautų nestandartinių valdiklių gamybos, o įrangos kaina išaugtų >70 000 EUR.	Atmestas. Techniškai nesuderinamas su vaizdo stebėjimo srautais, o jo įtraukimas sužlugdytų viešojo pirkimo konkursą.

4.4. Techninės specifikacijos reikalavimai serverių ir saugyklos infrastruktūrai

Lentelė Nr. 7: Techninės specifikacijos punktai serveriams ir saugyklai

Punkto Nr.	Reikalavimo pavadinimas	Detalus techninis reikalavimas (Pirkimo specifikacija)
REQ-SRV-01	Serverių architektūros modelis	Tiekėjas privalo pateikti paskirstytos architektūros sprendimą (atitinkantį *Master/Satellite* modelį), kurį sudaro vienas centralizuotas aplikacijų ir duomenų bazės serveris (MAS) ir ne mažiau kaip du (2) aktyvūs vaizdo įrašymo serveriai (SAS). Jokie vaizdo įrašymo srautai negali būti rašomi tiesiogiai į centralizuotą duomenų bazės serverį.
REQ-SRV-02	Aukštas prieinamumas (N+1 rezrvas)	Infrastruktūroje privalo būti numatytas bent vienas (1) papildomas fizinis rezervinis įrašymo serveris. Sugedus bet kuriam iš dviejų aktyvių įrašymo serverių, rezervinis serveris perimtų neveiksnaus serverio kamerų srautų arba ateityje būtų naudojamas kaip trečias aktyvus serveris.
REQ-SRV-03	Tinklo pralaidumas ir hibridinis srautų priėmimas	Kiekvienas įrašymo serveris privalo turėti ne mažiau kaip dvi (2) integruotas 2,5 Gbps (SFP+) optinio tinklo sąsajas. Šios sąsajos privalo būti sukonfigūruotos aktyvaus agregavimo režimu (LACP / *Link Aggregation*), užtikrinant ne mažesnį kaip 5 Gbps suminį

		pralaidumą vienam serveriui bei fizinių linijų dubliavimą. Tinklo posistemė privalo būti pritaikyta sinchroniškam hibridinių srautų priėmimui tiek iš seniūnijų šviesolaidinių linijų, tiek iš uždaro LTE tinklo išorinių lauko įrenginių (CPE), integruotų bendrame vaizdo VLAN segmente.
REQ-SRV-04	Diskų posistemės architektūra	Vaizdo įrašų saugojimui privalo būti naudojamos pramoninės diskai Enterprise klasės. Vaizdo srautų rašymas ir klaidų taisymo valdymas privalo būti vykdomas programiniu lygmeniu (*Software-Defined Storage*), tolygiai paskirstant pariteto duomenis per visus disko elementus (*Erasure Coding* mechanizmu), visiškai eliminuojant vieno disko našumo apribojimus. Suminė fizinė naudinga talpa turi būti ne mažesnė kaip 400 TB. Centralizuotos duomenų bazės SQL failai privalo būti fiziškai izoliuoti nuo vaizdo saugyklos ir talpinami atskirame NVMe/SSD RAID 1 (*Mirror*) diske. Vaizdo įrašų srautai saugomi atskirame pramoniniame RAID5 arba RAID6 diskų masyve.
REQ-SRV-05	Automatinis disko keitimas (Hot-Spare)	Kiekviename iš dviejų aktyvių įrašymo serverių, be duomenų ir pariteto diskų, privalo būti įdiegtas ir sukonfigūruotas bent vienas „Hot-Spare“ (aktyvaus rezervo) diskas. Sugedus bet kuriam duomenų diskui, masyvas privalo akimirksniu pradėti automatinį duomenų atstatymą (*rebuild*) į „Hot-Spare“ diską, nesiunčiant jokių fizinių užklausų administratoriui.
REQ-SRV-06	Fizinis talpos rezervas (Erasure Coding optimizavimas)	Bendra visos sistemos pateikiama fizinė diskų talpa (įskaitant pariteto ir atsarginius diskus) turi būti ne mažesnė kaip 480 TB, kuri būtų sudaryta iš pramoninių 20 TB talpos diskų. Ši talpa privalo garantuoti, kad visi 330 kamerų vaizdo srautai (su bendru projektiniu naudingumu ~1,48 Gbps) bus nepertraukiamai saugomi ne trumpiau kaip 30 dienų maksimalia gamykline raiška (nemažiau kaip 15 kadrų per sekundę sparta, H.264 arba H.265 kompresija), kaip numatyta inžineriniame scenarijuje.
REQ-SRV-07	Aparatinis srautų priėmimas	Įrašymo serverių aparatinė dalis (valdikliai ir procesoriai) privalo būti suprojektuoti taip, kad užtikrintų stabilų ir nepertraukiamą duomenų įrašymą į diskų lentynas, kai bendras sistemos įeinantis vaizdo srautas piko metu pasiekia 4 Gbps (įvertinus TCP/IP viršsąnaudas ir 20% inžinerinį rezervą ir galimus pikus).

		Duomenų praradimas dėl procesoriaus ar disko posistemio perkrovos (*frame dropping*) yra nepriimtinas.
REQ-SRV-08	Nuotolinis valdymas ir monitoringas	Visi tiekiami serveriai privalo turėti prievadą gamykliškai numatytą jungti prie tinklo ir būtų naudojamas nuotoliniam įrenginio valdymui
REQ-SRV-09	Maitinimo dubliavimas	Visi serveriai ir išorinės diskų lentynos privalo įrenginyje turėti ne mažiau kaip du (2) karštojo keitimo (*Hot-Swap*) maitinimo šaltinius, veikiančius 50/50 krūvio dalijimosi režimu.

4.6. INTEGRACIJOS SU IŠORINĖMIS INSTITUCIJOMIS

4.6.1. Integracinės sąsajos ir technologinis pasirengimas duomenų mainams

Vilniaus rajono savivaldybės vaizdo stebėjimo sistema projektuojama kaip atvira, korporatyvinio lygio platforma, kurioje numatytas technologinis pasirengimas ir galimybė ateityje vykdyti duomenų mainus su išorinėmis valstybinėmis institucijomis bei operatyvinėmis tarnybomis: Lietuvos kelių policijos biuru (LKPB), Informatikos ir ryšių departamentu (IRD) bei valstybės įmone „Regitra“, jei tokia prieiga ir duomenų perdavimo teisė Užsakovui bus suteikta teisės aktų nustatyta tvarka.

Siekiant, kad potencialūs duomenų mainai neapkrautų centrinio aplikacijų serverio (MAS) ir nesutrikdytų 330 kamerų nuolatinio 2,148 Gbps vaizdo srauto įrašymo į RAID 5 arba RAID6 masyvą, sistemoje projektuojamas asinchroninio duomenų eksporto per saugų integracinį šliuzą modelis:

1. Duomenų mainų izoliavimas per saugų šliuzą: Programinėje ir aparatinėje įrangoje turi būti suprojektuota galimybė duomenų mainus vykdyti per dedikuotą šliuzą, esantį izoliuotoje tinklo zonoje (angl. *Demilitarized Zone – DMZ*). VMS sistema privalo gebėti generuoti ir siųsti transporto priemonių valstybinių numerių (ANPR) bei objektų metaduomenis (markę, modelį, spalvą) į šį šliuzą, užtikrindama saugų išorinių užklausų priėmimą ir izoliavimą nuo vidinės duomenų bazės.
2. Technologinis pasirengimas integracijai su Kelių policijos sistemomis: VMS programinė įranga privalo turėti techninį suderinamumą ir funkcinį pasirengimą eksportuoti užfiksuotų transporto tranzitų metaduomenis (valstybinio numerio nuotraukas, laiko žymas, lokacijas) į Kelių policijos centralizuotas informacines sistemas. Šis funkcionalumas, gavus atitinkamus Policijos leidimus ir technines sąsajas (API), turi leisti suderinti automatinį perspėjimų (angl. *alerts*) generavimą, jei užfiksuotas numeris sutampa su lokaliai į VMS įkeltu ieškomų transporto priemonių sąrašu.
3. Galimybė integruotis su valstybės registrais (VĮ „Regitra“): VMS ANPR modulyje turi būti numatyta techninė galimybė integruotis su valstybės registrais transporto priemonių duomenų tikrinimui, jei tokia prieiga ir duomenų teikimo sutartys bus suteiktos bei

pasirašytos teisės aktų nustatyta tvarka. Šis pasirengimas numato galimybę kamerų sugeneruotus transporto priemonių markės, modelio ir spalvos atributus kryžmiškai lyginti su registro duomenimis, siekiant nustatyti galimus numerių klastojimo atvejus, kai tai leidžia išorinio registro API prieinamumas.

4. Suderinamumas su duomenų eksporto standartais: Sistema privalo palaikyti standartizuotus XML/JSON formatų duomenų išrašus, skirtus galimam incidentų ir audito žurnalų medžiagos perdavimui teisėsaugos institucijoms pagal teisinius BDAR reikalavimus.

Lentelė Nr. 8: Techniniai ir funkciniai reikalavimai integracinėms sąsajoms

Reikalavimo ID	Integracijos komponentas	Minimalūs techniniai reikalavimai (Pirkimo specifikacija)
REQ-INT-01	Protokolai ir šifravimas	Visi suprojektuoti integraciniai API mainai su išorinėmis sistemomis privalo būti vykdomi tik per saugų HTTPS protokolą, naudojant TLS 1.2 šifravimą, visiškai apsaugant perduodamus duomenis nuo perėmimo ar modifikavimo.
REQ-INT-02	Duomenų formatai ir pralaidumas	Integracinis šliuzas privalo gamykliškai palaikyti standartizuotus REST API protokolus (JSON / XML) duomenų formatus ir užtikrinti technologinį pasirengimą apdoroti iki nemažiau kaip 100 užklausų per sekundę (RPS), garantuojant stabilų darbą piko valandomis eismo srauto metu respublikinių kelių ANPR taškuose.
REQ-INT-03	Duomenų buferizavimas ir lokalus saugojimas	Integracinis šliuzas privalo turėti funkciją automatiškai kaupti ir buferizuoti tranzitų metaduomenis bei nuotraukas vidinėje sistemos saugykloje, užtikrinant duomenų stabilumą ir pasirengimą vėlesniam asinchroniniam jų perdavimui, jei išorinės priimančios sistemos ar ryšio kanalai taptų laikinai nepasiekiami.

4.7. TEISINIS IR SAUGUMO ATITIKTIES ĮVERTINIMAS (BDAR IR NIS2)

4.7.1. Bendrojo duomenų apsaugos reglamento (BDAR) reikalavimų įgyvendinimas

Vilniaus rajono savivaldybės vaizdo stebėjimo sistemos plėtra iki 330 pramoninių kamerų apimties tiesiogiai susijusi su masiniu asmens duomenų (vaizdo įrašų, biometrinių bruožų, transporto priemonių valstybinių numerių) rinkimu ir apdorojimu. Siekiant užtikrinti visišką atitiktį ES Reglamentui 2016/679 (BDAR), pirkimo techninėse specifikacijose įtvirtinami šie privalomi inžineriniai saugikliai:

- Duomenų minimizavimas ir privatumo maskavimas: VMS platforma privalo užtikrinti teisinį balansą tarp asmens duomenų apsaugos (BDAR) ir nusikalstamumo prevencijos tikslų. Dinaminis veidų ir numerių maskavimas privalo būti vykdomas programiškai, vaizdo atvaizdavimo (peržiūros) metu kliento stotelėje, o ne pirminiame įrašymo sraute. Tai garantuoja, kad įrašų saugykloje (RAID 5 arba RAID 6 masyve) esantys duomenys išlaiko pradinę teisinę įrodomąją vertę. Eksportuojant vaizdo medžiagą trečiosioms šalims (pvz., piliečių prašymu), VMS privalo gamykliškai leisti atlikti permanentinį vaizdo suliejimą (angl. *hard export blur*), negrįžtamai paslepiant visų pašalinių asmenų veidus ir automobilių numerius, kurie nepatenka į incidento apimtį, taip pilnai patenkinant Valstybinės duomenų apsaugos inspekcijos gaires.
- Asmens duomenų šifravimas judėjime ir ramybėje: Perduodant asmens duomenis iš nutolusių taškų (vaikų žaidimų aikštelių, respublikinių kelių zonų), privaloma naudoti saugius šifravimo protokolus RTSPS / TLS 1.2, veikiančius mobiliojo ryšio operatoriaus izoliuotame uždarame VPN tinkle (Private APN). SQL duomenų bazėje saugomi asmenų metaduomenys ir tranzitų nuotraukos privalo būti šifruojami pačiuose NVMe/SSD diskuose naudojant SED (Self-Encrypting Drive) AES-256 bitų aparatinę technologiją.
- Griežtas duomenų saugojimo terminas (30 dienų): Sistema privalo užtikrinti automatinį ir nekeičiamą duomenų naikinimo ciklą. Pasibaigus LR teisės aktuose numatytam 30 dienų terminui, vaizdo įrašai ir su jais susiję metaduomenys turi būti negrįžtamai ištrinami naudojant FIFO (angl. *first-in, first-out*) algoritmą.

4.7.2. NIS2 Direktyvos ir LR Kibernetinio saugumo įstatymo atitiktis

Kaip regioninės svarbos viešojo administravimo institucija, Vilniaus rajono savivaldybė patenka į subjektų, kuriems taikomi sugriežtinti Europos Sąjungos NIS2 direktyvos ir Lietuvos Respublikos kibernetinio saugumo įstatymo reikalavimai, sąrašą. Vaizdo stebėjimo infrastruktūra yra klasifikuojama kaip ypatingos svarbos sistemos elementas, todėl Tiekėjas privalo realizuoti šiuos saugumo mechanizmus:

- Nekeičiamas naudotojų audito žurnalas (Tamper-proof Audit Trail): Vadovaujantis NIS2 kibernetinio saugumo reikalavimais, sistema privalo registruoti visus naudotojų veiksmus (prisijungimą, atsijungimą, vaizdo peržiūrą, archyvo eksportą, kameros nustatymų keitimą) į dedikuotą SQL audito žurnalą. Šis žurnalas privalo būti apsaugotas nuo modifikavimo (angl. *Tamper-proof*). Net ir administratoriaus teises turintis naudotojas neturi turėti techninės galimybės ištrinti ar koreguoti audito įrašų per VMS vartotojo sąsają. Tiekėjas privalo realizuoti šiuos saugumo mechanizmus integruodamas sistemą su centralizuota katalogų tarnyba.
- Vaidmenimis grįsta prieigos kontrolė (RBAC) ir AD integracija: Prieiga prie vaizdo valdymo sistemos ir jos infrastruktūros privalo būti autorizuojama tik per saugų LDAP (Active Directory over TLS) protokolą, susiejant operatorių paskyras su savivaldybės darbuotojų

tapatybėmis. Prisijungimui prie administravimo sąsajų privaloma užtikrinti dviejų faktorių autentifikavimą (2FA).

- Asmeninė vadovų atsakomybė ir rizikų valdymas: Įgyvendinant NIS2 reikalavimus, techninėje specifikacijoje suformuoti atmetimo kriterijai (pvz., draudimas tiekti įrangą iš riziką keliančių šalių, atitiktis NDAA standartams, privalomas TPM 2.0 modulių buvimas serveriuose). Tai apsaugo savivaldybės administraciją ir VMS valdymo vadovus nuo teisinės bei finansinės atsakomybės (baudų iki 7 mln. EUR), numatytos už aplaidumą ir nepakankamų kibernetinio saugumo priemonių įdiegimą ypatingos svarbos tinkle.

Lentelė Nr. 9: Teisinės ir saugumo atitikties techniniai reikalavimai

Punkto Nr.	Saugumo komponentas	Detalus techninis reikalavimas (Pirkimo specifikacija)
SEC-SRV-01	BDAR atitiktis: Archyvo maskavimas peržiūros metu	Dinaminis veidų ir numerių maskavimas privalo veikti kaip peržiūros lygio filtras (*Dynamic Client Masking*), nepažeidžiantis originalaus įrašo pradinės būsenos diske. VMS konfigūracijoje turi būti numatyta galimybė sukurti dvigubos autorizacijos taisyklę (angl. *Dual Authorization / Four-Eyes Principle*), reikalaujančią dviejų skirtingų pareigūnų patvirtinimo (antrinio tapatybės autorizavimo), norint laikinai atidengti (demaskuoti) originalius asmens bruožus archyvo analizės metu.
SEC-SRV-02	NIS2 atitiktis: Audito vientisumas	Audito žurnalo įrašai privalo būti saugomi SQL duomenų bazėje dedikuotuose NVMe/SSD diskuose (RAID 1), visiškai atskiriant juos nuo vaizdo įrašų masyvo (RAID 5 arba RAID 6). Bet koks bandymas fiziškai koreguoti SQL audito lenteles rankiniu būdu privalo automatiškai generuoti kritinį aliarmo pranešimą IT skyriaus stebėjimo sistemose.
SEC-SRV-03	Tiekimo grandinės saugumas (NDAA)	Visi serveriniai komponentai, maršrutizatoriai, išoriniai 5G įrenginiai (CPE) bei visos 330 IP kamerų privalo būti pagamintos šalyse, kurios nėra priskiriamos prie riziką keliančių valstybių pagal LR Nacionaliniam saugumui užtikrinti svarbių objektų apsaugos įstatymą. Tiekėjas privalo pateikti oficialias gamintojų atitikties deklaracijas.
SEC-SRV-04	Srautų šifravimas judėjime hibridiniame tinkle	Visi duomenų srautai tarp centrinio aplikacijų serverio (MAS), įrašymo serverių (SAS) ir operatorių darbo vietų privalo būti šifruojami naudojant TLS 1.2 protokolus. Perduodant vaizdą iš nutolusių taškų privalo būti naudojamas saugus RTSP (RTSP over TLS) arba lygiavertis protokolas. Taškuose, kur naudojamas

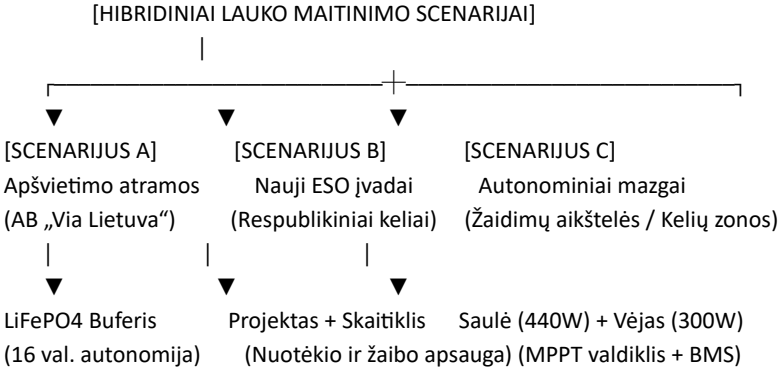
		uždaras GSM LTE tinklas su išoriniais lauko įrenginais (CPE), mobiliojo ryšio tiekėjo srautas papildomai privalo būti visiškai izoliuotas dedikuotame APN/VPN kanale, ir veikiantis kaip uždaras L3 MPLS APN/ VPN tinklas be išėjimo į viešąjį internetą. Prisijungimas prie sistemos iš išorės turi būti vykdomas per ugniasienę ir jungiantis per 2FA
SEC-SRV-05	Identiteto valdymas ir centralizuotas RBAC	VMS platforma privalo palaikyti integraciją su Užsakovo centralizuota katalogų tarnyba per saugų LDAP (Active Directory over TLS) protokolą. Teisių valdymas privalo būti pagrįstas vaidmenimis (angl. *Role-Based Access Control - RBAC*). Administratoriaus ir operatorių prisijungimui prie VMS klientų sąsajų ar Web portalų privalo būti užtikrinta galimybė aktyvuoti autentifikavimą (2FA), naudojant standartinius laiko algoritmus (TOTP).
SEC-SRV-06	Nekeičiamas audito žurnalas (Audit Trail & Tamper Resistance)	Vadovaujantis NIS2 kibernetinio saugumo reikalavimais, sistema privalo registruoti visus naudotojų veiksmus (prisijungimas, atsijungimas, vaizdo peržiūra, archyvo eksportas, kameros nustatymų keitimas) į dedikuotą SQL audito žurnalą. Šis žurnalas privalo būti apsaugotas nuo modifikavimo (angl. *Tamper-proof*). Net ir administratoriaus teises turintis naudotojas neturi turėti techninės galimybės ištrinti ar koreguoti audito įrašų per VMS vartotojo sąsają.
SEC-SRV-07	Saugus nuotolinis valdymas (KVM/IPMI Sauga)	Nuotolinio valdymo valdikliai privalo veikti visiškai izoliuotame valdymo tinkle. Privaloma pakeisti visus gamyklinius slaptažodžius pagal Užsakovo slaptažodžių politiką (min. 14 simbolių, naudojant didžiąsias/mažąsias raides, skaičius ir specialiuosius ženklus). Valdiklių žiniatinklio sąsajos privalo priimti prisijungimus tik per HTTPS su galiojančiais vidinio savivaldybės sertifikavimo centro (CA) išduotais sertifikatais.
SEC-SRV-08	Kibernetinio saugumo audito sertifikavimas	Tiekėjas privalo pateikti kvalifikacinius įrodymus, kad siūloma vaizdo valdymo programinė įranga (VMS) ir serverinė įranga bus suprojektuota laikantis tarptautinių kibernetinio saugumo standartų ir Tiekėjas turi galiojantį ISO/IEC 27001 arba lygiavertį sertifikatą. Tiekiami serveriai privalo būti pagaminti šalyje, kuri nėra priskiriama prie riziką keliančių valstybių pagal LR

		Nacionaliniam saugumui užtikrinti svarbių objektų apsaugos įstatymą (atitiktis NDAA nuostatoms).

4.8. ENERGETINĖS INFRASTRUKTŪROS INŽINERINIAI SPRENDINIAI IR ALTERNATYVOS

4.8.1. Hibridinių lauko maitinimo mazgų architektūra ir inžinerinis pagrindimas

Siekdamas užtikrinti nepertraukiamą 330 pramoninių kamerų bei išorinių 5G ryšio įrenginių (CPE) veikimą 24/7/365 režimu, Tiekėjas privalo įgyvendinti hibridinius maitinimo sprendinius, pritaikytus specifinėms geografinėms sąlygoms. Visi lauko maitinimo komponentai privalo būti integruoti į hermetiškas, antivandalines lauko komutacines spinteles, montuojamas ant kamerų atramų.



1. Scenarijus A: Akumuliatoriniai buferiniai blokai apšvietimo tinkluose (~120 taškų)
   - Inžinerinis sprendinys: Taškuose, kur įranga montuojama ant savivaldybės arba AB „Via Lietuva“ valdomų gatvių apšvietimo atramų, lauko spintoje privaloma įdiegti pramoninį buferinį UPS maitinimo šaltinį su didelės talpos LiFePO4 (Ličio geležies fosfato) baterijų moduliu.
   - Veikimo technologija: Tamsiu paros metu, kai apšvietimo linija yra aktyvi (tiekiama 230VAC įtampa), maitinimo blokas užtikrina nuolatinį kamerų ir ryšio įrangos veikimą bei vienu metu atlieka priverstinį greitąjį baterijų įkrovimą. Šviesiu paros metu, kai apšvietimo linija išjungiama, valdiklis be įtampos pertrūkio (0 ms perjungimo laikas) pereina prie maitinimo iš akumuliatorių. Baterijų talpa privalo garantuoti ne mažiau kaip 19 valandų autonominį sistemos veikimą esant maksimaliai apkrovai ir -20 °C išorinei temperatūrai. Užsakovas prisiima atsakomybę už leidimų suderinimą su AB „Via Lietuva“.
2. Scenarijus B: Fizinis prisijungimas prie skirstomųjų tinklų (~40 taškų)
   - Inžinerinis sprendinys: Strateginiuose kelių mazguose ir didelėse kryžminėse sankryžose respublikinių kelių apsaugos zonoje, projektuojamas naujas fizinis prijungimas prie skirstomųjų tinklų operatoriaus (ESO) žemos įtampos linijų.

- Vykdymo tvarka: Tiekėjas privalo savo lėšomis parengti supaprastintus elektros projektus, suderinti trasų schemas kelių apsaugos zonose, įrengti lauko apskaitos-paskirstymo spintas (jeigu reikalauja ESO) ir atlikti reikiamus darbus Visos spintos privalo turėti integruotą apsaugą nuo viršįtampių bei nuotėkio reles, apsaugančias įrangą nuo žaibo iškrovų kelio juostoje.

3. Scenarijus C: Autonominiai hibridiniai atsinaujinančios energijos mazgai (~60 mazgų)
    - Inžinerinis sprendinys: Visiškai energetiškai izoliuotuose respublikinių kelių taškuose (kur kabelių klojimas kelio juostoje teisiškai draudžiamas) bei seniūnijų vaikų žaidimų ir sporto aikštelėse (kur nėra arti esančių elektros įvadų) projektuojamos visiškai autonominės gamybos stotys ant dedikuotų stiebų.
    - Hibridinė generacija: Elektros energijos gamybai privaloma naudoti kombinuotą saulės ir vėjo energijos modelį. Komplektą sudaro monokristalinis saulės modulis (min. 440W) ir pramoninis mikro vėjo generatorius (min. 300W). Kadangi Lietuvoje lapkričio–vasario mėnesiais saulės insoliacija nukrenta iki kritinės ribos, vėjo generatorius yra privalomas inžinerinis komponentas, beveik užtikrinantis nuolatinį 24/7 vaizdo perdavimą ištisus metus.

Lentelė Nr. 10: Energetinės infrastruktūros ir lauko mazgų techninė specifikacija

Reikalavimo ID	Komponentas	Detalūs techniniai ir funkciniai reikalavimai (Pirkimo specifikacija)
REQ-PWR-01	Pramoninė LiFePO4 buferinė sistema (Scenarijus A)	Lauko sąlygoms pritaikytas UPS valdiklis su integruotu LiFePO4 baterijų moduliu. Nominali talpa ne mažesnė kaip 100Ah prie 24VDC įtampos. Gamykliškai integruota Baterijų valdymo sistema (BMS), užtikrinanti apsaugą nuo giliojo iškrovimo, perkrovimo ir trumpojo jungimo. Darbinės temperatūros intervalas nuo -20 °C iki +50 °C. Minimalus gyvavimo ciklas – 2000 ciklų išlaikant ne mažiau kaip 80% pirminės talpos.
REQ-PWR-02	Lauko apskaitos-paskirstymo spintos (Scenarijus B)	Antivandalinė pastatoma arba montuojama lauko spinta, apsaugos klasė ne žemesnė kaip IP65, mechaninio atsparumo klasė min. IK10. Įrengta sertifikuota vieta skirstomųjų tinklų operatoriaus skaitikliui. Komplekte privaloma pramoninė B+C (I+II) klasės viršįtampių apsauga (SPD), suderinta su ne mažesne kaip 6kV žaibo iškrovos apsauga, bei automatiniai jungikliai (MCB) ir nuotėkio relė (RCD).

REQ-PWR-03	Autonominis saulės ir vėjo hibridinis komplektas (Scenarijus C)	Saulės modulis: Monokristalinis, galia min. 440W, naudingumo koeficientas min. 21%, atsparumas krušai min. IK08. Vėjo generatorius: Horizontalios arba vertikalios ašies, nominali galia min. 300W prie 11 m/s, startinis vėjo greitis ne didesnis kaip 2,0 m/s (pritaikyta silpniems regiono vėjams). Valdiklis: Išmanusis MPPT valdiklis su integruota RS485/SNMP sąsaja, skirta baterijos įkrovos lygio (SoC) perdavimui į VMS sveikatos monitoringo modulį.
REQ-PWR-04	Lauko mazgo mikroklimato ir saugumo kontrolė (Visiems scenarijams)	Kiekviena lauko komutacinė spintelė privalo turėti integruotą automatinį termostatą, valdomą kaitinimo elementą (≥ 50W) ir priverstinės ventiliacijos filtrų sistemą, arba spintoje gali būti montuojamas LiFePO4 baterija, turinti integruotą kaitinimo elementą Spintoje privalo būti įdiegtas fizinio atidarymo magnetinis jutiklis (tamper switch), kuris laidiniu būdu jungiamas prie kameros aliarmo įėjimo, pavojaus signalą akimirksniu perduodant į centrinį VMS aliarmo žurnalą.

4.9. SISTEMOS APTARNAVIMAS IR SLA (SERVICE LEVEL AGREEMENT) REIKALAVIMAI

4.9.1. Garantinės priežiūros ir techninio aptarnavimo bendrosios nuostatos

Siekdamas užtikrinti nepertraukiamą 330 pramoninių IP kamerų, uždarojo duomenų perdavimo tinklo ir centrinio serverių mazgo veikimą 24/7/365 režimu, pirkimo laimėtojas (toliau – Paslaugų teikėjas) įsipareigoja teikti autorizuotas garantinės priežiūros ir techninio aptarnavimo paslaugas pagal pasirašytą SLA (*Service Level Agreement*) paslaugų lygio sutartį.

Atsižvelgiant į tai, kad savivaldybės vaizdo stebėjimo sistema apdoroja ypatingos svarbos viešojo saugumo duomenis bei integruojasi su valstybiniais registrais, techninės priežiūros reglamentas skirstomas į dvi esmines kategorijas:

1. Proaktyvi prevencinė priežiūra: Pusmetiniai sisteminiai tirkinimai, skirti programiškai įrašų saugyklų (diskų) fizinės būklės stebėjimui, mikroklimato (šildymo/vėdinimo) elementų patikrai lauko spintose prieš žiemos ir vasaros sezonus bei optinių stiklų valymui seniūnijose.
2. Reaktyvus incidentų šalinimas: Neatidėliotinas techninio personalo reagavimas ir fizinis vykimas į incidento vietą (įskaitant geografiškai nutolusius taškus, vaikų žaidimų aikšteles

bei AB „Via Lietuva“ atramas valstybinės reikšmės kelių apsaugos zonose), sugedusių komponentų keitimas ir ryšio parametrų atkūrimas.

4.9.2. Incidentų klasifikacija ir reakcijos bei sutaisymo laiko reglamentas

Visi vaizdo stebėjimo sistemos infrastruktūros sutrikimai yra griežtai klasifikuojami pagal jų įtaką savivaldybės viešosios tvarkos užtikrinimui ir duomenų praradimui. Paslaugų teikėjas privalo užtikrinti garantuotą reakcijos laiką (angl. *Response Time*) ir vidutinį gedimo pašalinimo laiką (angl. *Resolution Time / MTTR*) pagal šią matricą:

Lentelė Nr. 11: SLA incidentų valdymo ir terminų matrica

Incidento lygis	Gedimo aprašymas ir sisteminis poveikis	Reakcijos laikas (max.)	Gedimo pašalinimo laikas (max.)	Delspinigiai ir sankcijos už vėlavimą
Kritinis (Lygis 1)	Centrinės infrastruktūros arba kritinių taškų gedimas: - Centrinio aplikacijų serverio (MAS) ar SQL duomenų bazės nepasiekiamumas. - Suminio vaizdo įrašymo nutraukimas SAS serveriuose. - Daugiau nei 10 kamerų arba viso uždaro tinklo MPLS APN/VPN ryšio dingimas vienu metu. - Daugiau nei 5 vnt. transporto numerių atpažinimo (ANPR) taško gedimas.	1 valanda (24/7/365)	8 darbo valandos	100,00 EUR už kiekvieną pavėluotą valandą.
Didelis (Lygis 2)	Lokalių stebėjimo taškų sutrikimai: - Nuo 1 iki 10 vaizdo stebėjimo kamerų neveiksnumas seniūnijose arba vaikų žaidimų aikštelėse. - Vienos operatoriaus darbo vietos VRSA patalpose aparatinis gedimas.	2 valandos (Darbo laiku)	24 darbo valandos	50,00 EUR už kiekvieną pavėluotą valandą.
Mažas (Lygis 3)	Nekritiniai funkciniai sutrikimai: - Pavienių kamerų stikliuko užterštumas (aprasojimas, užnešimas purvu). Lauko spintelės mikroklimato (termostato/šildytuvo) gedimas	8 valandos (Darbo laiku)	48 darbo valandos	20,00 EUR už kiekvieną pavėluotą darbo dieną.

	žemos temperatūros metu. - VMS naudotojo sąsajos neesminių nustatymų korekcijos. - Nuotolinio monitoringo (SNMP) valdiklių metaduomenų vėlavimas.			

4.9.3. Privalomi operaciniai SLA reikalavimai Tiekėjui

- Privalomas įrangos pakaitinis fondas: Paslaugų teikėjas privalo savo lėšomis Vilniaus rajone įrengti ir palaikyti fizinį įrangos pakaitinį fondą (angl. *Spare Parts Depot*). Šiame fonde nuolat privalo būti nemažiau kaip po 2 vnt. nuo lauko kamerų (kiekvieno iš Tipų A, B, C, D, E), po 2 vnt. pramoninių lauko komutatorių, išorinių 5G įrenginių (CPE) bei pramoninių 20 TB Enterprise diskų. Jei gedimo neįmanoma pašalinti vietoje per numatytą terminą, Paslaugų teikėjas privalo per protingą laiką sumontuoti identišką pakaitinę įrangą iš fondo, o sugedusį elementą išsiųsti gamintojo remontui, Užsakovui nepatiriant jokių papildomų kaštų.
- Specializuota incidentų registravimo sistema (Helpdesk): Paslaugų teikėjas privalo suteikti VRSA IT naudotojo prieigą prie elektroninės incidentų registravimo ir sekimo platformos (*Helpdesk / Service Desk*), veikiančios 24/7/365 režimu. Kiekvienas incidentas sistemoje fiksuojamas su automatine laiko žyma, o skaičiavimas pradedamas nuo bilieto (angl. *ticket*) užregistravimo akimirkos.
- Darbo valstybinės reikšmės kelių zonose specifika: Kadangi 94 kamerų taškai (įskaitant 26 ANPR taškus) yra išsidėstę AB „Via Lietuva“ valdomų kelių apsaugos zonose, Tiekėjas privalės užtikrinti, kad jo techninės priežiūros komandos turės galiojančius leidimus aukštybiniams darbams kelių juostose, automobilinius bokštelius su specialiais žymėjimais bei atitinkamą personalo atestavimą, kad SLA terminai (8 valandų MTTR Kritiniams gedimams) nebūtų pažeisti dėl leidimų derinimo terminų incidento dieną.

4.10. PROJEKTO ĮGYVENDINIMO ETAPAI (GANTT GRAFIKAS)

4.10.1. Projekto vykdymo laiko juostos struktūra

Atsižvengiant į Vilniaus rajono savivaldybės vaizdo stebėjimo sistemos plėtros apimtį (330 kamerų lauko mazgų įrengimas) bei hibridinės infrastruktūros specifiką, bendras projekto realizavimo laikotarpis yra preliminaria planuojamas 24 mėnesių (2 metų) trukmės nuo viešojo pirkimo sutarties pasirašymo dienos, darbus skirstant į žingsius (etapus).

Lentelė Nr. 12. Projekto įgyvendinimo etapų grafikas (Gantt)

Etapo ID ir darbų aprašymas	Y1 Q1	Y1 Q2	Y1 Q3	Y1 Q4	Y2 Q1	Y2 Q2	Y2 Q3	Y2 Q4

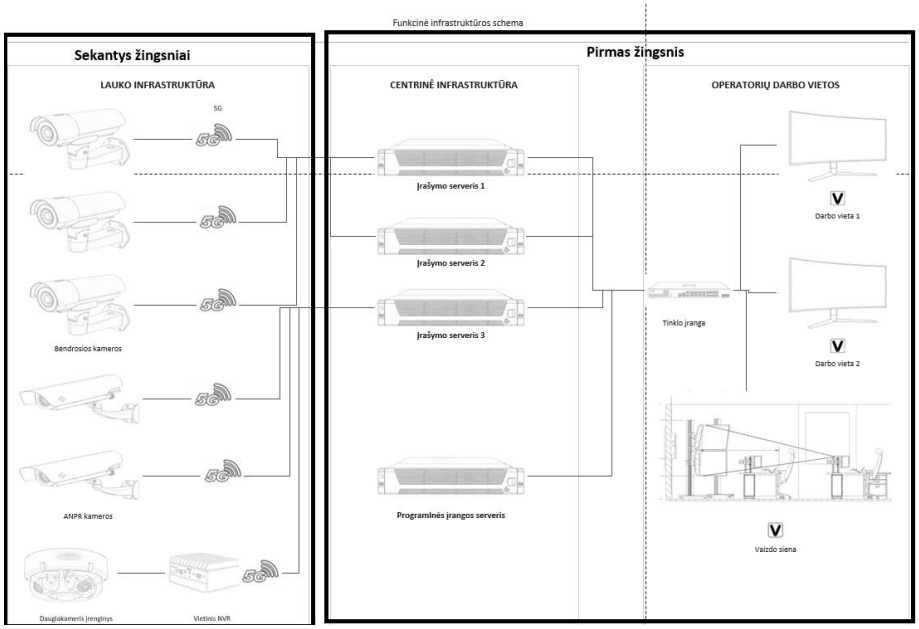
ETP-01: Centrinio mazgo ir VMS DB diegimas - Serverių (MAS/SAS) montavimas - SQL Server Standard diegimas ir kietinimas - Operatorių darbo vietų VRSA įrengimas	[X]	[X]						
ETP-02: Ryšio infrastruktūros paruošimas - Uždaro privataus MPLS APN/VPN tinklo sukonfigūravimas - L3 VPN/MPLS centrinės prieigos pajungimas į šviesolaidį - LAN IP adresacijos plano ir VMS VLAN sudarymas	[X]	[X]						
ETP-03: Projektavimas ir derinimai - Sąlygų gavimas ir projektai su AB „Via Lietuva“ - Supaprastinti ESO el. projektai kelių zonose, aki turimos prisijungimo sąlygos - Žemės darbų ir atramų statybos leidimai	[X]	[X]	[X]	[X]				
ETP-04: Esamos būklės integracija (110 kam.) - Buitinių ir pasenusių įrenginių keitimas - Esamų srautų perjungimas į centralizuotą VMS		[X]	[X]	[X]				
ETP-05: Fizinis naujų mazgų įrengimas - Kamerų montavimas ant atramų ir aikštelėse - LiFePO4 buferinių maitinimo dėžučių montavimas - Hibridinių saulės/vėjo autonominių stiebų statyba			[X]	[X]	[X]	[X]	[X]	
ETP-06: API integracijos ir SAT testavimas - Integracija su policijos (LKPB), Regitros API - 4 Gbps tinklo streso testai - Personalo apmokymai ir sistemos pridavimas							[X]	[X]

5. RINKOS TYRIMAS, ALTERNATYVŲ ANALIZĖ IR REALIŲ KAŠTŲ BIUDŽETAS

5.1. Lietuvos savivaldybių vaizdo stebėjimo pirkimų praktikos ir metodinių įkainių analizė Finansinis 330 vaizdo stebėjimo taškų plėtros biudžeto pagrindimas Vilniaus rajono savivaldybėje yra formuojamas remiantis realiais pramoninės įrangos įsigijimo normatyvais, elektros tinklų projektavimo įkainiais bei įvertinant kainų indeksavimą (rizikos rezervą) dėl numatomo pirkimo vykdymo po 6 mėnesių.

Lietuvos savivaldybių patirtis rodo, kad didžiausios biudžeto paklaidos atsiranda neteisingai įvertinus el. įvadų atvedimo (ESO) ir suderinimų kelių apsaugos zonose kaštus.
Žemiau pateikiami perskaičiuoti faktiniai rinkos normatyvai, galiojantys šių dienų pirkimuose.

Lentelė Nr. 13: Viešųjų pirkimų rinkos kainodaros realių įkainių matrica (su infliacijos rezervu)
Funkcinė schema



1 ŽINGSNIS 2026/2027 metai -

Vaizdo įrašymo įranga (Serverinė), operatoriaus darbo vietas, Programinė įranga, esamų kamerų vietų centralizavimas, duomenų perdavimas, priežiūra ir diegimo dabai

Vaizdo įrašymo įranga

Nr	***Aprašymas***	**Matas**	**Kiekis**	***Kaina eur be PVM/vnt.***	***Viso Kaina eur be PVM***
1.	*APP server*	Vnt.	*1*	14416,00	*14416,00*
2.	*REC server (*archyvas ir metaduomenys)*	Vnt.	*1*	52818,00	*52818,00*
3.	*REC server (*archyvas ir metaduomenys)*	Vnt.	*1*	52818,00	*52818,00*
4.	*REC server (*archyvas ir metaduomenys)*	Vnt.	*1*	52818,00	*52818,00*
5.	*Serveriams*	Vnt.	*1*	5308,00	*5308,00*
6.	*KDV*	Vnt.	*1*	6440,45	*6440,45*
7.	*55" Large Screen Monitors video wall*	Vnt.	*2*	2273,19	*4546,38*
					189164,83

Vaizdo programinė įranga

Nr	Aprašymas	Matas	Kiekis	Kaina eur be PVM/vnt.	Viso Kaina eur be PVM
1.	VMS licencija kamerai (apjungiant seniūnijos kameras, esamose lokacijose)	Vnt.	110	242,00	48400,00
2.	VM programinė įranga	Vnt.	1	9509,88	9509,88
3.	VMS&Management programinė įranga	Vnt.	1	4840,19	4840,19
					62750,07

Diegimo darbai

Nr	Aprašymas	Matas	Kiekis	Kaina eur be PVM/vnt.	Viso Kaina eur be PVM
1.	Sistemos, serverių paruošimo darbai	Vnt.	1	7200,00	7200,00
2.	Apjungiant seniūnijos kameras, esamose lokacijose ir užkeičiant naujomis	Vnt.	110	800,00	88 000,00
					95 200

Kameros

Nr	Aprašymas	Matas	Kiekis	Kaina eur be PVM/vnt.	Viso Kaina eur be PVM
1.	Naujos 8 MP Bullet kameros	Vnt.	99	1799,00	178101,00
2.	Naujos 32 MP Panoraminės kameros	Vnt.	11	5472,00	60192,00
3	Instaliacinės medžiagos, ir 24VAC maitinimo blokai kameroms	Vnt.	110	100,00	11000,00
					249 293,00

Abonentiniai - paslaugos

Nr	Aprašymas	Terminas	Kiekis	Kaina eur be PVM/mėn/. vnt.	Viso kaina eur be PVM/mėn	Viso Kaina eur be PVM
1.	Duomenų perdavimas MPLS APN/VPN 5G	60 mėn.	61	50,00	3 050,00	183 000,00
2.	Priežiūra	60 mėn.	110	30,00	3 300,00	198 000,00
						381 000,00

Bendra suma per 5 metus 977 407,83 ***eur be PVM***

2 ŽINGSNIS 2027/2028 metai -

Naujų kamerų ANPR policijai naujose vietoje ir dalies (pvz. šiukšlių konteineriai) seniūnijų, jungimas į centralizuotą sistemą, duomenų perdavimas, priežiūra ir diegimo dabai

Vaizdo programinė įranga

Nr	***Aprašymas***	**Matas**	**Kiekis**	***Kaina eur be PVM/vnt.***	***Viso Kaina eur be PVM***
1.	*VMS licencija naujoms kameroms (apjungiant ANPR kameras, esamose lokacijose)*	Vnt.	*26*	242,00	*6 292,00*
2.	*ANPR licencija*	Vnt.	*26*	*1200,00*	31 200,00
3.	*Naujų VMS licencija naujoms kameroms*	Vnt.	*50*	242,00	12 100,00
					49 592,00

Diegimo darbai

Nr	***Aprašymas***	**Matas**	**Kiekis**	***Kaina eur be PVM/vnt.***	***Viso Kaina eur be PVM***
1.	*Sistemos, serverių paruošimo darbai*	Vnt.	*76*	150,00	11 400,00
2.	*Apjungiant naujas ANPR ir vaizdo kameras, naujose lokacijose*	Vnt.	*76*	800,00	60 800,00
					72 200

Naujos kameros

Nr	***Aprašymas***	**Matas**	**Kiekis**	***Kaina eur be PVM/vnt.***	***Viso Kaina eur be PVM***
1.	*Naujos 8 MP Bullet kameros*	Vnt.	*50*	*1799,00*	*89 950,00*
2.	*Naujos ANPR kameros*	Vnt.	*26*	*6384,00*	*60 192,00*
3.	*Akumuliatorius 100Ah su įkrovėju, pašildymu, apsauga, monitoringu ir su pilnai paruostu komutaciniu skydu 500x400x250*	Vnt.	*102*	*1730,00*	*176 460,00*

4.	*Instaliacinės medžiagos, ir 24VAC maitinimo blokai kameroms*	Vnt.	*102*	*100,00*	*10 200,00*
					336 802,00

Abonentiniai - paslaugos

Nr	***Aprašymas***	**Terminas**	**Kiekis**	***Kaina eur be PVM/mėn/. vnt.***	***Viso kaina eur be PVM/mėn***	***Viso Kaina eur be PVM***
1.	*Duomenų perdavimas MPLS APN/VPN 5G*	48 mėn.	*102*	*50,00*	*5 100,00*	*244 800,00*
2.	*Priežiūra*	48 mėn.	*102*	*30,00*	*3 060,00*	*146 880,00*
						391 680,00

Bendra suma per 4 metus 850 274,00 ***eur be PVM***

3 ŽINGSNIS 2028/2029 metai -

Naujų PTZ kamerų policijai naujose vietoje ir dalies (pvz. šiukšlių konteineriai, vaikų žaidimo aikštelės, kapinės) seniūnijų, jungimas į centralizuotą sistemą, duomenų perdavimas, priežiūra ir diegimo dabai

Vaizdo programinė įranga

Nr	***Aprašymas***	**Matas**	**Kiekis**	***Kaina eur be PVM/vnt.***	***Viso Kaina eur be PVM***
1.	*VMS licencija naujoms kameroms (apjungiant PTZ kameras, esamose lokacijose)*	Vnt.	*55*	242,00	*13 310,00*
2.	*Naujų VMS licencija naujoms kameroms*	Vnt.	*60*	242,00	14 520,00
					27 830,00

Diegimo darbai

Nr	***Aprašymas***	**Matas**	**Kiekis**	***Kaina eur be PVM/vnt.***	***Viso Kaina eur be PVM***
1.	*Sistemos, serverių paruošimo darbai*	Vnt.	*115*	150,00	17 250,00
2.	*Apjungiant naujas PTZ ir vaizdo kameras, naujose lokacijose*	Vnt.	*115*	800,00	92 000,00
					109 250,00

Naujos kameros

Nr	Aprašymas	Matas	Kiekis	Kaina eur be PVM/vnt.	Viso Kaina eur be PVM
1.	Naujos 8 MP Bullet kameros	Vnt.	60	1799,00	107 940,00
2.	Naujos PTZ kameros	Vnt.	55	2847,00	156 585,00
3.	Akumuliatorius 100Ah su įkrovėju, pašildymu, apsauga, monitoringu ir su pilnai paruostu komutaciniu skydu 500x400x250	Vnt.	115	1730,00	198 950,00
4.	Instaliacinės medžiagos, ir 24VAC maitinimo blokai kameroms	Vnt.	115	100,00	11 500,00
					474 975,00

Abonentiniai - paslaugos

Nr	Aprašymas	Terminas	Kiekis	Kaina eur be PVM/mėn/. vnt.	Viso kaina eur be PVM/mėn	Viso Kaina eur be PVM
1.	Duomenų perdavimas MPLS APN/VPN 5G	36 mėn.	115	50,00	5 750,00	207 000,00
2.	Priežiūra	36 mėn.	115	30,00	3 450,00	124 200,00
						331 200,00

Bendra suma per 4 metus 943 255,00 ***eur be PVM***

4 ŽINGSNIS 2029/2030 metai -

Naujų Bullet kamerų policijai naujose vietoje ir likusios dalies (pvz. šiukšlių konteineriai, vaikų žaidimo aikštelės, kapinės) seniūnijų, jungimas į centralizuotą sistemą, duomenų perdavimas, priežiūra ir diegimo dabai

Vaizdo programinė įranga

Nr	Aprašymas	Matas	Kiekis	Kaina eur be PVM/vnt.	Viso Kaina eur be PVM
1.	VMS licencija naujoms kameroms (apjungiant Bullet kameras, esamose lokacijose)	Vnt.	13	242,00	3 146,00
2.	Naujų VMS licencija naujoms kameroms	Vnt.	65	242,00	15 730,00
					18 876,00

Diegimo darbai

Nr	***Aprašymas***	**Matas**	**Kiekis**	***Kaina eur be PVM/vnt.***	***Viso Kaina eur be PVM***
1.	*Sistemos, serverių paruošimo darbai*	Vnt.	*78*	150,00	11 700,00
2.	*Apjungiant naujas PTZ ir vaizdo kameras, naujose lokacijose*	Vnt.	*78*	800,00	62 400,00
					74 100,00

Naujos kameros

Nr	***Aprašymas***	**Matas**	**Kiekis**	***Kaina eur be PVM/vnt.***	***Viso Kaina eur be PVM***
1.	*Naujos 8 MP Bullet kameros (policijai)*	Vnt.	*13*	*1799,00*	*23 387,00*
2.	*Naujos PTZ kameros*	Vnt.	*65*	*1799,00*	*116 935,00*
3.	*Akumuliatorius 100Ah su įkrovėju, pašildymu, apsauga, monitoringu ir su pilnai paruostu komutaciniu skydu 500x400x250*	Vnt.	*78*	*1730,00*	*134 940,00*
4.	*Instaliacinės medžiagos, ir 24VAC maitinimo blokai kameroms*	Vnt.	*78*	*100,00*	*7 800,00*
					283 062,00

Abonentiniai - paslaugos

Nr	***Aprašymas***	**Terminas**	**Kiekis**	***Kaina eur be PVM/mėn/. vnt.***	***Viso kaina eur be PVM/mėn***	***Viso Kaina eur be PVM***
1.	*Duomenų perdavimas MPLS APN/VPN 5G*	24 mėn.	*53*	*50,00*	*5 750,00*	*63 600,00*
2.	*Priežiūra*	24 mėn.	*78*	*30,00*	*2 340,00*	*56 160,00*
						119 760,00

Bendra suma per 4 metus 495 798,00 ***eur be PVM***

Orientaciniai kainų dydžiai

Infrastruktūros komponentas	**Reali šių dienų rinkos kaina su PVM (€)**	**Kainodaros ir inžinerinis pagrindimas, įvertinant pusmečio kainų augimo riziką**
Pramoninis lauko stebėjimo taškas (8MP kamera ant esamos atramos)	**2 500,00 – 3 200,00** už vieną tašką	Pramoninė lauko kamera (8MP), hermetiška antivandalinė lauko spintelė su automatika, pramoninis L2 jungiklis, viršįtampių apsauga, montavimo ir aukštybinių darbų kaštai.
Specializuotas ANPR transporto kontrolės taškas	**9 500,00 – 13 000,00** už vieną tašką	Kameros su *Global Shutter* jutikliu, didelio galingumo impulsinis IR pašvietimas, techninis suderinamumas, sertifikuoti programinės įrangos moduliai.
ESO el. projektavimas ir inžineriniai suderinimai (Respublikinių kelių zonose – Scenarijus B)	**2 800,00 – 3 500,00** už vieną įvadą	**Tik fiksuoti kaštai.** Supaprastinto el. projekto parengimas, topografinės nuotraukos tikslinimas, suderinimas su kelių valdytoju (AB „Via Lietuva“) bei fiksuotas ESO prijungimo mokestis. Žemės kasimo ir kabeliavimo darbai neįtraukti. Užsakovas turi iš ESO išimti prisijungimo sąlygas
Autonominis hibridinis energetinis mazgas (Saulė + Vėjas – Scenarijus C)	**2 000,00 – 2 500,00** už vieną komplektą	Konstrukcinis stiebas ant pamato, 440W monokristalinis modulis, pramoninis 300W vėjo generatorius, išmanusis MPPT valdiklis, klimatizuotas LiFePO4 baterijų konteineris.
Serverių branduolys (SDS / RAID)	**160 000,00 – 190 000,00** bazinė investicija	Didelio našumo Dual-CPU SAS serveriai, MAS serveris, Windows licencijos pagal branduolius, pramoniniai UPS bei **400 TB** programiškai valdoma JBOD saugykla.

6.2. Vaizdo valdymo programinės įrangos (VMS) gamintojų palyginamoji analizė

Siekdamas užtikrinti viešųjų pirkimų technologinio neutralumo, skaidrumo ir tiekėjų konkurencijos principus, Užsakovas atliko trijų sprendimų VMS funkcinių galimybių palyginimą. Vertinimas atliktas pagal kritinius projekto kriterijus: suderinamumą su *On-Premise MAS/SAS* architektūra, programiškai valdomos saugyklos palaikymą, dinaminį privatumo maskavimą peržiūros lange ir dvigubos autorizacijos principą.

Lentelė Nr. 22: Pramoninių VMS platformų funkcinių parametrų palyginimas

Vertinimo kriterijus	**Gamintojas A**	**Gamintojas B**	**Gamintojas C**
MAS/SAS architektūra	**Pilnas gamyklinis palaikymas**. Atskirtas konfigūracijos valdymo serveris nuo nepriklausomų įrašymo mazgų.	**Pilnas gamyklinis palaikymas**. Naudojamas centralizuotas valdymo serveris ir paskirstyti įrašymo serveriai.	**Pilnas gamyklinis palaikymas**. Architektūra bazuojama ant centralizuoto direktorato ir paskirstytų serverių.
Programinė saugykla (SDS)	**Pilnas gamyklinis palaikymas**. Srautai rašomi tiesiai į diskų masyvus per vidinį srautinį failų variklį.	**Pilnas gamyklinis palaikymas**. Vidinis įrašymo variklis optimizuotas tiesioginiam nuosekliam rašymui.	**Pilnas gamyklinis palaikymas**. Naudojama integruota *Scale-Out* programiškai valdoma saugyklos architektūra.
Dynamic Client Masking	**Integruotas AI filtras**. Dinaminis veidų/numerių suliejimas atliekamas peržiūros lange, archyvas lieka originalus.	**Integruotas AI filtras**. Palaiko dinaminį privatumo maskavimą vartotojo sąsajoje realiu laiku ir archyve.	**Integruotas AI modulis**. Naudojamas integruotas *Privacy Protector* modulis dinamiškam privatumo užtikrinimui.
Dviguba autorizacija	**Gamyklinis *Four-Eyes* principas**. Reikalauja dviejų skirtingų pareigūnų slaptažodžių vaizdo laikinam atidengimui.	**Gamyklinis palaikymas**. Integruota *Dual Authorization* funkcija aliarmo ar vaizdo patvirtinimui.	**Gamyklinis palaikymas**. Sukonfigūruota *Supervisor Validation* darbo eiga privatumo teisių nuėmimui.

Finansinė pastaba pirkimo dokumentų rengimui (Apsauginė sąlyga):

Rekomenduojama konkurso sąlygose numatyti, kad Tiekėjas tiek „Microsoft SQL Server“, tiek VMS kamerų licencijas privalo perduoti Užsakovo nuosavybėn kaip amžinąsias licencijas (*Perpetual Licenses*), o ne kaip laikiną prenumeratą (*Subscription*). Tai užtikrins, kad pasibaigus 3 ar 4 metų sutarties laikotarpiui ir nustojus mokėti už programinės įrangos atnaujinimus

(*Software Assurance*), pati vaizdo stebėjimo sistema, duomenų bazė ir vaizdo įrašymas išliks visiškai veiksni ir funkcionuojanti be papildomų teisinių ar finansinių apribojimų, o savivaldybė patirs tik einamuosius ryšio ir SLA priežiūros kaštus

7.1. BAIGIAMOSIOS IŠVADOS IR REKOMENDACIJOS

7.1.1. Esminės inžinerinės ir teisinės išvados

- Paskirstyta VMS architektūra. *Master/Satellite* modelis užtikrintų stabilų 330 kamerų centralizuotą valdymą.
- Rezervinis vaizdo įrašymo serveris perimtų vaizdo įrašymą, esant didelei apkrovai, trūkstant vaizdo įrašams vietos arba įvykusiam įrašymo serverio gedimui.
- Ekonomiškiausia RAID 5 saugykla. Paritetui naudojami 2 dedikuoti diskai serveryje (200 TB naudinga talpa per įrašymo serverį).
- Privalomas „Hot-Spare“ rezervas. Gedimo atveju duomenų atstatymas prasideda automatiškai.
- Saugus branduolių licencijavimas duomenų bazei (*Per Core)* modelis apsaugo nuo *Microsoft Multiplexing* pažeidimų.
- Uždaras MPLS APN/VPN tinklas. Nutolusiuose taškuose srautas izoliuojamas dedikuotame APN/VPN kanale, naudojant neprastesnes 5G prieigas arba šviesolaidines prieigas.
- Išorinių įrenginių naudojimas. Lauko antenos CPE eliminuoja signalo slopinimo problemą.
- Griežta NIS2 atitiktis. Įtvirtinti atmetimo kriterijai: TLS 1.2 ir nekeičiamas audito žurnalas.

7.2.2. Rekomendacijos pirkimo sąlygų įgyvendinimui

- Derinimų su AB „Via Lietuva“ kontrolė Teikėjui, o leidimų gavimas Užsakovo atsakomybėje.
- Akumuliatorinių sprendinių diegimas. Apšvietimo linijose reikalauti min. 19 valandų veikiančių LiFePO4 baterijų.
- Kelių apsaugos zonų projektavimas. Supaprastintus el. projektus (Scenarijus B) patikėti rangovui.
- Autonominė saulės/vėjo generacija. Žaidimų aikštelėse taikyti hibridinį Scenarijų C, kai nėra kitų variantų.
- Visapusiškas streso testavimas. Prieš pridavimą atlikti pilną 4 Gbps tinklo apkrovos testą