

**VALSTYBĖS UŽSAKYMO
„MAŽOSIOS ORO GYNYBOS SISTEMOS (MOGS) IŠVYSTYMAS“
TECHNINĖ UŽDUOTIS**

I. BENDROJI DALIS

1. Valstybės užsakymu siekiama sukurti nacionalinį pajėgumą – mažosios oro gynybos sluoksnio sistemą (toliau – MOGS).

2. Valstybės užsakymu kuriamo produkto siekiamybė – Lietuvoje sukurta ir pagaminta MOGS, skirta papildyti esamą LK oro erdvės stebėjimo ir kontrolės sistemos (toliau – OESKS) kuriamą atpažintą oro paveikslą (toliau – AOP) ir formuoti vientisą objektų, skrendančių žemuose oro erdvės aukščiuose, aptikimą, apjungiant oro erdvės objektų aptikimo, identifikavimo ir sekimo duomenis visoje Lietuvos Respublikos teritorijoje ir oro erdvėje bei už Lietuvos Respublikos ribų tiek, kiek tokius duomenis teikia integruoti nacionaliniai, sąjungininkų ar kiti autorizuoti sensoriai ir duomenų šaltiniai, integruojant skirtingų tipų sensorių duomenis į vieningą ekosistemą; duomenis, su minimalia delsa, perduoti AOP kūrimui, pagerinti karinių vienetų ir kitų valstybinių institucijų bei LR gyventojų išankstinį perspėjimą apie grėsmes iš oro bei užtikrinti greitą ir efektyvų reagavimą bei grėsmės neutralizavimą.

3. Geografinė MOGS architektūra negali būti techniškai apribota Lietuvos Respublikos valstybės siena.

4. MOGS operacinis efektyvumas apibrėžiamas nuo sensoriaus duomenų gavimo iki patvirtintos atžymos, jos sekimo, identifikavimo / klasifikavimo ir grėsmės vertinimo, sprendimo perdavimo efektoriui ir jo inicijavimo. Siekiamas rezultatas, kad sistema užtikrina laike išmatuojamų galimų operacinių scenarijų įgyvendinimą pagal nustatytus operacinius kriterijus (laiką iki patvirtintos atžymos ir jos judėjimo trajektorijos sudarymo, prognozuojamos judėjimo trajektorijos sudarymą, trajektorijos atsinaujinimą laike bei sprendimo perdavimo efektoriams bei jų inicijavimo trukmę).

5. Šioje techninėje užduotyje nustatomi MOGS duomenų perdavimo ir duomenų apdorojimo platformoms keliami sukūrimo, išvystymo ir įdiegimo reikalavimai. Ši techninė užduotis apibrėžia MOGS vystymą, kurios technologinis branduolys turi užtikrinti skirtingų tipų sensorių integravimą, duomenų surinkimą, perdavimą, sinchronizavimą, koreliavimą ir suliejimą, oro erdvės objektų aptikimą, sekimą, identifikavimą / klasifikavimą, grėsmės vertinimą ir perdavimą OESKS, duomenų sanitavimą ir sprendimo perdavimą efektoriams bei jų inicijavimą.

6. Šioje techninėje užduotyje reikalavimai nekeliami apdorotų duomenų integravimo platformai, duomenų sanitavimo ir duomenų atvaizdavimo platformoms dėl realiai egzistuojančių techninių sprendinių / produktų. Apdorotų duomenų integravimo platforma yra LK naudojama techninė įranga vienpusiam duomenų perdavimui ir galima įsigyti pagal galiojančias technines specifikacijas. Duomenų sanitavimo platforma yra NATO praktikoje naudojamas Air Situation Data Exchange Gateway (NCIA paslauga Nr. APP052) yra sertifikuota bei naudojama NATO valstybių kaip patikimas būdas atpažinto oro paveikslo sanitavimui iki NEĮSLAPTINTA / NATO UNCLASSIFIED. Duomenų atvaizdavimo platforma privalo palaikyti standartizuotus duomenų mainų protokolus, užtikrinančius visapusišką sąveikumą ir duomenų eksportą į vadovavimo ir valdymo (toliau – V2) sistemas, įskaitant SitaWare, TAK (angl. „Tactical assault kit“), kartu išlaikant galimybę naudoti alternatyvias V2 sistemas. Taip pat

privaloma užtikrinti kryžminį suderinamumą (angl. cross-platform compatibility) ir korektišką duomenų vizualizavimą „Windows“, „Android“ ir „iOS“ operacinėse sistemose, naudojant stacionarius ir nešiojamuosius kompiuterius bei mobiliuosius galinius įrenginius, įskaitant išmaniuosius telefonus bei planšetinius kompiuterius“.

7. MOGS privalo gebėti veikti kaip savarankiška vadovavimo ir valdymo sistema NEIŠSLAPTINTOJE aplinkoje, užtikrinanti vientisą procesą nuo sensoriaus duomenų gavimo iki oro erdvės objekto aptikimo, patvirtintos atžymos sudarymo, sekimo, identifikavimo / klasifikavimo ir grėsmės vertinimo, integruoti efektorius ir įgyvendinti procesą nuo sensoriaus iki efektoriaus (angl. Sensor-to-Effector / Sensor-to-Shooter).

8. Dalyvis privalo įsipareigoti išvystyti, įdiegti duomenų perdavimo ir duomenų apdorojimo platformas bei visas 5 (duomenų perdavimo, duomenų apdorojimo, apdorotų duomenų integravimo, duomenų sanitavimo, duomenų atvaizdavimo) platformas integruoti į bendrą sistemą užtikrindamas jos vientisumą, sąveikumą ir tinkamą veikimą.

9. MOGS įteisinimo ir akreditavimo procesai yra Užsakovo atsakomybė.

10. MOGS turi būti skirta neįslaptintos informacijos, taip pat informacijos, kuri pažymėta NEIŠSLAPTINTA / NATO UNCLASSIFIED/LIMITE žymomis, apdorojimui ir saugojimui“.

II. TECHNINIAI PARAMETRAI

11. Bendrieji reikalavimai MOGS:

11.1. Atsparumas kibernetinėms grėsmėms: architektūriniu ir programiniu lygmeniu sistema turi būti pritaikyti Nulinio pasitikėjimo architektūros (angl. *Zero Trust Architecture*) ir Duomenimis grindžiama saugumo (angl. *Data centric security*) principai. Kiekviena užklausa, prieiga ar duomenų paketas turi būti autentifikuojami ir autorizuojami nepriklausomai nuo jų kilmės vietos tinklo;

11.2. Duomenų konfidencialumas (angl. *Confidentiality*): visi sensorių identifikuojantys duomenys ir sensorių duomenys turi būti šifruojami ne žemesnės kaip TLS 1.2 versijos protokolu, palaikant TLS 1.3 versiją, ir ne silpnesniu nei AES-256 klasės algoritmu;

11.3. Duomenų vientisumas ir tikrumas (angl. *Integrity*): visi duomenys patenkantys į sistemą turi būti apsaugoti nuo duomenų modifikavimo ir klastojimo, turi būti galimybė patikrinti visų duomenų paketų, perduodamų į platformą ir joje apdorojamų, tikrumą ir juos identifikuoti naudojant skaitmeninius parašus bei ne silpnesnę nei SHA-256 maišos (angl. Hash value) funkciją, o duomenų klasifikavimo metaduomenų rišimą ir vientisumą užtikrinant pagal STANAG 4774/4778;

11.4. Duomenų pasiekiamumas (angl. *Availability*): sistemos programinė ir techninė architektūra turi užtikrinti funkcionavimą (24/7/365 režimu) su pasiekiamumo rodikliu ne mažesniu kaip 99,9%. Dalyvis privalo įgyvendinti sistemos avarinio atkūrimo (angl. *Disaster Recovery*) sprendimą

11.5. Daugiapakopis autentifikavimas: prieiga prie visų sistemoje esančių duomenų turi būti apsaugota daugiapakopiu (ne mažiau 2 faktorių) autentifikavimu;

11.6. Duomenų perdavimo vėlavimas (angl. *Low Latency*) ir operacinis tempas (angl. *Operational Tempo*): duomenų perdavimas ir apdorojimas sistemos viduje ir tarp platformų užtikrinti objekto aptikimo – patvirtintos atžymos – sekimo – identifikavimo / klasifikavimo – grėsmės vertinimo – sprendimo priėmimo – šūvio atlikimo laiko langą, užtikrinant nuo sensoriaus iki efektoriaus procesą:

11.6.1. Duomenų pralaidumas intensyviomis sąlygomis: sistema privalo išlaikyti nustatytus vėlavimo rodiklius, kai vienu metu apdorojama, koreliuojama ir sprendimams priimti pateikiama ne mažiau kaip 1000 aktyvių objektų;

11.6.2. Sprendimo perdavimo efektoriams trukmė (Sensor-to-Shooter laikas): Architektūrinis pasirengimas sprendimo perdavimui efektoriams (angl. *Sensor-to-Shooter / Sensor-to-Effector*): turi būti

sukurti ir dokumentuoti standartizuoti integravimo principai bei sąsajos, leidžiančios prijungti efektorius nekeičiant pagrindinės sistemos architektūros. Integravus efektorius, bendra sistemos vėlavimo trukmė nuo patvirtintos atžymos sudarymo iki sprendimo priėmimo / naikinimo komandos perdavimo efektoriumi turi neviršyti 2 sekundžių;

11.6.3. Atžymos (trajektorijos) atsinaujinimo laikas: galutinio vartotojo sąsajoje (duomenų atvaizdavimo platformoje) atvaizduojamos objekto padėties senumas nuo duomenų gavimo iš sensoriaus momento neturi viršyti 2 sekundžių.

11.7. Duomenų perdavimo būdai: sistema turi palaikyti skirtingus duomenų perdavimo būdus (Ethernet, 4G/5G, palydovinis ryšys, taktinis radijo ryšys), automatiškai pasirinkti tinkamiausią perdavimo būdą pagal konfigūruojamą kriterijų rinkinį (pralaidumą, delsą ir ryšio patikimumą);

11.8. Įvykių (angl. *Log*) valdymas: sistema turi užtikrinti centralizuotą įvykių kaupimą, saugojimą ir analizę;

11.9. Platforma turi palaikyti atnaujinimų ir konfigūracijos pakeitimų diegimą be veiklos sustabdymo, naudojant nuolatinės integracijos ir nuolatinio diegimo principus.

11.10. MOGS turi palaikyti centralizuotai valdomą geografinį suskirstymą į operacinius rajonus. Užsakovo nustatytam centrinio valdymo subjektui turi būti sudaryta galimybė kurti, keisti ir panaikinti operacinius rajonus, nustatyti jų geografines ribas, priskirti jiems sensorius, naudotojus ir vadovavimo elementus bei konfigūruoti duomenų prieinamumo ir valdymo teises.

11.11. Centrinis sistemos valdymo lygmuo turi matyti bendrą visų operacinių rajonų oro situacijos vaizdą, o operacinio rajono vadovavimo elementui pagal suteiktas teises turi būti automatiškai perduodami jo rajonui aktualūs objektų, grėsmių ir sensorių duomenys.

11.12. Objektui judant tarp operacinių rajonų sistema turi užtikrinti nenutrūkstamą sekimą ir informacijos perdavimą tarp atitinkamų vadovavimo elementų, neprarandant objekto sisteminio identifikatoriaus, sekimo istorijos, klasifikacijos, grėsmės vertinimo ir kitų su objektu susijusių duomenų.

11.13. MOGS architektūroje turi būti numatytas standartizuotas efektorių integravimo sluoksnis (angl. Effector Adapter Layer / Effector Integration Layer), integruoti skirtingų tipų, skirtingų gamintojų ir skirtingo veikimo principo efektorius, įskaitant automatizuotai paleidžiamus bepiločius perėmėjus, nekeičiant pagrindinės sistemos architektūros ir duomenų modelio. MOGS architektūroje ir licencijavime neturi būti nustatyto fiksuoto maksimalaus integruojamų efektorių skaičiaus.

11.14. MOGS architektūroje turi būti numatytas centralizuotas efektorių registras, kuriame kiekvienam efektoriui suteikiamas unikalus identifikatorius ir pagal technines galimybes tvarkoma informacija apie efektoriaus tipą, geografinę padėtį, priklausomybę, parengties ir ryšio būseną, veikimo / efekto nuotolį, galimų neutralizuoti objektų kategorijas, naudojimo apribojimus, turimą pajėgumą ir priskyrimą operaciniam rajonui.

11.15. MOGS turi gebėti susieti aptiktą ir sekamą oro grėsmę su vienu ar keliais situacijoje prieinamais efektoriais ir pateikti autorizuotam operatoriui rekomenduojamą efektorių arba efektorių rinkinį, įvertinant objekto poziciją ir prognozuojamą trajektoriją, grėsmės lygį, objekto tipą, efektoriaus vietą, parengtį, veikimo zoną, techninį tinkamumą konkrečiam taikiniui, operacinio rajono ribas ir nustatytas valdymo teises.

11.16. MOGS turi palaikyti konfigūruojamus automatizavimo lygius: informacijos pateikimą operatoriui; automatinį objekto klasifikavimą ir rekomenduojamo veiksmo pateikimą; konkretaus efektoriaus rekomendavimą, kai veiksmas inicijuojamas operatoriaus patvirtinimu; ir, kai tai leidžia Užsakovo nustatytos autorizavimo taisyklės, automatizuotą autorizavimo efektoriaus inicijavimą. Visi sistemos ir operatorių sprendimai bei veiksmai turi būti registruojami ir audituojami.

12. Reikalavimai duomenų perdavimo platformai:

12.1. Platforma turi būti atviros architektūros (angl. Open Architecture) modulinė, plečiama ir diegiama valdomoje infrastruktūroje, išlaikant galimybę veikti be privalomos priklausomybės nuo viešojo interneto, išorinių debesijos valdymo ar programinės įrangos kaip paslaugos sprendimų;

12.2. Duomenų perdavimas turi būti vykdomas asinchroniniu publikavimo–prenumeravimo (angl. Publish/Subscribe) principu, leidžiančiu tą patį duomenų srautą perduoti keliems autorizuotiems gavėjams ir tęsti perdavimą po laikino ryšio sutrikimo bei mažo vėlavimo (angl. Low Latency) sąlygomis;

12.3. Platforma turi užtikrinti naudotojų, įrenginių ir paslaugų autentifikavimą, prieigos teisių valdymą, perduodamų ir saugomų duomenų šifravimą bei duomenų klasifikavimo metaduomenų naudojimą pagal STANAG 4774, STANAG 4778 ir ACP-240 reikalavimus arba jų aktualias redakcijas;

12.4. Platformos komponentai turi veikti aukšto prieinamumo režimu (angl. High Availability, HA), neturėti vieno gedimo taško (angl. Single Point of Failure). Sutrikus mazgui ar ryšio kanalui turi būti vykdomas automatinis persijungimas (angl. Failover);

12.5. Duomenų bazės komponentas:

12.5.1. Komponentas turi saugoti virtualaus tinklo konfigūraciją, tinklo objektus, prieigos taisykles, komponentų būsenos informaciją ir sertifikatų metaduomenis;

12.5.2. Duomenų bazė turi veikti ne mažiau kaip dviejuose mazguose, naudoti sinchroninį arba patvirtintų duomenų neprarandantį replikavimo mechanizmą ir automatinį persijungimą aktyviu / aktyviu (angl. Active/Active) arba aktyviu / pasyviu (angl. Active/Passive) režimu;

12.5.3. Duomenų bazės ryšiai ir laikmenoje saugomi duomenys turi būti šifruojami, o duomenys bei schema – eksportuojami dokumentuotu formatu.

12.6. Vidinės vardų sistemos (angl. Domain Name System, DNS) komponentas:

12.6.1. Komponentas turi aptarnauti platformos vidines vardų zonas ir užtikrinti sensorių, serverių, maršrutizatorių bei surinkimo punktų vardų išrišimą;

12.6.2. DNS paslauga turi veikti ne mažiau kaip dviejuose egzemplioriuose, palaikyti zonų replikavimą ir tęsti darbą be priklausomybės nuo viešųjų DNS paslaugų;

12.6.3. Zonų ir įrašų valdymui turi būti pateikta grafinė administravimo sąsaja ir dokumentuota taikomųjų programų sąsaja (angl. Application Programming Interface, API).

12.7. Saugaus virtualaus tinklo (angl. Virtual Private Network, VPN) komponentas:

12.7.1. Komponentas turi sujungti sensorius, platformos paslaugas ir duomenų surinkimo punktus į valdomą šifruotą virtualų tinklą;

12.7.2. Turi būti užtikrinamas šifravimas nuo galo iki galo (angl. End-to-End Encryption);

12.7.3. Komponentas turi centralizuotai valdyti įrenginių ir naudotojų registravimą, autentifikavimą bei prieigos taisykles ir turėti grafinę administravimo sąsają, API bei veiksmų auditą.

12.8. Sertifikatų centro (angl. Certification Authority, CA) komponentas:

12.8.1. Komponentas turi išduoti ir valdyti X.509 skaitmeninius sertifikatus platformos naudotojams, įrenginiams, paslaugoms ir duomenų perdavimo mazgams;

12.8.2. Turi būti palaikomas visas sertifikatų gyvavimo ciklas: išdavimas, atnaujinimas, sustabdymas, atšaukimas ir būsenos tikrinimas, naudojant sertifikatų atšaukimo sąrašus arba realaus laiko būsenos tikrinimą;

12.8.3. Sertifikatų centro privatūs raktai turi būti apsaugoti aparatiniaame saugos modulyje (angl. Hardware Security Module, HSM) arba lygiaverčiu būdu; turi būti palaikomas automatizuotas sertifikatų išdavimas, administratorių teisių atskyrimas ir veiksmų auditas.

12.9. Publikavimo–prenumeravimo duomenų perdavimo komponentas:

12.9.1. Komponentas turi paskirstyti būdu ir mažu vėlavimu perduoti duomenis vienam arba keliems prenumeratoriams, o duomenų siuntėjas neturi būti tiesiogiai priklausomas nuo konkretaus gavėjo;

12.9.2. Nutūkų ryšiui, duomenys turi būti laikinai kaupiami ir automatiškai perduodami ryšiui atsikūrus; turi būti galima valdyti duomenų srautų prioritetą, buferį, saugojimo terminą ir pakartotinį perdavimą;

12.10. Platforma turi naudoti sertifikatais pagrįstą abipusį autentifikavimą, turėti administravimo ir integravimo sąsajas, o visi platformos komponentai turi būti techniškai suderinami su Zenoh ir NetBird produktais.

12.11. Perdavimo platforma turi užtikrinti bendrą laiko bazę (laiko sinchronizavimą) daugiasensorei koreliacijai ir sąveiką su galiojančiais NATO standartais pagal integruojamų sensorių tipus bei sąjungininkų sąsajas;

12.12. Platforma turi turėti duomenų saugyklą, veikiančią pagal duomenų ežero (angl. Data Lake) principus, skirtą struktūrizuotų, pusiau struktūrizuotų ir nestruktūrizuotų duomenų kaupimui bei saugojimui;

12.13. Platforma turi palaikyti heterogeninių sensorių integravimą per standartizuotą sensorių adaptavimo sluoksnį (angl. Sensor Adapter Layer), užtikrinantį naujų sensorių prijungimą nekeičiant pagrindinės sistemos logikos. Sistemos architektūroje, duomenų modelyje ir programinės įrangos licencijavime neturi būti nustatyto fiksuoto maksimalaus integruojamų sensorių skaičiaus; sensorių skaičius turi būti plečiamas horizontaliai, didinant reikalingus skaičiavimo, duomenų perdavimo ir saugojimo išteklius, nekeičiant pagrindinės sistemos architektūros:

12.13.1. Platforma turi palaikyti skirtingų fizikinių veikimo principų, skirtingų tipų ir skirtingų gamintojų sensorius, įskaitant, bet neapsiribojant, radiolokacinius, radijo dažnio / elektroninės žvalgybos, akustinius, elektrooptinius, infraraudonųjų spindulių, vaizdo kamerų, pasyvių bei kitus oro erdvės stebėjimo duomenų šaltinius.

12.13.2. Naujo tipo sensoriaus integravimas turi būti atliekamas sukuriant arba konfigūruojant atitinkamą sensoriaus adapterį, nekeičiant kitų jau integruotų sensorių veikimo ir pagrindinės duomenų apdorojimo platformos programinės logikos.

12.13.3. Sistema turi turėti centralizuotą sensorių registrą, kuriame kiekvienam sensoriui suteikiamas unikalūs identifikatoriai ir pagal technines galimybes saugoma bei atnaujinama informacija apie sensoriaus tipą, geografinę padėtį, priklausomybę, būseną, pasiekiamumą, stebėjimo / aptikimo zoną, duomenų patikimumo rodiklius, ryšio būseną ir priskyrimą operaciniam rajonui.

12.14. Platforma turi užtikrinti sąveiką su galiojančiais NATO standartais pagal integruojamų sensorių tipus bei sudaryti galimybę integruoti kosminių sistemų perduodamus duomenis.

13. Duomenų apdorojimo platformai:

13.1. Platforma turi užtikrinti duomenų apdorojimo ir valdymo funkcionalumą, įskaitant duomenų tvarkymą, transformavimą, duomenų saugos užtikrinimą bei duomenų ir rezultatų paėmimą bei perdavimą kitoms informacinėms sistemoms, palaikydama tiek paketinį, tiek srautinį apdorojimą ir struktūrizuotus, pusiau struktūrizuotus bei nestruktūrizuotus duomenis;

13.2. Platforma turi užtikrinti duomenų analizės ir vizualizavimo funkcijas, sudarančias galimybę naudotojams analizuoti duomenis, gauti aktualią informaciją ir priimti duomenimis pagrįstus sprendimus realiuoju laiku;

13.3. Platforma turi gebėti vykdyti mašininio mokymosi algoritmus, kaupti operatorių patvirtintus, pakeistus ar atmetus objektų klasifikavimo ir grėsmės vertinimo sprendimus kaip mokymui tinkamus duomenis ir sudaryti galimybę šiuos duomenis naudoti kontroliuojamam klasifikavimo bei grėsmės vertinimo modelių mokymui ir tobulinimui. Mašininio mokymosi modelių mokymas, keitimas ir diegimas turi būti valdomas, audituojamas ir versijuojamas, išlaikant galimybę atkurti ankstesnę modelio versiją;

13.4. Platforma turi būti horizontaliai ir (ar) vertikalčiai plečiama, išlaikant nustatytus našumo parametrus didėjant objektų, sensorių, naudotojų, duomenų šaltinių ir operacinių rajonų skaičiui.

Sistemos architektūroje ir licencijavimo modelyje neturi būti nustatyto fiksuoto maksimalaus integruojamų sensorių skaičiaus, o architektūra turi būti parengta tokiu pačiu principu plėsti integruojamų efektorių skaičių;

13.5. Platforma turi būti paremta moduline architektūra ir palaikyti integraciją su informacinėmis sistemomis bei įvairiais duomenų šaltiniais per standartizuotas dokumentuotas taikomųjų programų sąsajas (angl. Application Programming Interface, API), kurios užtikrintų vartotojų ir sistemų autentifikavimą, autorizavimą bei integracinių veiksmų registravimą;

13.6. Platforma turi automatiškai apskaičiuoti ir atvaizduoti kiekvieno sekamo objekto tapatumo patikimumo koeficientą, išreikštą procentine verte (0–100 %), įvertinant skirtingų sensorių pateikiamų duomenų tikimybę priklausyti tam pačiam fiziniam objektui, užtikrinti objekto judėjimo trajektorijos atvaizdavimą nuo pirminio aptikimo momento per visą skrydį, apjungiant ir suliejant skirtingų sensorių duomenis. Taip pat atlikti būsimos trajektorijos prognozę, remiantis objekto judėjimo parametrais ir sekimo duomenimis;

13.7. Platforma turi automatiškai siūlyti kiekvieno sekamo objekto klasifikaciją pagal visus prieinamus skirtingų sensorių duomenis, įskaitant greitį, aukštį, trajektoriją, manevravimo charakteristikas, elektroninius, akustinius, vaizdinius ir kitus prieinamus požymius, priskiriant objektą atitinkamai kategorijai ir pateikiant klasifikavimo patikimumo koeficientą. Autorizuotas operatorius turi galėti sistemos pasiūlytą klasifikaciją patvirtinti, pakeisti arba atmesti ir objektą klasifikuoti rankiniu būdu. Operatorius priimti sprendimai turi būti registruojami ir, juos patvirtinus kaip tinkamus mokymui, naudojami klasifikavimo algoritmams tobulinti;

13.8. Platforma turi palaikyti operacinio žemėlapių atnaujinimą realiuoju laiku arba beveik realiuoju laiku, kai duomenų atnaujinimo delsa neviršija 5 sekundžių nuo duomenų gavimo iš šaltinio;

13.9. Žemėlapyje turi būti atvaizduojami objektai pagal STANAG 2019 (galiojanti versija) ir su jais susijusią informaciją, kurią vartotojas galėtų modifikuoti ir pritaikyti pagal operacinę poreikį;

13.10. Platforma turi pateikti naudotojams su operacine aplinka susijusią informaciją, įskaitant reljefo, infrastruktūros ir meteorologinius duomenis pagal integruotų duomenų šaltinių prieinamumą;

13.11. Platforma turi užtikrinti automatinį ir rankinį objektų rūšiavimą, grėsmės vertinimą ir prioritetų nustatymą pagal konfigūruojamus kriterijus, įskaitant grėsmės lygį, objekto tipą, klasifikavimo patikimumą, atstumą, greitį, aukštį, judėjimo ir prognozuojamą trajektoriją, artėjimą prie saugomų objektų ar teritorijų ir operacinę svarbą. Autorizuotas operatorius turi galėti rankiniu būdu nustatyti ar pakeisti objekto rūšį, grėsmės lygį ir prioritetą. Tokie operatoriaus sprendimai turi būti registruojami ir, juos patvirtinus kaip tinkamus mokymui, naudojami automatiniams klasifikavimo ir grėsmės vertinimo algoritmams tobulinti;

13.12. Platformoje turi būti funkcija sensorių, kurių išduodamų duomenų negalima konvertuoti į vieningą formatą, duomenų stebėjimui, analizei ir atvaizdavimui galutiniam vartotojui pagal suteiktas teises;

13.13. Platforma privalo realiuoju laiku (angl. in real-time) priimti, dekoduoti, koreliuoti ir atvaizduoti ne mažiau kaip 1000 aktyvių antropogeninės kilmės oro erdvės objektų (taikinių / sekų) vienu metu, neviršydama nustatytų vėlavimo ir techninės įrangos išteklių ribų. Nurodytas 1000 aktyvių antropogeninės kilmės oro erdvės objektų skaičius yra minimalus sistemos našumo reikalavimas ir negali būti laikomas maksimaliu sistemos architektūriniu ar licenciniu apribojimu;

13.14. Platforma, atlikdama objekto identifikavimą, privalo pateikti patikimumo koeficientą (procentine išraiška) ir užtikrinti, kad klaidingų teigiamų atpažinimų (angl. False Positive) dažnis neviršytų 5 %, naudojant įvairiarūšius (akustinius, vaizdo, radijo dažnio, radiolokacinius ir pan.) sensorių duomenis;

13.15. Platforma privalo užtikrinti, kad laikas nuo pirminio objekto užfiksavimo sensoriuje iki patvirtintos atžymos (stabilaus sisteminio pėdsako) ir jo judėjimo trajektorijos sudarymo platformoje

neviršytų 2 sekundžių, o objekto grėsmės vertinimas būtų koreliuojamas su tikėtina objekto skrydžio trukme fiksuojančių sensorių matomumo ribose ir vertinamoje zonoje esančio efektoriaus veiksmingu efekto nuotoliu;

13.16. Platforma privalo užtikrinti, kad objekto priskyrimo objektų kategorijai (paukštis / balionas / debesy / bepilotis orlaivis ir pan.) laikas turi būti pasiekiamas užtikrinant nustatytą pasitikėjimo slenkstį ir neviršijant maksimalios klaidingų teigiamų (angl. False Positive) ribos, išnaudojant įvairiarūšius (akustinius, vaizdo, radijo dažnio, radiolokacinius ir pan.) sensorių duomenis;

13.17. Platforma turi gebėti realiuoju laiku automatiškai aptikti, identifikuoti ir klasifikuoti gamtinės bei biologinės kilmės objektus (trikdžius) ir taikyti dinaminį jų slopinimą (angl. Clutter Mitigation / Suppression) užtikrinant, kad šie objektai neperkrautų operatoriaus sąsajos, tačiau išliktų sistemos atmintyje tolimesnei analizei;

13.18. Platforma privalo automatiškai apdoroti, sinchronizuoti ir sulieti iš skirtingų šaltinių gaunamus telemetrijos duomenis, identifikuoti dubliuojamus įrašus ir pašalinti sensorines paklaidas. Skirtingiems sensoriams aptikus tą patį fizinį objektą, sistema turi koreliuoti duomenis ir, pasiekus nustatytą patikimumo slenkstį, išlaikyti vieną sisteminį objekto identifikatorių bei vientisą sekimo istoriją.

13.19. Kiekvienam MOGS suformuotam fiziniam oro erdvės objektui turi būti suteiktas vieningas sisteminis identifikatorius. Objekto identifikatorius ir jo istorija turi būti išlaikomi perduodant sekimą tarp skirtingų sensorių, objektui pereinant tarp operacinių rajonų, laikinai praradus dalies sensorių kontaktą ir keičiantis pagrindiniam objektą sekančiam sensoriui.

III. VALSTYBĖS UŽSAKYMO ETAPAI

14. Valstybės užsakymas įgyvendinamas 3 etapais:

14.1. I etapo rezultatas (iki 2 mėn.) – veikiantis prototipas apimantis duomenų perdavimo bei duomenų apdorojimo platformų sukūrimą ir sprendimo perdavimas efektoriams per duomenų atvaizdavimo platformą. Prototipe turi būti ne mažiau kaip 5 integruoti skirtingo tipo sensoriais. Nurodytas ne mažiau kaip 5 skirtingų tipų sensorių skaičius yra prototipo integravimo ir veikimo demonstravimo kriterijus ir negali būti laikomas maksimaliu sistemoje integruojamų sensorių skaičiumi;

14.2. II etapo rezultatas (iki 6 mėn.) – MOGS veikianti kaip savarankiška sistema, kurioje integruoti valdomi sensoriai ir efektoriai (nacionalinis lygmuo). Šiame etape turi būti realizuotas centralizuotas sensorių ir efektorių registrai, nacionalinio lygmens bendro oro situacijos vaizdo formavimas ir centralizuotai konfigūruojamų operacinių rajonų funkcionalumas, įskaitant duomenų/sprendimo perdavimas atitinkamo operacinio rajono vadovavimo elementui ir nenutrūkstamas objektų sekimo perdavimas tarp operacinių rajonų;

14.3. III etapo rezultatas (iki 12 mėn.) – MOGS integravimas su OESKS, bei su Sąjungininkų duomenų perdavimo platformomis. Galutinis MOGS rezultatas turi išlaikyti atvirą ir dokumentuotą architektūrą sensorių ir efektorių integravimui, nereikalaujant keisti pagrindinės MOGS architektūros ir duomenų modelio.

15. Valstybės užsakymo vykdymo metu periodiškai turės būti pademonstruoti tarpiniai rezultatai.

IV. KOMPLEKTACIJA

16. Galutinė MOGS sistemos komplektacija ir jos sudedamųjų dalių apimtis bus patikslinta, įvertinus konsultacijų su pramonės atstovais rezultatus ir rinkoje prieinamus techninius sprendinius. Tikslūs galutinės įrangos kiekiai šiame etape nenustatomi, kadangi sistema projektuojama kaip atviros ir

modulinės architektūros, sudarant galimybę ją nuosekliai plėsti vertikaliai, didinant atskirų komponentų pajėgumą, ir horizontaliai, prijungiant papildomus komponentus, platformas ar funkcinius modulius. MOGS architektūroje ir programinės įrangos licencijavime neturi būti nustatyti fiksuoti maksimalūs integruojamų sensorių, operacinių rajonų ar integruojamų efektorių skaičiaus apribojimai; sistemos pajėgumas turi būti didinamas pridėdant reikalingus techninius ir programinius išteklius, nekeičiant pagrindinės architektūros.

17. Dalyvis atsako už techninės ir programinės įrangos reikalingos projektui įgyvendinti pateikimą.

V. GARANTINIS LAIKOTARPIS

18. Įsigytai įrangai turi būti suteiktas ne mažiau kaip 24 mėnesių garantinis laikotarpis, skaičiuojamas nuo pirkėjo ir pardavėjo priėmimo – perdavimo akto pasirašymo datos.

19. Dalyvis atsako už MOGS priežiūrą bei palaikymą (angl. SLA) ne mažiau kaip 24 mėnesių laikotarpiui nuo pirkėjo ir pardavėjo priėmimo – perdavimo akto pasirašymo datos.
