Panevėžio mechatronikos centras
Pilėnų g. 30-1A
Panevėžys
+370 6 5533 156
Ataskaitą parengė: dr. Donatas Pelenis ir Dovydas Barauskas

Panevėžio energija - šilumos ir karšto vandens skaitiklių skaitmenizavimas - analizė

2025-12-10

SANTRAUKA

Europos Sąjungos direktyvos dėl atsinaujinančių energijos išteklių ir šilumos apskaitos skaitmenizavimo numato, kad iki 2026 m. vasario 21 d. visuose centralizuotai šilumą gaunančiuose pastatuose turi būti įrengti nuotoliniu būdu nuskaitomi šilumos ir karšto vandens skaitikliai.

AB „Panevėžio energija“ šiame kontekste valdo apie 64 tūkst. apskaitos prietaisų parką (KVS, ŠAP, ENReader ir kt.), dalis jų jau turi LoRaWAN ar OMS ryšį, tačiau nemaža dalis įvadinių skaitiklių vis dar priklausomi nuo 2G GPRS ryšio, kuris iki 2030 m. bus palaipsniui išjungiamas. Pagrindinis ataskaitos klausimas – kokia technologiškai ir ekonomiškai pagrįsta architektūra bei eksploatacijos modelis leidžia laiku ir tvariai modernizuoti šilumos ir karšto vandens apskaitos sistemą Panevėžyje, užtikrinant ES reikalavimų, saugumo ir duomenų apsaugos atitiktį.
Atlikta esamos infrastruktūros analizė parodė, kad skaitiklių parkas yra mišrus – nuo senesnių mechaninių iki modernių ultragarsinių KVS ir ŠAP su LoRaWAN, wM-Bus/OMS ar NFC moduliais. Šiuo metu Panevėžyje veikia keturios LoRaWAN bazinės stotys, kurios užtikrina patikimą ryšį ~90 % prijungtų skaitiklių; likęs ~10 % yra „probleminės“ vietos (rūsiai, storos sienos, miesto pakraščiai), kuriose ryšys silpnas arba jo visai nėra. Duomenų bazės ir IT pusėje identifikuota, kad nėra vieningos MDMS/DB sistemos – įvairių tiekėjų duomenys sujungiami rankiniu būdu per mėnesines ataskaitas, todėl vėluoja klaidų aptikimas, nėra centralizuotų KPI ir SLA stebėsenos.

LoRaWAN tinklo modeliavimui sukurtas algoritmas, naudojantis realias pastatų geometrijas, aukščius ir vegetacijos sluoksnius iš OpenStreetMap bei ITU-R rekomendacijų pagrindu sudarytus slopinimo modelius. Jis leidžia automatiškai suplanuoti papildomų bazinių stočių kiekį ir

vietas, kad būtų padidinta aprėptis ir sumažintas „neuždengtų“ objektų skaičius iki kelių procentų, neperkraunant tinklo ir nekuriant perteklinės infrastruktūros. Tuo pačiu metu įvadinių skaitiklių daliai numatoma migracija nuo 2G GPRS prie LTE-M/NB-IoT, naudojant naujus radijo modulius, saugų APN/VPN ir TLS pagrįstą telemetriją. Technologijų palyginime įvertintos LoRaWAN ir NB-IoT modulių bei skaitiklių kainos, licencinės ir ryšio paslaugų išlaidos, prieigos stotelių ir SIM kortelių OPEX, taip pat personalo (FTE) poreikis. LoRa-tik scenarijuje TCO labiausiai lemia prieigos stotelių eksploatacija ir LoRa operacijų komandos darbas, tuo tarpu NB-tik scenarijuje didžiausia dalis yra ilgalaikiai SIM kaštai (iki ~2,6 mln. € per 15 metų, jei visi įrenginiai būtų NB-IoT).

Jautrumo analizė parodė, kad NB SIM kainos padvigubėjimas žymiai padidina NB-tik scenarijaus TCO, o LoRa tinklas yra santykinai atsparus prieigos stotelių kiekio svyravimams. Optimalus kompromisas gaunamas mišriame scenarijuje, kai NB-IoT naudojamas tik problemiškiems KVS (rūsiai, atokūs objektai) ir visiems įvadiniams ŠAP (~10–20 % visų įrenginių): papildoma „draudimo“ kaina lyginant su LoRa-tik scenarijumi sudaro apie 0,36–0,70 mln. € per 10 metų, tačiau ženkliai sumažina ryšio riziką ir vizitų dėl gedimų skaičių.

Ataskaita įvertina tris eksploatacijos modelius – SaaS, hibridinį ir self-hosted – ir parodo, kad SaaS modelis leidžia greičiausiai pasiekti aukštus SLA, bet su didesnėmis ilgalaikėmis licencinėmis sąnaudomis; self-hosted suteikia pilną kontrolę ir mažiausią OPEX, bet reikalauja brandžios IT/OT komandos ir nuolatinio DR/testavimo režimo. Hibridinis modelis, kai LoRaWAN tinklo serveris (LNS) ir įrenginių flotilės valdymas perkami kaip paslauga (pvz., The Things Stack Cloud su 99,9 % SLA), o ingestas, MDMS ir analitika veikia įmonės valdomoje ES debesijoje, ataskaitoje argumentuotai įvardijamas kaip tinkamiausias Panevėžio masteliui. Toks modelis leidžia išlaikyti vieneto kainą apie 0,23–0,26 €/įreng./mėn. šiandieninėmis sąlygomis ir palikti galimybę vėliau migruoti į self-hosted LNS, sumažinant OPEX iki ~0,06–0,08 €/įreng./mėn. esant ~1 FTE komandai.

Sistemos CAPEX pusėje siūloma remtis atvirojo kodo komponentais (Linux, PostgreSQL/TimescaleDB, Mosquitto/EMQX, Kafka, Prometheus, Grafana, Keycloak, Ansible ir kt.), kuriems nereikia licencinių „už vartojimą“ mokesčių; pagrindinio NB-IoT/LoRaWAN ingest, DB, API, monitoringui ir CI/CD numatyta apie 1500 inžinerinių valandų, arba ~116 000 € CAPEX, kuris tampa pagrindine platformos investicija. Saugos architektūra suprojektuota pagal GDPR, NIS2, CRA, RED ir MID reikalavimus – naudojamas end-to-end šifravimas (LoRaWAN OTAA, AES-128, TLS 1.2/1.3), raktų valdymas HSM pagrindu, RBAC/SSO bei auditų politika.

Ataskaita parodo, kad AB „Panevėžio energija“ gali pasiekti ES direktyvų atitiktį ir pereiti prie pilnai nuotolinės šilumos ir karšto vandens apskaitos, pasirinkdama mišrią LoRaWAN + NB-IoT technologijų kombinaciją ir hibridinį eksploatacijos modelį. LoRaWAN išlieka pagrindiniu ryšio kanalu daugumai butų skaitiklių, o NB-IoT naudojamas kaip „draudimo polisas“ problemiškoms lokacijoms ir įvadiniams skaitikliams, taip subalansuojant TCO, patikimumą ir diegimo terminus.

Rekomenduojama etapais: (1) sutvarkyti vieningą MDMS/DB ir integracijas su esama apskaitos sistema; (2) įgyvendinti LoRaWAN tinklo sutankinimą pagal parengtą modelį ir lygiagrečią LTE-M/NB-IoT migraciją įvadiniams ŠAP; (3) atlikti pilotą su hibridiniu LNS modeliu, po kurio priimti sprendimą dėl ilgalaikės architektūros (kritiškai vertinant TCO ir komandos brandą); (4) iki 2026-02-21 užbaigti viso skaitiklių parko perėjimą prie nuotolinio nuskaitymo, kartu įdiegiant GDPR ir NIS2 atitinkančius procesus bei KPI/SLA stebėseną.

ATITIKTIS PASLAUGŲ SUTARČIAI (1.1.1–1.1.5)

Užduotys:

1.1.1 Išnagrinėti naujausias, rinkoje egzistuojančias, šilumos ir karšto vandens apskaitos nuotolinių duomenų surinkimo ir perdavimo technologijas, jų privalumus ir trūkumus tiek technologiniu tiek ekonominiu požiūriu,

1.1.2. Ištirti, bevielių skaitmeninių perdavimo įrenginių bei ryšio tinklų suderinamumą, duomenų perdavimo patikimumą, energetinių poreikių užtikrinimo būdus;

1.1.3. Pasiūlyti optimizuotą technologinių sprendinių visumą, leidžiančią ekonomiškai pagrįstomis kainomis nuotoliniu būdu nuskaityti ir perduoti skaitiklių duomenis;

1.1.4. Įvertinti telemetrijos priėmimo infrastruktūros architektūros pasirinkimus, jų privalumus ir trūkumus, bei suprojektuoti duomenų priėmimo, kaupimo ir atvaizdavimo sistemą;

1.1.5. Įvertinti skirtingas duomenų tiekimo sutrikimo rizikas ir pasiūlyti sprendimo būdus, sumažinant nepatogumą ir kaštus šilumos vartotojams bei šilumos tiekėjui;

1.1.1. Technologijų analizė (technologiniai ir ekonominiai privalumai / trūkumai)

Ataskaitos vietos patikrinimui:

- „PROJEKTO KONTEKSTAS IR AKTUALUMAS“
- „TEISINĖ IR TECHNOLOGINĖ APLINKA (ES DIREKTYVŲ REIKALAVIMAI, 2G IŠJUNGIMO KONTEKSTAS) PROBLEMATIKA“
- „INFRASTRUKTŪROS ANALIZĖ“
- „TELEMETRINIŲ ĮRENGINIŲ DUOMENŲ SURINKIMO METODAI APSKAITOS ĮRENGINIUOSE“
- „LORAWAN IR NB-IOT SKAITIKLIŲ KAINŲ SKIRTUMO PAGRINDIMAS“
- „LORAWAN IR NB-IOT TECHNOLOGIJŲ EKONOMINIS PALYGINIMAS“ (CAPEX/OPEX/TCO poskyriai)
- „EKSPLOATACIJOS MODELIAI (SAAS, HIBRIDAS, SELF-HOSTED) IR SLA“

1.1.2. Suderinamumas, patikimumas ir energetika (įrenginiai ↔ tinklas ↔ IT)

Ataskaitos vietos patikrinimui:

- „INFRASTRUKTŪROS ANALIZĖ“ (suderinamumo sluoksniai: M-Bus/wM-Bus/OMS, LoRaWAN/NB-IoT/LTE, integracijos)
- „TELEMETRINIŲ ĮRENGINIŲ DUOMENŲ SURINKIMO METODAI APSKAITOS ĮRENGINIUOSE“ (siuntimo periodika, energijos biudžetas)
- „DUOMENŲ PERDAVIMO KOKYBĖ IR TINKLO APRĖPTIS“
- „PATIKIMUMO MATAVIMAS IR DUOMENŲ PILNUMO KPI“
- „LORAWAN TINKLO MODELIAVIMAS PANEVĖŽIO ENERGIJOS APSKAITOS PRIETAISŲ DUOMENŲ SURINKIMUI“
- „EKSPLOATACIJOS MODELIAI (SAAS, HIBRIDAS, SELF-HOSTED) IR SLA“ + „PRIĖMIMO KRITERIJAI IR KPI RIBOS“

1.1.3. Optimizuota sprendinių visuma (ekonomiškai pagrįstomis kainomis)

Ataskaitos vietos patikrinimui:

- „LORAWAN IR NB-IOT TECHNOLOGIJŲ EKONOMINIS PALYGINIMAS“ (CAPEX/OPEX/TCO ir jautrumo logika)
- „REKOMENDACIJA B - VYSTYTI LoRaWAN 70% - NB-IOT 30% TINKLĄ“
- „OPTIMIZUOTOS SPRENDINIŲ VISUMOS APRAŠAS“ + „Siūloma sprendinių visuma (komponentai):“
- „EKSPLOATACIJOS MODELIAI (SAAS, HIBRIDAS, SELF-HOSTED) IR SLA“ (modelio pasirinkimo argumentai)

1.1.4. Telemetrijos priėmimo infrastruktūros architektūra ir sistemos projektas

Ataskaitos vietos patikrinimui:

- „DABARTINĖ PE SERVERIŲ IR DUOMENŲ BAZĖS ARCHITEKTŪRA“
- „DUOMENŲ PRIĖMIMO, KAUPIMO IR ATVAIZDAVIMO SISTEMOS FUNKCINIS PROJEKTAS“ + „Rekomenduojamas end-to-end duomenų srautas:“
- „ATITIKTIS IR SERTIFIKATAI – GDPR, RADIO EQUIPMENT DIRECTIVE, MID, NIS2“ (saugos architektūros principai)
- „EKSPLOATACIJOS MODELIAI (SAAS, HIBRIDAS, SELF-HOSTED) IR SLA“ (architektūros pasirinkimų argumentai)

1.1.5. Duomenų tiekimo sutrikimų rizikos ir mažinimo sprendimai

Ataskaitos vietos patikrinimui:

- „TEISINĖ IR TECHNOLOGINĖ APLINKA (... 2G IŠJUNGIMO KONTEKSTAS) ...“ (išorinės rizikos)

- „DUOMENŲ PERDAVIMO KOKYBĖ IR TINKLO APRĖPTIS“ (probleminės zonos)
- „PATIKIMUMO MATAVIMAS IR DUOMENŲ PILNUMO KPI“ + „PRIĖMIMO KRITERIJAI IR KPI RIBOS“ (KPI/SLA rizikos valdymui)
- „LORAWAN TINKLO MODELIAVIMAS ...“ (aprėpties didinimo priemonės)
- „RIZIKŲ VERTINIMAS IR DUOMENŲ TIEKIMO SUTRIKIMŲ VALDYMO PRIEMONĖS“ (rizikų registras ir priemonės)

TERMINOLOGIJA

KVS – karšto vandens skaitiklis; ŠAP – šilumos apskaitos prietaisas; AMR – automatinis rodmenų surinkimas; IoT – daiktų internetas; LPWAN – mažų energijos sąnaudų plataus nuotolio tinklai; LoRaWAN – ilgojo nuotolio radijo ryšio tinklas; NB-IoT – siaurajuostis daiktų interneto ryšys mobiliojo tinklo infrastruktūroje; GPRS – 2G paketinių duomenų perdavimas; SRD – trumpųjų nuotolių radijo įrenginiai; M-Bus – laidinis skaitiklių ryšio standartas; wM-Bus – belaidė M-Bus versija; OMS – atvirasis matavimo standartas; BLE – Bluetooth Low Energy; ADR – adaptacinis duomenų perdavimo spartų valdymas LoRaWAN tinkle; RAN – radijo prieigos tinklas; EPC – LTE branduolio tinklas; PSM – energijos taupymo režimas NB-IoT įrenginiuose; eDRX – prailginta išjungto priėmimo trukmė NB-IoT įrenginiams; LNS – LoRaWAN tinklo serveris; MDMS/MDM – skaitiklių duomenų valdymo sistema; MQTT – lengvas žinučių perdavimo protokolas; API – paslaugų programavimo sąsaja; DB – duomenų bazė; SaaS – programinė įranga kaip paslauga; SIM/eSIM – mobiliojo ryšio autentifikacijos moduliai; VPN – virtualus privatus tinklas; TLS – saugaus ryšio protokolas; AES – simetrinio šifravimo algoritmas; DevEUI – LoRaWAN įrenginio unikalus identifikatorius; OTAA – įrenginio aktyvavimas per radijo ryšį LoRaWAN tinkle; HSM – aparatinis saugių raktų modulis; RBAC – teisių valdymas pagal roles; SSO – vieno prisijungimo mechanizmas; GDPR/BDAR – bendrasis duomenų apsaugos reglamentas; EED – energijos vartojimo efektyvumo direktyva; EPBD – pastatų energinio naudingumo direktyva; RED – radijo įrangos direktyva; MID – matavimo priemonių direktyva; NIS2 – tinklų ir informacinių sistemų saugumo direktyva; CRA – kibernetinio atsparumo aktas; CAPEX – kapitalo investicijos; OPEX – veiklos sąnaudos; TCO – bendra nuosavybės kaina; ROI – investicijų grąža; KPI – veiklos rodikliai; SLA – paslaugų lygio susitarimas; FTE – pilno etato ekvivalentas.

ATASKAITOS TIKSLAS

Šios ataskaitos tikslas – išanalizuoti AB „Panevėžio energija“ šilumos sunaudojimo apskaitos dabartinę būklę ir pateikti strateginį planą jos modernizavimui bei skaitmenizavimui. Dokumente apibrėžiamos esamos infrastruktūros problemos, įvertinami teisiniai ir technologiniai aplinkos veiksniai, ir pasiūlomi keli modernizacijos scenarijai. Remiantis atlikta analize, pateikiamos rekomendacijos ir tolimesni veiksmai, padėsiantys bendrovei efektyviai pereiti prie nuotolinio duomenų nuskaitymo ir valdymo sistemos, atitinkančios šiuolaikinius reikalavimus.

PROJEKTO KONTEKSTAS IR AKTUALUMAS [S-1.1.1][S-1.1.3]

Šilumos vartojimo apskaitos skaitmeninimas šiuo metu yra ypač aktualus energetikos sektoriuje. ES energetikos efektyvumo ir atsinaujinančių išteklių direktyvos skatina didesnį skaidrumą bei efektyvumą tiekiant šilumą galutiniams vartotojams. AB „Panevėžio energija“, kaip centralizuotai šilumą tiekianti bendrovė Panevėžio mieste ir regione, susiduria su būtinybe modernizuoti šilumos ir karšto vandens apskaitos sistemas. Tradiciniai rodmenų nurašymo metodai nebeatitinka šiuolaikinių poreikių – vartotojai tikisi automatizuoto atsiskaitymo, o tiekėjui svarbu laiku gauti tikslius duomenis analizei ir operatyviam valdymui.

Projektu siūloma atlikti taikomuosius tyrimus ir parengti šilumos suvartojimo apskaitos skaitmenizavimo sprendimą, skirtą individualiems šilumos vartotojams daugiabučiuose namuose. Tai leistų Panevėžio miestui tapti pavyzdiniu skaitmenizuotos šilumos apskaitos diegimo miestu – būtų užtikrintas didesnis šilumos tiekimo skaidrumas, mažesnės sąskaitos gyventojams dėl tikslesnio apskaitos duomenų surinkimo, o sukurtą sprendimą būtų galima pritaikyti ir nacionaliniu mastu. Šiuo metu rinkoje egzistuoja keletas nuotolinio duomenų nuskaitymo (telemetrijos) sprendimų, tačiau jų diegimas masiškai susijęs su nemenkomis problemomis. Pavyzdžiui, daugybės duomenų surinkimo mazgų įdiegimas kiekviename bute gali būti ekonomiškai nepateisinamas – tokia įranga brangi, turi perteklinių funkcijų ir reikalauja papildomos priežiūros (pvz., dažnai keisti baterijas). Dėl šios priežasties būtina ieškoti optimizuotų technologinių sprendinių, kurie už priimtiną kainą leistų nuotoliniu būdu nuskaityti skaitiklių rodmenis. Atsižvelgiant į tai, mūsų projekte planuojama eksperimentiškai palyginti skirtingas belaidžio duomenų perdavimo technologijas (NB-IoT, LoRa, Bluetooth LE ir kt.) ir nustatyti, kurios iš jų tinkamiausios centralizuotos šilumos vartotojų apskaitai. Projekto rezultatas – parengtos rekomendacijos dėl optimalios duomenų surinkimo infrastruktūros parinkimo ir sukurti prototipiniai sprendimai, parodantys, kaip jie galėtų būti pritaikomi daugiabučiuose gyvenamuosiuose namuose praktikoje. Taip bus pagrindžiama modernizacijos nauda Panevėžio bendruomenei ir sustiprinamas bendrovės technologinis pranašumas.

TEISINĖ IR TECHNOLOGINĖ APLINKA (ES DIREKTYVŲ REIKALAVIMAI, 2G IŠJUNGIMO KONTEKSTAS) PROBLEMATIKA [S-1.1.1][S-1.1.5]

Bendrovės modernizacijos planus pirmiausia lemia teisiniai reikalavimai. Europos Sąjungos direktyva 2018/2001 dėl atsinaujinančių išteklių naudojimo energetikoje bei nauja Direktyva (ES) 2023/2413, skatinanti šilumos sunaudojimo apskaitos skaitmenizavimą, numato, kad iki 2026 m. vasario 21 d. visuose centralizuotos šilumos vartotojų pastatuose turi būti įdiegtos nuotolinio nuskaitymo apskaitos priemonės. Tai reiškia, kad per artimiausius metus AB „Panevėžio energija“ privalo užtikrinti, jog visi šilumos ir karšto vandens skaitikliai klientų objektuose būtų modernizuoti ir galėtų nuotoliniu būdu teikti duomenis. Neįgyvendinus šio reikalavimo, bendrovei grėstų sankcijos, o vartotojai nepatirtų direktyvose numatytos naudos.

Technologinė aplinka taip pat sparčiai keičiasi. Mobiliojo ryšio infrastruktūra pereina prie naujesnių kartų: šiuo metu telekomunikacijų operatoriai planuoja laipsniškai atsisakyti senesnių tinklų. Pvz., 3G ryšio tinklai Lietuvoje jau pradėti išjunginėti ir artimiausiais metais bus visiškai išjungti, o 2G ryšys, nors ir veiks iki ~2030 m., laikomas pasenusia technologija. Daug komunalinių apskaitos prietaisų (signalizacijos, nuotolinio valdymo vartai, skaitikliai) vis dar naudoja 2G/GPRS modulius, todėl operatoriai ragina jau dabar planuoti jų keitimą modernesniais. Ši tendencija tiesiogiai paliečia AB „Panevėžio energija“ turimą įrangą – daugelis šiuo metu naudojamų duomenų perdavimo įrenginių (modemų) veikia 2G GPRS tinkle. Technologinės aplinkos analizė taip pat apima naujų IoT ryšio technologijų atsiradimą: pastaraisiais metais išplito siaurajuosčio daiktų interneto NB-IoT ryšys, taip pat privačių ir viešų tinklų sprendimai, tokie kaip LoRaWAN, kurie leidžia ekonomiškai perduoti mažos apimties duomenis dideliais atstumais. Taip pat pasirodė modernūs skaitikliai su BLE (Bluetooth Low Energy) ryšiu trumpiems atstumams. Visa ši aplinka sukuria prielaidas rinktis geriausią techninį sprendimą, bet kartu verčia atidžiai planuoti – reikia užtikrinti, kad pasirinkta technologija būtų ilgalaikė (veiktų ir po 2030 m.), suderinama su kitomis sistemomis ir atitiktų teisės aktų reikalavimus.

INFRASTRUKTŪROS ANALIZĖ [S-1.1.1][S-1.1.2][S-1.1.4]

Bendrovė eksploatuoja mišrią, kelių technologinių lygių apskaitos prietaisų infrastruktūrą. Šiuo metu Panevėžio mieste ir regioniniuose padaliniuose naudojami tiek modernūs ultragarsiniai ar elektroniniai, tiek senesni mechaniniai vandens ir šilumos skaitikliai. Daugiabučių namų karšto vandens skaitikliai (KVS) ir dalis šilumos apskaitos prietaisų (ŠAP) aprūpinti nuotolinio nuskaitymo įranga, daugiausia paremta LoRaWAN technologija. Iš viso Panevėžyje įdiegta 3 715 LoRa ryšiu duomenis perduodančių buitinių vandens skaitiklių ir 355 šilumos apskaitos įrenginiai. Šie skaitikliai – tai įvairių gamintojų įrenginiai: Qalcosonic W1 (286 vnt.), Hydrodigit (71 vnt.), Zenner Minomess (2 176 vnt.), Wehrle WeCount-S (1 177 vnt. instaliuoti, dar ~1 200 paruošti diegimui) ir Qalcosonic E3 (355 vnt. butuose, 6 vnt. įvaduose). Visi šie įrenginiai turi integruotus LoRaWAN, OMS bevielio M-Bus arba NFC ryšio modulius, leidžiančius automatiškai perduoti rodmenis.

Duomenų perdavimui iš pastatų įvadinių apskaitos prietaisų vis dar dažniausiai naudojamas 2G GPRS ryšys, nors jis palaipsniui keičiamas į 4G LTE. Šiuo metu 335 įvadiniai šilumos skaitikliai jau aprūpinti LTE modemais, tačiau apie 72 % vis dar veikia su 2G įranga. Duomenų nuskaitymui naudojami valdikliai ENReader, kurie per M-Bus sąsają surenka informaciją iš šilumos skaitiklių. Regionuose naudojami vandens skaitikliai dažniausiai priklauso UAB „Aukštaitijos vandenys“ ir turi impulsinį išėjimą – šiuo tikslu naudojami impulsų adapteriai ENCOpulse arba PA-1, leidžiantys integruoti analoginius skaitiklius į skaitmeninio nuskaitymo sistemą.

Panevėžio mieste LoRa tinklas veikia jau penktus metus, šiuo metu jį sudaro 4-6 antenos. Tačiau, jų aprėptis užtikrina patikimą duomenų perdavimą tik apie 90 % PE aptarnaujamų įrenginių – ypač ribotai veikia miesto pakraščiuose. Regioniniuose padaliniuose (Kėdainiai, Pasvalys,

Rokiškis, Zarasai, Kupiškis) LoRa tinklas neveikia, todėl apie 60 000 mechaninių KVS vis dar reikalauja deklaravimo ar fizinės patikros.

Šiuo metu naudojami skaitikliai (Qalcosonic, B Meters, Zenner, Wehrle, Maddalena) dažniausiai turi NFC arba optinę sąsają konfigūravimui, bet ne visi palaiko centralizuotą duomenų kaupimą. Skirtingų gamintojų sprendimai neretai reikalauja atskiros programinės įrangos, todėl trūksta vientisos integracijos su vieninga duomenų baze ar atvaizdavimo sistema. Būtina kurti centralizuotą architektūrą, kuri leistų apjungti skirtingus ryšio protokolus (LoRaWAN, wM-Bus, M-Bus) ir užtikrintų ilgalaikį duomenų saugojimą, automatizuotą eksportą ir vizualizaciją.

Suderinamumo požiūriu kritiniai trys sluoksniai: (1) matavimo sąsajos (M-Bus / wM-Bus) ir duomenų profiliai (OMS), (2) perdavimo sluoksnis (LoRaWAN SRD 868 MHz arba operatorinis NB-IoT/LTE-M), (3) integracija į duomenų priėmimo ir apskaitos sistemas per API/eksportus. Siekiant sumažinti gamintojų fragmentaciją, rekomenduojama pirkimuose fiksuoti OMS profilio palaikymą ir sertifikuotą LoRaWAN įgyvendinimą, o NB-IoT įvadiniams įrenginiams numatyti saugų APN/VPN ir TLS telemetriją [OMS Group, 2023; LoRa Alliance, 2020].

Bendrovė susiduria su infrastruktūros modernizavimo iššūkiais: ribota LoRa aprėptis, priklausomybė nuo pasenusios 2G įrangos, ir skirtingų tiekėjų skaitiklių integravimo problemos riboja pažangios apskaitos plėtrą bei galimybę visiškai atsisakyti vartotojų deklaracijų. Atsižvelgiant į 2G technologijos palaikymo nutraukimo perspektyvą iki 2030 m., būtina strateginė infrastruktūros atnaujinimo programa.
Remiantis gautais PE dokumentais, parkas susideda iš maždaug 61 495 KVS butuose ir po vieną bendrą KVS bei vieną ŠAP kiekviename įvade (iš viso apie 1 562 įvadus), taip pat po vieną įvado valdiklį (ENReader) kiekvienam namui; tokiu būdu bendra apskaitos prietaisų suma siekia apie 64 619. Pastatų lygmens eksploatacinės charakteristikos ir šilumos sąnaudų lentelės yra parengtos visiems aptarnaujamiems miestams ir naudojamos kaip aprėpties modelių bei nuskaitomumo KPI bazė (2025-04 ataskaitų rinkiniai rodo tipinę daugiabučių tipologiją ir karšto vandens cirkuliacijos schemas) [7], [2.18], [2.0], [2.2], [2.3].

TELEMETRINIŲ ĮRENGINIŲ DUOMENŲ SURINKIMO METODAI APSKAITOS ĮRENGINIUOSE [S-1.1.2]

Duomenų nuskaitymas šiuo metu vykdomas keliais skirtingais būdais, priklausomai nuo apskaitos prietaiso tipo ir jo įrengimo vietos. Centriniai (įvadiniai) šilumos skaitikliai daugelį metų naudojo 2G GPRS modemus, kurie periodiškai perduoda rodmenis per mobiliojo ryšio tinklą. Pastaraisiais metais nauji įrenginiai komplektuojami su 4G LTE technologiją palaikančiais modemais, užtikrinančiais spartesnį ir patikimesnį duomenų perdavimą, ypač ten, kur 2G signalas yra ribotas ar netrukus taps nebepalaikomas.

Buitiniai vandens ir šilumos skaitikliai, ypač Panevėžio mieste, naudoja LoRaWAN ryšį. Šie skaitikliai nustatytu dažniu (dažniausiai 1–2 kartus per parą, kai kuriais atvejais konfigūruojami iki 4 ir daugiau kartų) siunčia vadinamąsias telegramas į mieste išdėstytas LoRa bazines stotis. Surinkti duomenys toliau perduodami į centrinę duomenų kaupimo sistemą internetiniu ryšiu. Telegramose pateikiamas sunaudoto vandens ar šilumos kiekis, galimi aliarmų pranešimai (pvz., nuotėkis, atbulinis srautas), taip pat baterijos įkrovos būsena.

Baterijos tarnavimo laikas vertinamas energijos biudžetu: vidutinė srovė I_avg priklauso nuo TX ciklo energijos ir siuntimo dažnio, todėl didinant siuntimo intervalą proporcingai mažėja I_avg ir ilgėja tarnavimo laikas. Praktikoje baterijos resursas apskaičiuojamas sumuojant TX ciklų ir miego režimo sąnaudas, o siuntimo intervalas parenkamas taip, kad užtikrintų tikslinį tarnavimo laiką ir reikiamą duomenų pilnumą.

Papildomai praktiniam vertinimui taikoma paprasta energijos biudžeto lygtis: tarnavimo_laikas ~= C_bat / I_avg, kur I_avg ~= (E_TX*N_TX + E_RX*N_RX + I_sleep*T_sleep)/T. Didinant siuntimo dažnį (pvz., nuo 1 iki 4 kartų per parą), N_TX didėja proporcingai ir trumpėja baterijos resursas, jei kiti parametrai nekinta. NB-IoT/LTE-M atveju į biudžetą įtraukiami prisijungimo, pakartotinių siuntimų ir energijos taupymo režimų (PSM/eDRX) ciklai [3GPP, 2016].

Priklausomai nuo gamintojo, skaitikliai gali būti konfigūruojami per artimojo lauko ryšį (NFC) ar optinę infraraudonųjų spindulių sąsają (IrDA). Kadangi LoRaWAN topologija remiasi asimetriniu (uplink-only) ryšiu, realaus laiko duomenų prieinamumas nėra užtikrinamas – rodmenys prieinami tik pagal nustatytą siuntimo grafiką.

Regioniniuose padaliniuose (Kėdainiuose, Pasvalyje, Rokiškyje, Zarasuose, Kupiškyje), kur nuotolinio duomenų nuskaitymo sistema dar nėra įdiegta, skaitiklių rodmenys renkami tradiciniais metodais – vartotojų deklaravimu arba vietiniu nurašymu. Tai didina administracinius kaštus, mažina duomenų tikslumą bei riboja operatyvų reagavimą į gedimus. Todėl diegiami LoRa ryšio sprendimai bei svarstomi techniniai būdai, kaip į sistemą integruoti ir senesnius impulsinius ar mechaninius skaitiklius pasitelkiant impulsų adapterius ar išorinius valdiklius.

Panevėžio mieste jau formuojamas pavyzdinis centralizuotos apskaitos modelis, kurio tikslas – užtikrinti automatizuotą, tikslią ir savarankiško deklaravimo nereikalaujančią skaitiklių duomenų apskaitą.

DABARTINĖ PE SERVERIŲ IR DUOMENŲ BAZĖS ARCHITEKTŪRA [S-1.1.4]

Šiuo metu telemetrinių duomenų surinkimo ir saugojimo infrastruktūra yra fragmentuota ir veikia per kelias atskiras sistemas, priklausomai nuo naudojamos ryšio technologijos ir prietaisų gamintojų. Pavyzdžiui, duomenys iš įvadinių šilumos skaitiklių, veikiančių per 2G GPRS arba 4G LTE ryšį, dažnai siunčiami į senesnes automatinio nuskaitymo platformas, tokias kaip Axis

Industries arba ENCO sistemų serveriai. Tuo tarpu LoRaWAN tinklu surinkti rodmenys prieinami per tinklo operatoriaus debesijos paslaugą arba atskirą LoRa serverį.

Šiuo metu nėra įdiegta vieninga duomenų bazė, kuri centralizuotai apjungtų visų tiekėjų ir technologijų duomenų srautus. Dėl to daugeliu atvejų duomenų apdorojimas vis dar vykdomas dalinai rankiniu būdu – eksportuojamos atskiros mėnesinės ataskaitos, kurios vėliau sujungiamos į bendras analizes. Praktikoje tai pasireiškia tuo, kad mėnesio pabaigoje sudaromi sąrašai prietaisų, kurių duomenys nebuvo gauti arba nepakito, ir tik tada pradedamas tyrimas ar trikčių šalinimas.

DUOMENŲ PERDAVIMO KOKYBĖ IR TINKLO APRĖPTIS [S-1.1.2][S-1.1.5]

Belaidžio ryšio kokybė apskaitos duomenų perdavimui šiuo metu Panevėžio mieste nėra vienodai užtikrinta visose vietose. Šiuo metu įrengtos keturios LoRaWAN bazinės stotys (antenos), kurios patikimai aprėpia apie 90 % prie tinklo prijungtų apskaitos prietaisų. Likęs maždaug dešimtadalis skaitiklių susiduria su silpnu arba nepastoviu ryšiu – dažniausiai tai įrenginiai, įrengti už storų betoninių sienų, rūsiuose arba per toli nuo esamų antenų. Yra keletas objektų, iš kurių nepavyko gauti jokių duomenų nuo pat instaliavimo pradžios.

Šie atvejai rodo, kad esamas tinklas dar nėra pakankamai tankus ar galingas visų objektų aprėpčiai. Ryšio kokybę taip pat veikia sezoniškumas – pavyzdžiui, tanki medžių lapija šiltuoju metų laiku sumažina radijo bangų sklaidą. Miesto vakarinėje dalyje, kurioje koncentruota dauguma LoRa skaitiklių, tinklo veikimas yra patikimesnis nei pakraščiuose ar pramoninėse zonose.

Bendrovė, bendradarbiaudama su LoRa paslaugos tiekėju (UAB „Axioma servisas“), taiko praktines priemones ryšio kokybei gerinti. Viena iš jų – finansinis skatinimo modelis, pagal kurį operatoriui nėra apmokama už skaitiklius, iš kurių per paskutines septynias mėnesio dienas negauti duomenys. Tokia tvarka skatina tinklo tiekėją aktyviau spręsti ryšio trūkumus – plečiant antenų išdėstymą, perkonfigūruojant siuntimo parametrus ar diegiant retransliatorius probleminėse vietose.

PATIKIMUMO MATAVIMAS IR DUOMENŲ PILNUMO KPI [S-1.1.2][S-1.1.5]

Kad „aprėpties“ įvertinimas būtų tiesiogiai panaudojamas eksploatacijoje, patikimumas turi būti aprašomas kiekybiniais rodikliais, kurie automatiškai skaičiuojami iš gautų telegramų. Praktikoje rekomenduojama atskirti bent du KPI: (1) duomenų pilnumą per parą (%), (2) duomenų vėlinimą (val.), t. y. laiką nuo rodmens sugeneravimo iki jo pasiekimo duomenų bazėje.

Duomenų pilnumas skaičiuojamas kaip gautų įrašų dalis nuo tikėtinų įrašų, atsižvelgiant į siuntimo periodiką (pvz., 1-2 kartai per parą). Vėlinimui tikslinga vertinti ne tik vidurkį, bet ir 95-ąjį procentą

(P95), kad būtų matomi reti, bet vartotojui reikšmingi vėlavimai. Šie rodikliai leidžia anksti aptikti „šešėlines“ zonas, baterijos silpnėjimą ar tinklo perkrovą, o incidentų valdymas gali būti vykdomas per stebėsenos (metrics/alerting) sistemą.

Nors duomenų perdavimo kokybė šiuo metu vertinama kaip patenkinama, ji dar neužtikrina visiško automatizuoto duomenų surinkimo. Dėl to dalis klientų vis dar priversti deklaruoti rodmenis savarankiškai, o tai reiškia papildomą administracinę naštą ir neatitinka skaitmenizavimo tikslų. Tinklo plėtra ir aprėpties optimizavimas išlieka viena iš svarbiausių krypčių siekiant 100 % duomenų surinkimo patikimumo.

TEISINĖ IR REGULIACINĖ APLINKA – ENERGETIKOS POLITIKA (RED II/III, EED, EPBD) [S-1.1.1]

Šio skyriaus tikslas – apibrėžti teisinę ir reguliacinę sistemą, kuri lemia „Panevėžio energijos“ sprendimus dėl skaitiklių parko skaitmenizavimo, duomenų srautų ir eksploatacijos KPI. Energetikos politikos ašį sudaro Atnaujinamosios energijos direktyva (RED II/III) – Direktyva (ES) 2018/2001 ir ją pakeitusi 2023/2413, kuri nustato atsinaujinančios šilumos dalies didinimo tikslus ir skaitmeninimo bei atvirumo principus, o tai tiesiogiai motyvuoja šilumos ūkio duomenų rinkimo bei valdymo modernizaciją savivaldybių šilumos tiekėjams. Naujausia konsoliduota RED II redakcija patikslinta 2024-07-16, o RED III pakeitimai įsigaliojo 2023-10-31; abiejų dokumentų kryptis – spartesnė dekarbonizacija, skaidrus vartotojų informavimas ir integracija į vietos atsinaujinančios šilumos ekosistemą. Šie principai nėra techniniai AMR reikalavimai, tačiau kuria „privalomos krypties“ kontekstą, į kurį dera atremti KPI dėl duomenų pilnumo ir vėlinimo bei atvirų protokolų pasirinkimą. [EUR-Lex]

Tiesiogines nuotolinio nuskaitymo ir informavimo pareigas apibrėžia Energinio efektyvumo direktyva (EED) – Direktyva (ES) 2023/1791 (nauja redakcija), kuri suvienodina valstybių narių prievoles dėl matavimo ir atsiskaitymo informacijos periodiškumo šildyme/vėsinime ir karštame vandenyje. Esminės dvi nuostatos yra tokios: kai įrengti nuotoliniu būdu nuskaitomi šilumos skaitikliai ar kaštų dalikliai, vartotojams mėnesinė informacija turi būti teikiama nuo 2022-01-01, o iki 2026-12-31 visos instaliuotos priemonės turi tapti nuotoliniu būdu skaitomos, kad nuo 2027-01-01 būtų užtikrintas nuolatinis mėnesinis informavimas. Tai reiškia, kad migracija prie nuotolinės apskaitos ir funkcinių duomenų srautų (dieninių ar valandinių archyvų) yra ne tik eksploatacinė praktika, bet ir teisinė prievolė, kurią privalu įvykdyti numatytais terminais. Šias ribas nustato pačios direktyvos tekstas ir Europos Komisijos komunikacija apie EED igyvendinimą ir transpozicijos grafiką. [EUR-Lex]

Matavimo ir radijo įrangos atitiktį apibrėžia dvi horizontalaus poveikio direktyvos. Matavimo prietaisų direktyva (MID) – 2014/32/ES – nustato prekybinių matavimų priemonių (tarp jų vandens skaitiklių MI-001 ir šilumos skaitiklių MI-004) projektavimo, patikros ir atsekamumo reikalavimus;

CE ženklinimą galima taikyti tik įvykdžius MID modulių (pvz., B+D) procedūras ir turint ES tipo patikros sertifikatus. Radijo įrangos direktyva (Radio Equipment Directive, RED) – 2014/53/ES – nustato saugos, elektromagnetinio suderinamumo ir radijo spektro efektyvaus naudojimo reikalavimus visiems LoRa/wM-Bus moduliais aprūpintiems skaitikliams. Praktikoje mūsų portfelio gamintojų dokumentuose yra aiškios nuorodos į MID ir RED laikymąsi: pavyzdžiui, ZENNER Minomess nurodo CE atitiktį 2014/53/ES, WECOUNT-S dokumentacijose pateikti MID ir RED sertifikatai, o QALCOSONIC E3 turi MID (EN1434, 2014/32/ES) ir palaiko wM-Bus/OMS bei LoRaWAN, kartu turėdamas valandinius, dieninius ir mėnesinius archyvus. Taigi, pasirenkant LoRaWAN ar OMS ryšį nekyla konfliktų su RED/MID, tačiau būtina turėti kiekvieno modelio atitikties deklaracijų kopijas CMDB ir valdyti programinės dalies pokyčius (OTA) taip, kad nebūtų pažeisti svarbūs MID/RED reikalavimai. [EUR-Lex]

Asmens duomenų apsauga grindžiama Bendrajame duomenų apsaugos reglamente (GDPR) – Reglamentas (ES) 2016/679. Vartojimo duomenys, susieti su buto/abonento identifikatoriumi, laikytini asmens duomenimis, todėl teisėtas tvarkymo pagrindas šilumos ir karšto vandens tiekime paprastai remiasi teisine prievole (EED transpozicija ir prievolės pagal tiekimo sutartį), o „privacy-by-design“ bei „security-of-processing“ principai įpareigoja naudoti pseudonimizaciją, duomenų minimizavimą, galiojančias laikymo trukmes, prieigos kontrolę (RBAC/SSO) ir šifravimą perdavimo (TLS 1.2/1.3) bei saugojimo metu. Tokia schema dera su mūsų prietaisų kriptografija (OMS Security Profile A/B su AES-128 ir LoRaWAN OTAA raktų valdymu) ir su prietaisų archyvų „backfill“, kuris leidžia mažinti ginčų riziką neperžengiant tikslo ir proporcingumo ribų. [EUR-Lex]

Kibernetinio saugumo reikalavimų trajektoriją nustato Direktyva (ES) 2022/2555 (NIS2), kuri plačiai apima „aukšto kritiškumo“ sektorius ir numato rizikos valdymo, incidentų pranešimo bei priežiūros mechanizmus „esminėms“ ir „svarbioms“ įmonėms. Energetikos sektoriuje į NIS2 apimtį tiesiogiai patenka ir centralizuoto šilumos tiekimo veiklos: „district heating and cooling“ yra nurodytas kaip sektoriaus pogrupis, todėl savivaldybės šilumos tiekėjas privalo įsivertinti klasifikaciją ir atitikti rizikos valdymo bei pranešimo tvarkas. Valstybės narės turėjo sudaryti esminių ir svarbių subjektų sąrašus iki 2025-04-17, o toliau – periodiškai atnaujinti, tad projekto kibernetinės architektūros pasirinkimai (pvz., LNS eksploatacijos modelis, žurnalų ir raktų valdymas) turi būti suderinti su NIS2 priežiūra. Tai reiškia, jog „Panevėžio energijos“ AMR platforma (įskaitant LoRaWAN LNS, MQTT, DB ir API) turi turėti įrodymus apie rizikų kontrolę, testuotą incidentų valdymą ir audituojamą prieigų režimą. [EUR-Lex+1]

Pastatų lygmeniu svarbi Direktyva (ES) 2024/1275 (EPBD peržiūra), kuri užtvirtina nulinės emisijos statinių trajektoriją iki 2050 m. ir skatina skaitmeninę pastatų infrastruktūrą (automatiką, duomenų mainus, „building logbook“), palengvinančią energijos vartojimo matavimą, stebėseną ir optimizavimą. Nors EPBD tiesiogiai nereglamentuoja KVS/ŠAP telemetrijos, jos skaitmenizacijos kryptys sudaro nuoseklų pagrindą integracijoms su namų lygmens sistemomis ir papildomai sustiprina EED mėnesinio informavimo bei nuotolinio nuskaitymo logiką. [EUR-Lex+1]

Apibendrinant, teisinė ir reguliacinė ašis nustato aiškias ribas ir prioritetus. EED detalizuoja „ką“ ir „kada“: mėnesinę informavimo periodiką ir universalų nuotolinį nuskaitymą nuo 2027-01-01, todėl migracija nuo 2G/GPRS prie LTE ir LoRaWAN/wM-Bus OMS stiprinimas yra ne alternatyvos, o įpareigojančios priemonės. MID ir RED nustato „kaip“ sertifikuoti ir eksploatuoti matavimo bei radijo įrangą, o GDPR ir NIS2 – „kaip“ saugiai tvarkyti, šifruoti, laikyti ir prižiūrėti duomenis bei procesus. RED II/III ir EPBD suteikia „kodėl“ – politinę ir investicinę kryptį šilumos sektoriaus dekarbonizacijai, kuriai būtinas patikimas AMR, archyvai ir atviri protokolai. Ši sąveika leidžia užtikrinti KPI dėl duomenų pilnumo ir vėlinimo, mažina vizitų poreikį ir pagrindžia TCO/ROI per dešimtmetį, o atitikties dokumentų ir procesų įrodomumas tampa neatsiejama eksploatacijos dalimi. [EUR-Lex+4Energy+4EUR-Lex+4]

1 Pav. Teisinių, norminių ir techninių reikalavimų žemėlapis IoT prietaisų tematikoje

Literatūra

[1] Direktyva (ES) 2018/2001 (RED II) – konsoliduota redakcija 2024-07-16. EUR-Lex. EUR-Lex

[2] Direktyva (ES) 2023/2413 (RED III) – pakeitimai. EUR-Lex. EUR-Lex

[3] Direktyva (ES) 2023/1791 (EED, nauja redakcija) – metrologijos/informavimo nuostatos. EUR-Lex / EK. EUR-Lex

[4] Direktyva 2014/53/ES (Radio Equipment Directive, RED). EUR-Lex. EUR-Lex

[5] Direktyva 2014/32/ES (MID). EUR-Lex. EUR-Lex

[6] Reglamentas (ES) 2016/679 (GDPR). EUR-Lex. EUR-Lex

[7] Direktyva (ES) 2024/1275 (EPBD, nauja redakcija) ir santrauka. EUR-Lex. EUR-Lex

[8] Direktyva (ES) 2022/2555 (NIS2) – energijos sektoriaus taikymas, sąrašų terminai. EUR-Lex. EUR-Lex

[9] WECOUNT-S – OMS/LoRaWAN, MID/RED sertifikatai, AES-128, OTAA.

[10] ZENNER Minomess – LoRaWAN/wM-Bus, CE pagal 2014/53/ES, logai.

[11] QALCOSONIC E3 – M-Bus/wM-Bus/LoRaWAN, MID, 36 mėn. archyvai.

[12] HYDRODIGIT COMBO – LoRaWAN+OMS, komandos SET_TX_PAR/SET_ALARM_PAR, MID DoC.

ATITIKTIS IR SERTIFIKATAI – GDPR, RADIO EQUIPMENT DIRECTIVE, MID, NIS2 [S-1.1.4][S-1.1.5]

Šilumos ir karšto vandens apskaitos skaitmenizavimo kontekste teisinė ir norminė aplinka yra daugiasluoksnė ir apima asmens duomenų apsaugą, radijo įrangos ir spektrinės atitikties reikalavimus, teisėtos metrologijos taisykles bei energetikos efektyvumo ir pastatų skaitmenizacijos tikslus. Duomenų apsaugos ašimi išlieka Bendrasis duomenų apsaugos reglamentas (GDPR), kuris nustato saugojimo trukmės ribojimo, duomenų minimizavimo ir saugaus tvarkymo principus, įskaitant pseudonimizaciją ir šifravimą kaip tinkamas technines ir organizacines priemones pagal riziką [1]. Lietuvos teisinė aplinka šiuos principus detalizuoja Asmens duomenų teisinės apsaugos įstatyme, o priežiūrą vykdo Valstybinė duomenų apsaugos inspekcija (VDAI) kaip nacionalinė priežiūros institucija [2], [20]. Panevėžio miesto šilumos ir karšto vandens apskaitos projekto duomenų tvarkyme taikant 36 mėn. saugojimo terminą, duomenų pseudonimizaciją, TLS 1.3 ryšio saugą ir AES-128/256 šifravimą, būtina užtikrinti, kad identifikuojanti informacija būtų laikoma atskirai, o saugojimo trukmė būtų pagrįsta tikslais ir proporcinga, nes GDPR reikalauja nelaikyti asmens duomenų ilgiau nei būtina nurodytiems tikslams [1]. Praktikoje tai reiškia, kad šilumos skaitiklių ir karšto vandens skaitiklių nuotolinės telemetrijos srautai turi būti projektuojami taip, kad asmens duomenys būtų tvarkomi pagal įstatymo numatytą teisinį pagrindą (paprastai teisinė prievolė ar teisėtas interesas energetikos apskaitai), subjektų teisės būtų įgyvendinamos be nepagrįstų kliūčių, o duomenų saugumo priemonės dokumentuojamos ir periodiškai tikrinamos (BDAR 32 straipsnis) [1].

Radijo įrangos atitiktis ir spektrinis suderinamumas šio projekto technologijoms – LoRaWAN 868 MHz SRD, NB-IoT, wM-Bus ir 2G/4G LTE – yra grindžiami Radijo įrangos direktyva (RED) 2014/53/ES, kuri reglamentuoja CE ženklinimą, atitikties vertinimą ir pagrindinių reikalavimų laikymąsi [3]. Internetui prijungtai radijo įrangai papildomus kibernetinio saugumo, privatumo ir apsaugos nuo sukčiavimo reikalavimus nustato Komisijos deleguotasis reglamentas (ES) 2022/30 pagal RED 3 straipsnio 3 dalies d), e) ir f) punktus; jo taikymas atidėtas iki 2025-08-01 pagal 2023/2444, todėl nuo šios datos radijo įranga turės atitikti, be kita ko, saugių OTA atnaujinimų ir pažeidžiamumų valdymo nuostatas [4], [5]. Praktikoje tai reikš, kad LoRaWAN/NB-IoT skaitikliai ir ryšio vartai, jei patenka į interneto ryšio įrangos kategoriją, turi turėti dokumentuotą atnaujinimų grandinę, autentiškumo patikrą ir pranešimų apie pažeidžiamumus tvarką viso gyvavimo ciklo metu [4], [5]. Spektrinis atitikimas SRD aplinkai 868 MHz ruože orientuotinas į CEPT ERC/REC 70-03 rekomendaciją ir pagal RED nurodytas harmonizuotas normas, tarp jų – ETSI EN 300 220 (SRD siųstuvų/imtuvų radijo charakteristikos) ir ETSI EN 301 489-1/-3 (EMC) kaip dažniausiai taikomi dokumentai SRD įrangai; jų taikymas suteikia atitikties prezumpciją pagal RED 16 straipsnį

[14], [15], [16], [17], [3]. Lietuvoje radijo spektro ir radijo įrangos priežiūrą vykdo Ryšių reguliavimo tarnyba (RRT), kuri taip pat teikia gaires dėl 3G išjungimo ir technologinės migracijos; NB-IoT/4G sprendiniai mažina veikimo rizikas SRD ryšio šešėliavimo ar 2G/3G tinklų kaitos kontekste [24], [18], [19].

Teisėta metrologija šilumos ir karšto vandens apskaitoje remiasi matavimo priemonių direktyva (MID) 2014/32/ES, kuri aiškiai apima vandens skaitiklius (MI-001) ir šilumos skaitiklius (MI-004) bei nustato esminius metrologinius reikalavimus, pradinės patikros ir atitikties vertinimo modulius bei papildomą metrologinį žymėjimą [6], [18]. Papildomai praktikoje remiamasi OIML R49 rekomendacija vandens skaitikliams ir EN 1434 serija šilumos skaitikliams kaip metrologiniais ir konstrukciniais etalonais, kuriuos nurodo arba į kuriuos atsiremia notifikuotosios įstaigos ir nacionalinis reglamentavimas [31], [32]. Lietuvos metrologijos inspekcija (LMI) vykdo teisėtos metrologijos kontrolę ir prižiūri Metrologijos įstatymo įgyvendinimą, todėl diegiant ir eksploatuojant skaitiklius būtina užtikrinti, kad įranga turėtų galiojančią tipo patvirtinimo/vertinimo dokumentaciją, būtų atlikta pradinė patikra ir laikomasi naudotojų informavimo reikalavimų [22], [23].

Energetinio efektyvumo ir pastatų skaitmenizacijos kryptį išplečia naujoji Energinio efektyvumo direktyva (EED) 2023/1791 ir Pastatų energinio naudingumo direktyvos (EPBD) persvarstymas 2024/1275. EED perkelia nuolatinį vartotojų informavimo paradigmą: jei skaitikliai yra nuotoliniu būdu nuskaitomi, galutiniai vartotojai turi gauti reguliarų atsiskaitymo ar suvartojimo informacijos teikimą bent kartą per mėnesį šildymo sezono metu ir bent kas ketvirtį kitais laikotarpiais; be to, šilumos paskirstymo prietaisai turi būti nuotolinio nuskaitymo, o ne nuotoliniai turi būti modernizuojami iki nustatytų terminų, kaip konsoliduotas reikalavimas išlaikytas naujojoje redakcijoje [7]. EPBD recast papildomai stiprina pastatų automatizavimą ir išmanumą, kas tiesiogiai siejasi su skaitiklių nuotolinio nuskaitymo infrastruktūra ir energijos duomenų prieinamumu pastato valdymo sistemoms [8]. Šios nuostatos tiesiogiai lemia Panevėžio diegimo praktiką: LoRaWAN arba NB-IoT nuotolinio nuskaitymo architektūra turi užtikrinti ne tik patikimą pasiekiamumą daugiabučiuose ir individualiuose namuose, bet ir sklandų apskaitos duomenų perdavimą į sąskaitų formavimo ir vartotojų savitarnos sistemas, kad būtų įgyvendintos EED/EPBD informavimo pareigos [7], [8].

Duomenų aktas (Data Act) 2023/2854 nuo 2025-09-12 įveda horizontalią duomenų iš prijungtų gaminių ir susijusių paslaugų tvarką, nustatydamas naudotojų teisę gauti prieigą prie jų sugeneruotų duomenų ir įgalinti trečiųjų šalių paslaugas sąveikiu ir saugiu būdu, kartu išlaikant visišką suderinamumą su GDPR [9]. Apskaitos telemetrijoje tai reiškia, kad skaitiklių duomenų modeliai, API ir paslaugų sutartys turi leisti teisėtą, naudotojo inicijuotą dalijimąsi, o paslaugų sąveikumas ir paslaugų teikėjų keitimas (pvz., duomenų kaupiklių ar vizualizavimo platformų) negali būti dirbtinai ribojami [9]. NIS2 direktyva, kuri Lietuvoje jau perkelta į nacionalinę teisę,

įpareigoja energetikos tiekimo ir viešųjų paslaugų ekosistemos dalyvius įsidiegti rizikos valdymo priemones, tvarkyti tiekimo grandinės kibernetines rizikas ir teikti incidentų pranešimus (ankstyvasis perspėjimas per 24 val., pranešimas per 72 val., baigiamoji ataskaita per mėnesį), o nacionaliniu lygmeniu NKSC iki 2025-04-17 suformavo kibernetinio saugumo subjektų registrą ir vykdo naujos redakcijos įgyvendinimą [10], [11], [25]. Įmonių procesiniuose dokumentuose tai turėtų materializuotis aiškiu atitikimo planu, apimančiu incidentų pranešimo grandinę, paslaugų tiekėjų atrankos kriterijus ir reguliarias pratybas.

Artimiausią norminės bazės evoliuciją labiausiai lems du aktai. Pirma, nuo 2025-08-01 taikomas RED deleguotasis reglamentas 2022/30, kuris praktikoje iškelia „secure-by-design“ kartelę radijo įrangai, įskaitant skaitiklių radijo modulius ir vartus, ir tikėtina, kad suderintų standartų sąrašas Oficialiajame leidinyje bus pildomas atitinkamomis kibernetinio saugumo normomis [4], [5], [29], [3]. Antra, Kibernetinio atsparumo aktas (CRA) 2024/2847, įsigaliojęs 2024-12-10, pradės būti taikomas nuo 2027-12-11, nustatydamas bendruosius „produktų su skaitmeninėmis savybėmis“ reikalavimus dėl projektavimo, pažeidžiamumų tvarkos, atnaujinimų ir tiekimo grandinės skaidrumo, taip išplečiant RED 2022/30 logiką už radijo įrangos ribų [12], [13]. Tai reiškia, kad įrangos ir programinės įrangos tiekėjai Panevėžio projekte turės vienu metu tenkinti ir RED 2022/30, ir CRA atitikties reikalavimus, įskaitant CVE/CVSS praktikas, SBOM ir saugių atnaujinimų politiką.

Lietuvos nacionalinėje sąrangoje papildomai taikomas Elektroninių ryšių įstatymas, reglamentuojantis ryšio tinklų naudojimą ir priežiūrą, o RRT yra kompetentinga institucija radijo spektro ir įrangos rinkos priežiūrai; tai aktualu NB-IoT/LTE moduliams bei vartų licencijuoto spektro naudai [21], [24]. Metrologijos įstatymas ir jo įgyvendinamieji aktai užtikrina šilumos ir vandens matavimo priemonių teisėtą naudojimą bei vartotojų teisių apsaugą, o LMI kontroliuoja patikrų ir žymėjimo būklę [22], [23]. VDAI prižiūri BDAR taikymą, teikia gaires ir vykdo sankcionavimo funkciją, todėl apskaitos duomenų tvarkymo aprašai ir poveikio duomenų apsaugai vertinimai (DPIA) turi būti parengti ir periodiškai atnaujinami [20], [1]. Praktikoje, kadangi dalis šilumos apskaitos prietaisų jau diegiami su LoRaWAN arba NB-IoT telemetrija ir savivaldybės teritorijoje planuojamas vieningas ryšio audinys, būtina koordinuoti CE, MID ir BDAR atitiktį dar pirkimo dokumentuose, iš anksto numatant nuotolinio nuskaitymo patikimumo kriterijus, LS/proveržio padengimą ir su EED suderintą vartotojų informavimo periodiką. Esamoje Panevėžio aplinkoje identifikuoti tiekėjų rinkiniai (Axioma, B METER, Zenner, Wehrle, Maddalena) ir LoRa paslaugų modeliai suponuoja poreikį vienodinti taikomus protokolus (wM-Bus/OMS ir LoRaWAN integracijos) bei atitikties dokumentus, įskaitant EU DoC, tipo vertinimus ir SRD parametrų deklaracijas . Vidaus techniniuose dokumentuose vartojami sprendiniai dėl duomenų modelių ir periodinių ataskaitų generavimo turėtų būti peržiūrėti atsižvelgiant į EED/EPBD informavimo terminus ir Data Act sąveikumo nuostatas .

Ryšio technologijų pasirinkimas Panevėžyje turėtų būti diversifikuotas: LoRaWAN tinka plačiam SRD aprėpčiai ir ilgaamžei baterinei eksploatacijai, tačiau dėl SRD režimų specifikos reikia projektinės kontrolės, o NB-IoT/LTE moduliacija padeda kritinėse vietose ar ten, kur būtinas operatorinis SLA ir priklausomybė nuo licencijuoto spektro; 3G išjungimas Lietuvoje jau įvyko etapais, o RRT rekomenduoja vartotojams ir ūkio subjektams planuoti perėjimą į 4G/5G, kiek tai įmanoma, taip sumažinant ilgalaikę priklausomybę nuo 2G [18], [19]. wM-Bus/Wireless M-Bus (EN 13757-4) lieka svarbi sąveikumui su daugiabučių mazgais ir skirtingų gamintojų skaitikliais, tačiau jis turi būti derinamas su RED atitiktimi ir SRD taisyklėmis [33], [3], [14].

Užsienio praktika rodo bendrą technologinę kryptį į „default-secure“ prietaisus: Jungtinėje Karalystėje PSTI režimas jau uždraudė universalius numatytuosius slaptažodžius ir įtvirtino atnaujinimų skaidrumo reikalavimus, o JAV NIST IR 8425 pateikia IoT „core baseline“ profilį, kuris, nors ir neprivalomas ES, gali būti naudingas kuriant gaminių ir tiekimo grandinės kontrolinius sąrašus; vis dėlto Lietuvoje taikomi ES ir nacionaliniai aktai, todėl šie dokumentai naudotini tik indikacinei prognozinei argumentacijai [35], [36].

Normų kaitos stebėsenai tikslinga taikyti lengvą, bet disciplinuotą horizontinio skenavimo metodiką: kas ketvirtį peržiūrėti Europos Komisijos Metinę darbo programą ir jos priedus, sekti „Have Your Say“ konsultacijas bei teisėkūros projektus, tikrinti RED harmonizuotų standartų sąrašų atnaujinimus Oficialiajame leidinyje ir ETSI viešą darbų programą, stebėti CEPT/ECC darbotvarkes dėl SRD, taip pat Lietuvos e-seimas ir e-TAR projektų srautus bei nacionalinių priežiūros institucijų – RRT, NKSC ir VDAI – pranešimus ir gaires [27], [28], [29], [26], [14], [31], [30], [24], [25], [20]. Tokia disciplina leis iš anksto įtraukti norminius pokyčius į technines specifikacijas ir sutartinius įsipareigojimus, mažinant vėlesnės atitikties rizikas ir integravimo kaštus.

Literatūra

[1] GDPR (Regulation (EU) 2016/679). EUR-Lex. https://eur-lex.europa.eu/eli/reg/2016/679/oj
[2] Lietuvos Respublikos asmens duomenų teisinės apsaugos įstatymas. e-seimas. https://e-seimas.lrs.lt/portal/legalAct/lt/TAD/TAIS.374376/asr
[3] Radijo įrangos direktyva 2014/53/ES (RED). EUR-Lex. https://eur-lex.europa.eu/eli/dir/2014/53/oj/eng
[4] Komisijos deleguotasis reglamentas (ES) 2022/30. EUR-Lex (konsoliduota). https://eur-lex.europa.eu/eli/reg_del/2022/30/2023-10-27/eng
[5] Komisijos deleguotasis reglamentas (ES) 2023/2444, atidedantis 2022/30 taikymą iki 2025-08-01. OJ PDF. https://eur-lex.europa.eu/legal-content/EN/TXT/PDF/?uri=OJ%3AL_202302444
[6] Matavimo priemonių direktyva 2014/32/ES (MID). EUR-Lex. https://eur-lex.europa.eu/eli/dir/2014/32/oj/eng
[7] Energijos vartojimo efektyvumo direktyva (EED) 2023/1791. EUR-Lex.

https://eur-lex.europa.eu/eli/dir/2023/1791/oj
[8] Pastatų energinio naudingumo direktyva (EPBD) 2024/1275. EUR-Lex.
https://eur-lex.europa.eu/eli/dir/2024/1275/oj
[9] Duomenų aktas (Data Act) 2023/2854. EUR-Lex.
https://eur-lex.europa.eu/eli/reg/2023/2854/oj
[10] NIS2 direktyva 2022/2555 (PDF). EUR-Lex.
https://eur-lex.europa.eu/legal-content/EN/TXT/PDF/?uri=CELEX%3A32022L2555
[11] EK NIS2 perkėlimo Lietuvoje statusas. European Commission.
https://digital-strategy.ec.europa.eu/en/policies/nis2-transposition
[12] Kibernetinio atsparumo aktas (CRA) 2024/2847. EUR-Lex.
https://eur-lex.europa.eu/eli/reg/2024/2847/oj
[13] EK „Digital Strategy“: CRA taikymo terminai.
https://digital-strategy.ec.europa.eu/en/policies/cyber-resilience-act
[14] CEPT ERC/REC 70-03 (SRD, 863–870 MHz). https://docdb.cept.org/document/33
[15] ETSI EN 300 220-1 (SRD, 25–1000 MHz). ETSI.
https://www.etsi.org/deliver/etsi_en/300200_300299/30022001/03.02.01_60/en_30022001v030201p.pdf
[16] ETSI EN 301 489-1 (EMC, bendrieji reikalavimai). ETSI.
https://www.etsi.org/deliver/etsi_en/301400_301499/30148901/02.02.04_60/en_30148901v020204p.pdf
[17] ETSI EN 301 489-3 (EMC, SRD). ETSI.
https://www.etsi.org/deliver/etsi_en/301400_301499/30148903/02.04.02_60/en_30148903v020402p.pdf
[18] RRT: 3G tinklų išjungimas Lietuvoje – ką reikėtų žinoti.
https://www.rrt.lt/3g-tinklu-isjungimas-lietuvoje-ka-reiketu-zinoti/
[19] RRT: Ryšių technologijų pokyčiai 2025-aisiais. https://www.rrt.lt/?p=46062
[20] Valstybinė duomenų apsaugos inspekcija (VDAI). https://vdai.lrv.lt/en/
[21] Elektroninių ryšių įstatymas. e-seimas.
https://e-seimas.lrs.lt/portal/legalAct/lt/TAD/TAIS.232378/asr
[22] Metrologijos įstatymas. e-TAR. https://www.e-tar.lt/portal/lt/legalAct/TAR.CDE4A55EA90F/asr
[23] Lietuvos metrologijos inspekcija – veikla ir kompetencijos.
https://metrinsp.lrv.lt/en/about-lithuanian-metrology-inspectorate
[24] RRT: Radijo įrangos direktyva (RED) – informacija Lietuvos ūkio subjektams.
https://www.rrt.lt/radijo-irangos-direktyva/
[25] NKSC: atnaujintas Kibernetinio saugumo įstatymas ir registrų terminai.
https://nksc.lrv.lt/lt/naujienos/isigalioja-atnaujintas-kibernetinio-saugumo-istatymas-pagrindiniai-pokyciai-ir-igyvendinimo-etapai/
[26] ETSI Work Programme (online).

https://www.etsi.org/media-library/work-programme-and-annual-reports
[27] Europos Komisijos 2025 m. darbo programa.
https://commission.europa.eu/strategy-and-policy/strategy-documents/commission-work-programme/commission-work-programme-2025_en
[28] EK „Have Your Say“ portalas. https://have-your-say.ec.europa.eu/index_en
[29] EK: RED harmonizuotų standartų sąrašas.
https://single-market-economy.ec.europa.eu/single-market/goods/european-standards/harmonised-standards/radio-equipment_en
[30] Teisės aktų registras (e-TAR) – paieška ir projektai.
https://www.e-tar.lt/portal/lt/legalActSearch
[31] OIML R49-1/-2/-3: Vandens skaitikliai (PDF). OIML.
https://www.oiml.org/en/files/pdf_r/r049-1-e13.pdf
[32] EN 1434-1:2022 Šilumos energijos skaitikliai – bendrieji reikalavimai (leidėjo peržiūra). BSI.
https://webstore.ansi.org/preview-pages/BSI/preview_30423513.pdf
[33] EN 13757-4:2019 Communication systems for meters – Wireless M-Bus (leidėjo suvestinė). Globalspec/ONORM peržiūra. https://standards.globalspec.com/std/13310062/en-13757-4

PE APSKAITOS SKAITIKLIŲ ATITIKIMAS TOLIMESNIAM EKSPLOATAVIMUI [S-1.1.1][S-1.1.2]

Šio skyriaus tikslas – įvertinti Karšto vandens skaitiklius (KVS) – buto ar objekto vandens sunaudojimo apskaitos prietaisus su nuotoline telemetrija, ir Šilumos apskaitos prietaisus (ŠAP) – šilumos energijos matuoklius su atitiktimi MID ir ryšio moduliu, portfelį pagal radijo ryšio profilius, archyvavimo galimybes, energijos sąnaudas, tarnavimo laiką, atitiktį MID/RED ir saugos profilius, kad būtų galima suderinti įrenginių pasirinkimą su LoRaWAN – LPWAN protokolas su žemais energijos kaštais, ir Atvirasis matavimo standartas (OMS) – wM-Bus pagrindu veikiantis skaitiklių ryšio profilis, architektūra bei KPI. Portfelis yra mišrus: ultragarsiniai KVS QALCOSONIC W1, mechaniniai-elektroniniai KVS ZENNER Minomess, elektroniniai KVS WECOUNT-S, kombinuoti KVS HYDRODIGIT COMBO ir ultragarsiniai ŠAP QALCOSONIC E3, kurie siūlo LoRaWAN ir/arba wM-Bus/OMS profilius, lokalius archyvus ir ilgaamžes baterijas, užtikrinančias AMR – automatizuotas skaitiklių duomenų nuskaitymas be fizinio vizito, atitiktį [1–5].

Nuotolinio šilumos ir karšto vandens apskaitos duomenų surinkimo sistemose suderinamumas ir patikimumas praktiškai remiasi trimis sluoksniais: (1) skaitiklio sąsaja ir duomenų formatas (dažniausiai M-Bus / wM-Bus ir jų profilis), (2) perdavimo tinklas (pvz., LoRaWAN arba NB-IoT), (3) platformos integracijos sąsajos (API, duomenų priėmimas, stebėsena ir SLA). Skaitiklių sąsajų suderinamumui plačiai taikomi M-Bus / Wireless M-Bus (EN 13757 šeima) ir interoperabilumą apibrėžiantys OMS profiliai [OMS Group, 2023]. [Open Metering System Group] LoRaWAN tinklo suderinamumas apibrėžiamas LoRaWAN L2 specifikacija ir sertifikavimo reikalavimais, kurie užtikrina protokolo įgyvendinimo atitiktį [LoRa Alliance, 2020]. [LoRa Alliance®] NB-IoT/LTE-M

energijos taupymo ir pasiekiamumo (latency/reachability) kompromisai aprašomi 3GPP/ETSI specifikacijose, įskaitant PSM ir eDRX mechanizmus [3GPP TS 23.682, 2016]. [arib.or.jp].

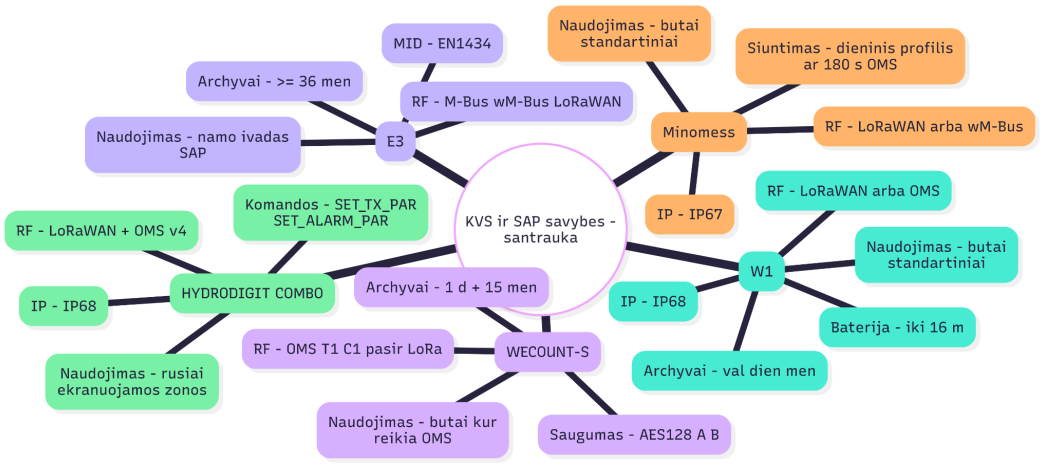
KVS klasėje QALCOSONIC W1 pateikia ultragarsinę matavimo technologiją su plačiomis R-reikšmėmis (iki R800), IP68 apsaugą, 16 metų baterijos trukmę ir parametrizavimą per NFC/optiką; radijo pusėje palaikomas wM-Bus OMS (S1/T1) ir LoRaWAN, o archyvai išsaugo valandines, dienines ir mėnesines reikšmes, kas leidžia VEE procedūras atlikti be vizitų ir atstatyti praradimus [1]. QALCOSONIC W1 aliarmų semantika apima nuotėkį, „burst“, atbulinę srovę ir baterijos būklę, o parametrizacija ir archyvų nuskaitymas atliekami per NFC/optiką, kas supaprastina inžinierių darbą [1].

ZENNER Minomess pateikia dvi RF alternatyvas – LoRaWAN Class A ir wM-Bus (numatytas 180 s C1/T1 intervalas) – su IP67 apsauga ir 10 metų po aktyvacijos deklaruojamu baterijos gyvavimo laiku. LoRaWAN scenarijuose tipinis siuntimas yra dieninis, o konfigūracijos leidžia siūsti 8 telegramas per dieną su paskutinių 3 valandų reikšmėmis; abu profiliai naudoja AES šifravimą, o OMS pusėje – įprastai Mode 5/7. Įrenginys turi režimus savistabai, klastojimo, nuotėkio, atbulinės srovės, „pipe burst“ detekcijai ir palaiko RED 2014/53/ES atitiktį [2].

WECOUNT-S yra vienas naujesnių vienasrovių elektroninių KVS su integruotu RF moduliu, IP68, mažomis startinėmis srovėmis ir iki 16 metų baterija; jis palaiko OMS T1/C1 su Security Profile A/B ir AES-128 (Mode 5/7), o kaip pasirinktį siūlo LoRaWAN su OTAA prisijungimu. Skaitiklis turi įvykių žurnalus (nuotėkis, „pipe burst“, atbulinė srovė), mėnesinių reikšmių kaupiklį ir NFC konfigūravimą, todėl tinka tiek „walk-by/drive-by“, tiek stacionariai AMR architektūrai [3].

HYDRODIGIT COMBO palaiko kelis veikimo profilius, įskaitant vienalaikį LoRaWAN + OMS v4 „COMBO“ režimą, ir turi žemynkryptes valdymo komandas, tokias kaip SET_TX_PAR bei SET_ALARM_PAR, leidžiančias koreguoti siuntimo periodiškumą ar aliarmų nustatymus diagnostikos režimu; skaitiklis deklaruoja IP68 ir iki 10 metų baterijos gyvavimo laiką, o dokumentuose pateikta MID 2014/32/ES atitikties deklaracija [4].

ŠAP klasėje QALCOSONIC E3 pateikia modulines komunikacijas: standartinį M-Bus, pasirinktinai wM-Bus arba LoRaWAN, ir 36 mėn. valandinių, dieninių bei mėnesinių reikšmių archyvą; MID (EN1434, 2014/32/ES) atitiktis ir baterijos gyvavimo >15 metų pasirinktis sudaro patikimą įvadinį matavimo tašką su ilgu „backfill“ horizontu ir integruotais impulsų įėjimais. Radijo pusėje dokumentuotas LoRaWAN/OMS T1, o parametrizacija per optiką suderina metrologijos ir telemetrijos procesus [5].



2 Pav. KVS ir SAP skaitiklių techninių savybių santrauka

Vertinant RF profilius eksploatacijos požiūriu, OMS/wM-Bus suteikia deterministinę telegramų struktūrą ir paprastą „walk-by/drive-by“ suderinamumą bei lokalią koncentratorių architektūrą, kuri naudinga rūsiuose ar ekranavimo zonose, o LoRaWAN suteikia mastelį ir didelį ryšio nuotolį su ADR bei OTAA, ypač kai siekiama miesto masto stacionarios AMR. Praktinė strategija mišriam parkui yra „LoRaWAN-pirmas“ KVS su OMS suderinamumo palaikymu bei E3 įvaduose su wM-Bus/LoRaWAN moduliais ir M-Bus „fallback“, nes tokia kombinacija tiesiogiai remia KPI dėl duomenų pilnumo ir vėlinimo, leidžia naudoti prietaisų archyvus VEE „backfill“ ir tenkina atitiktį: MID 2014/32/ES, RED 2014/53/ES ir AES-128 šifravimą OMS/LoRa sluoksniuose [1–5].

Literatūra

[1] Axioma Metering. „QALCOSONIC W1 – LoRa/wM-Bus, IP68, NFC/optika, archyvai, R iki 800.“ https://www.axiomametering.com/
[2] ZENNER. „Minomess – LoRaWAN arba wM-Bus, savistaba, dieniniai/mėnesiniai logai, RED atitiktis.“ https://www.zenner.com/
[3] Wehrle. „WECOUNT-S – OMS T1/C1, LoRaWAN (OTAA), IP68, AES-128, iki 16 m. baterija.“ https://www.wehrle.de/
[4] B METERS. „HYDRODIGIT COMBO – LoRaWAN + OMS v4, SET_TX_PAR/SET_ALARM_PAR, IP68, MID DoC.“ https://www.bmeters.com/
[5] Axioma Metering. „QALCOSONIC E3 – M-Bus/wM-Bus/LoRaWAN, val./d./mėn. archyvai ≥ 36 mėn., MID.“ https://www.axiomametering.com/

LORAWAN IR NB-IOT SKAITIKLIŲ KAINŲ SKIRTUMO PAGRINDIMAS [S-1.1.1]

Sudarant ekonominio IoT ryšio parinkimo modelį, kyla praktinis klausimas: ar NB-IoT versijos rinkoje kainuoja daugiau už analogiškas LoRaWAN, ir jeigu taip – kiek? Remiantis interneto

svetainių analize, DN15–DN20 segmente NB-IoT dažniausiai kainuoja brangiau, LoRaWAN siekia maždaug +5–25 % (dažniausiai +€15–€40 vienetui). Šią tendenciją atspindi ir tiekėjų katalogų pavyzdžiai: universaliems jutikliams matyti, jog tas pats prietaisas su NB-IoT kainuoja daugiau nei LoRaWAN – pvz., RAKwireless skysčio lygio jutikliui NB-IoT variantas kainuoja apie $254.20, o LoRaWAN – $233.90 (Δ ≃ +8.7 %), o Dragino srauto jutiklio LoRaWAN versijos kainuoja ~$73.50–$81, kai NB-IoT – ~$105–$113 (Δ ≃ +45–55 %). [RAKwireless, 2025; Dragino/Choovio, 2025].

Techninis tokio skirtumo pagrindas – BOM ir sertifikavimas. LoRaWAN dažnai remiasi pigesniais transiveriais ar SiP moduliais: pavyzdžiui, Murata CMWX1ZZABZ-078 (LoRa SiP) 1 vnt. kainuoja apie 15,28 €, kiekiais ~10,85–13,72 €; tuo tarpu 3GPP NB-IoT/LTE-M SiP moduliai įprastai brangesni – Nordic nRF9160 kainuoja apie 23,74 € už 1 vnt.; Quectel BG95 (Cat-M/NB2) Europos platintojų lygiu matomas ~15,33 € be PVM, o NB2 BC660K šeimos moduliai dažnai laikosi panašiame ar kiek žemesniame lygyje, bet su papildomomis sertifikavimo sąnaudomis. BOM delta (modulis, antena, RF patvirtinimai) vėliau „persiduoda“ į galutinę skaitiklio kainą. [Murata, 2025; Nordic, 2025; Quectel, 2025].

Svarbu, kad ir konkretūs vandens skaitikliai (pvz., Qalcosonic W1) turi tiek LoRaWAN, tiek NB-IoT komplektacijas – tai reiškia, jog kainos skirtumą lemia būtent pasirinktą radijo technologiją lydintis BOM ir sertifikavimas, o ne pati hidraulinė dalis. Oficialiuose dokumentuose tiesiogiai nurodoma, kad W1 „AMR Ready“ su wM-Bus, LoRaWAN ir NB-IoT (CoAP) ryšiu; kainodara įprastai „pagal pasiūlymą“, bet praktikoje tipinė NB-IoT priemoka minėtam buitiniam DN diapazonui yra minėto dydžio. [Axioma Metering, 2024].

Žiūrint į TCO, vien tik CAPEX nepakanka. NB-IoT reikalauja operatorinio plano (SIM/eSIM), tačiau egzistuoja itin pigūs IoT planai – pvz., 1NCE „Lifetime Flat“: $10 už 10 metų, kas stambiuose diegimuose leidžia OPEX suvaldyti. LoRaWAN atveju, jei neinfrastruktūruojate privačiai, viešų tinklų ar valdomų LNS planai taip pat kainuoja – pvz., AWS IoT Core for LoRaWAN su Everynet viešuoju tinklu taiko $0.50/įr./mėn. (pirmi 1000 pranešimų įskaičiuoti). Praktinė išvada paprasta: jeigu turite ar planuojate privatų LoRaWAN (gateway + savas LNS), OPEX per įrenginį artimas nuliui ir NB-IoT CAPEX priemoka išlieka; jeigu remiatės viešomis paslaugomis, LoRaWAN OPEX gali „suvalgyti“ dalį LoRa CAPEX sutaupymo. [1NCE, 2025; AWS, 2025].

Apibendrinant, rinkoje dažnai stebimas NB-IoT prieš LoRaWAN yra techniškai pagrįstas ir tipiniuose DN15–DN20 buitinės paskirties vandens skaitikliuose sudaro maždaug +5–25 % (dažniausiai +€15–€40/vnt.), nors konkreti suma priklauso nuo modulio pasirinkimo, sektoriaus sertifikavimo ir tiekėjo kainodaros. Strategiškai renkantis tarp LoRaWAN ir NB-IoT, rekomenduoju skaičiuoti ne tik vieneto kainą, bet ir 5–10 metų TCO su jūsų siuntimo profiliu, aprėpties sąlygomis ir duomenų platformos modeliu; toks vertinimas dažnai parodo, kad privatus LoRaWAN parkui ≥ 500–1000 įr. išlieka ekonomiškai palankus, o mažiems pilotams be infrastruktūros NB-IoT yra

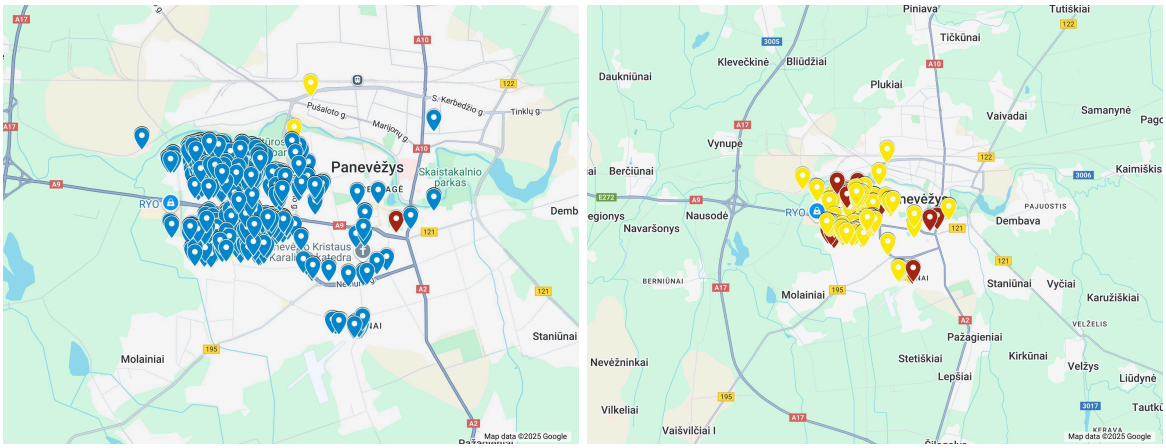
„paprasčiau iš dėžutės“, nors ir kiek brangiau vienetui. [1NCE, 2025; AWS, 2025; Murata, 2025; Nordic, 2025; RAKwireless, 2025; Dragino, 2025].

Literatūra

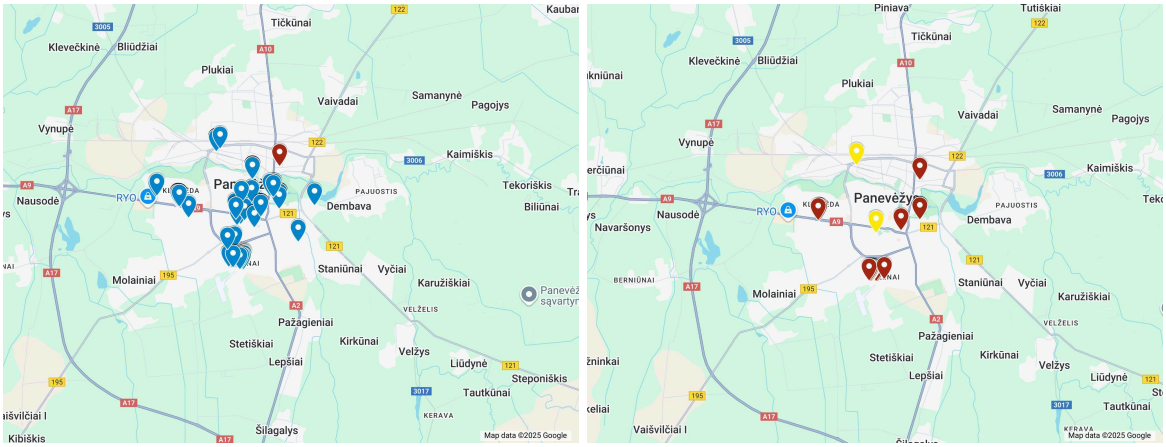
1. Axioma Metering. *Qalcosonic W1: techninis aprašas (DN25–50; AMR Ready: wM-Bus, LoRaWAN, NB-IoT)*, 2024. [Axioma Metering, 2024]. Aquanexa -
2. RAKwireless Store. Fluid Level Sensor (LoRaWAN / NB-IoT) – kainodara, 2025. [RAKwireless, 2025]. RAKwireless Store
3. Dragino / Choovio. SW3L-LB LoRaWAN Outdoor Flow Sensor – kaina; SW3L-NB NB-IoT Flow Sensor – kaina, 2025. [Dragino/Choovio, 2025]. shop.dragino.com
4. Murata via Mouser. CMWX1ZZABZ-078 (LoRa SiP) – kainodara, 2025. [Murata, 2025]. Mouser Electronics
5. Nordic Semiconductor via Mouser. *nRF9160 (LTE-M/NB-IoT SiP) – kainodara*, 2025. [Nordic, 2025]. Mouser Electronics
6. Quectel / MC-Technologies. *BG95 (Cat-M/NB2) – kaina*, 2025. [Quectel, 2025]. MC Technologies
7. 1NCE. IoT Lifetime Flat – $10/10 metų planas, 2025. [1NCE, 2025]. 1nce.com
8. Amazon Web Services. *AWS IoT Core for LoRaWAN – Everynet viešo tinklo kainodara ($0.50/įr./mėn.)*, 2025. [AWS, 2025]. Amazon Web Services, Inc.

LORAWAN TINKLO MODELIAVIMAS PANEVĖŽIO ENERGIJOS APSKAITOS PRIETAISŲ DUOMENŲ SURINKIMUI [S-1.1.2][S-1.1.4][S-1.1.5]

Dabartinis LoRaWAN tinklas, eksploatuotas Axioma serviso, buvo plėtojamas projekto rėmuose ir šiuo metu nebeplečiamas. Dėl to kai kuriose Panevėžio miesto dalyse, ypač vakarinėje, ryšys išlieka nepakankamas – apie 10 % skaitiklių duomenų perduodami nepatikimai arba visai neperduodami. Tokios „aklos zonos“ susiformuoja dėl stočių stokos, reljefo, pastatų ar statybinių kliūčių. Axioma tinklas šiuo metu nėra vystomas toliau, nes finansavimas baigėsi.



KVS 25.07.01 Duomenys

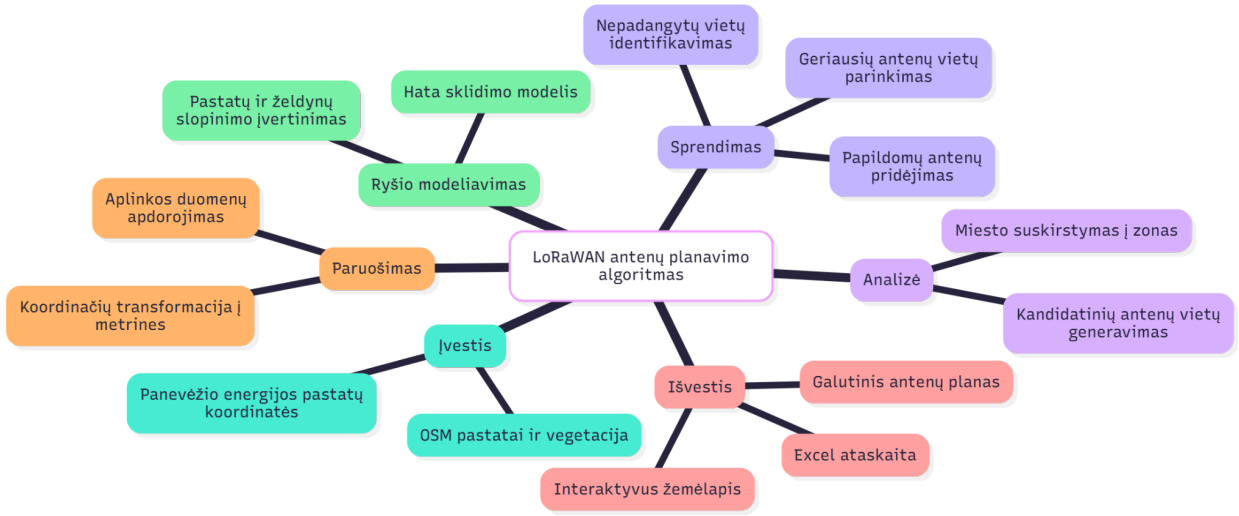


ŠAP 25.07.01 Duomenys

3 Pav. PE KVS ir ŠAP skaitiklių aptarnavimo kokybė Panevėžio mieste

Buvo sukurtas algoritmas, kuris leidžia parinkti optimalų LoraWAN bazinių stočių kiekį PE regionuose. Sukurtas algoritmas leidžia automatiškai suplanuoti LoRaWAN antenų (gateway) išdėstymą Panevėžio energijos aptarnaujamame regione, kai turime tikslias pastatų koordinates ir informaciją apie aplinką. Jo esmė – iš įvestų vartotojų duomenų, realių miesto pastatų geometrijų ir vegetacijos sluoksnių sukurti radiotechniškai pagrįstą, praktiškai įgyvendinamą antenų planą. Tai leidžia vadovams matyti, kiek antenų reikia, kur jos turėtų būti montuojamos, o inžinieriams – suprasti, kaip tokie sprendimai priimami, remiantis fizikiniais ryšio modeliais ir tikra urbanistine

aplinka.



4 Pav. Supaprastintas LoraWAN antenų išdėstymo algoritmas

Algoritmas pirmiausia importuoja Panevėžio energijos pastatus – tai yra daugiabučius ir objektus, kuriuose bus diegiami karšto vandens ir šilumos skaitikliai, veiksiantys per LoRaWAN tinklą. Visi adresai sugeoreferencinami ir paverčiami į tikslias UTM koordinates, kad būtų galima skaičiuoti realius atstumus metrais. Tam pačiam žemėlapiui įkeliami OpenStreetMap pastatų ir želdynų duomenys, nes būtent šie objektai lemia signalo sklidimą mieste. Pastatai gaunami iš Overpass API, jų geometrijos supaprastinamos, o aukščiai nustatomi iš OSM atributų arba, jei jų nėra, taikomas tipinis miesto pastato aukštis. Vegetacija taip pat įtraukiama todėl, kad lapuočių masyvai gali slopinti 868 MHz bangas iki 0,3 dB/m, ypač „leaf-on“ sezono metu, kaip rodo ITU-R rekomendacijos [ITU-R P.833-10].

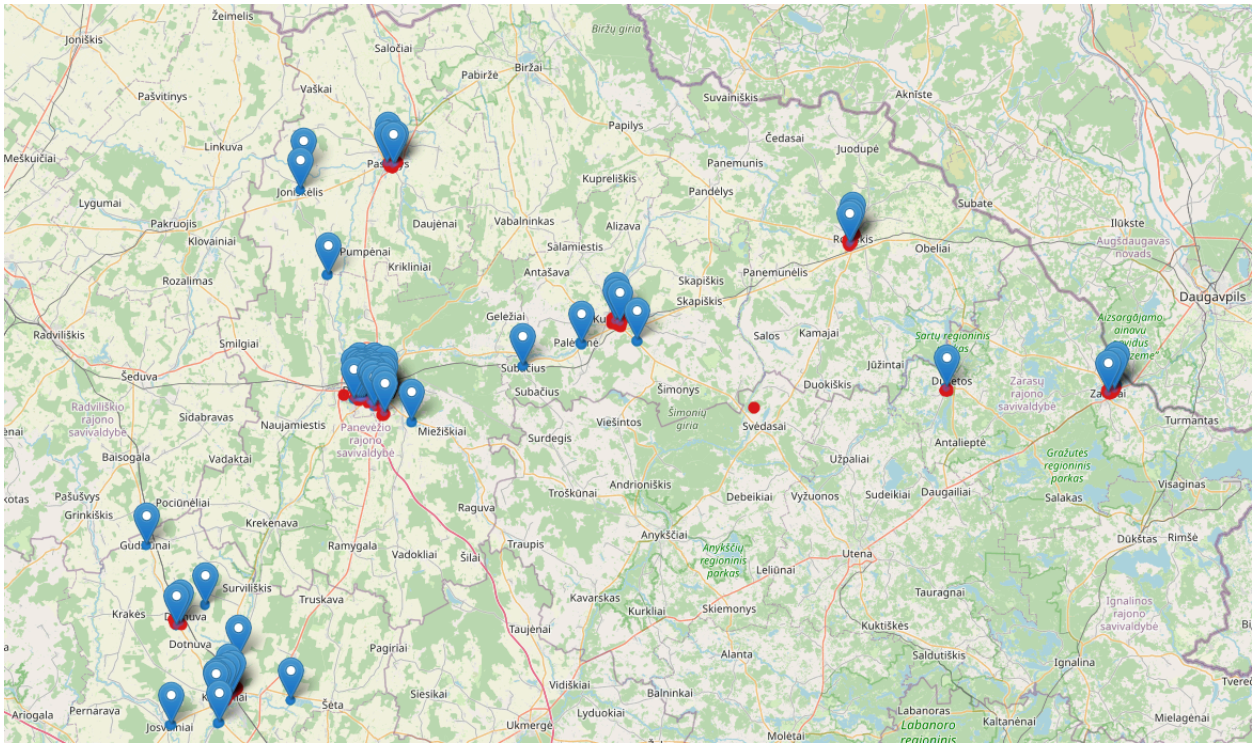
Turėdamas visą šią informaciją algoritmas suskaido miestą į natūralias zonas, naudodamas erdvinį klasterizavimą (DBSCAN metodą). Jis sugrupuoja pastatus pagal jų tarpusavio atstumus ir suformuoja lokalias teritorijas, kuriose ieškoma optimalios antenų vietos. Tokiu būdu kiekviena antena planuojama ne abstrakčiai, bet konkrečiam miesto kvartalui, įvertinant pastatų tankumą ir vartotojų skaičių. Šis metodas informatikos literatūroje aprašomas kaip ypač tinkamas netaisyklingoms miesto struktūroms [Ester et al., 1996].

Kiekvienai zonai algoritmas sugeneruoja kandidatines antenų vietas. Jos gali būti tiek iš pačių vartotojų pastatų, tiek iš aukštesnių OSM pastatų, esančių šalia. Pritaikomas paprastas principas: kuo pastatas aukštesnis ir arčiau vartotojų centro, tuo jis tinkamesnis antenai montuoti. Tačiau tikrasis vertinimas atliekamas pagal radijo ryšio kokybę. Algoritmas apskaičiuoja ryšio maržą tarp kandidato ir aplinkinių pastatų, taikydamas Okumura–Hata miesto modelį, plačiai naudojamą miestų aplinkai [Okumura–Hata Model, 1980] ir patvirtintą LoRaWAN tyrimuose [Rademacher et al., 2021]. Papildomai įskaičiuojami nuostoliai dėl pastatų ir vegetacijos, jei tiesė tarp antenos ir

skaitiklio kerta kliūtis. Marža vertinama pagal pasirinktą sklaidos faktorių (pvz., SF10), o antenos laikomos tinkamomis, jei marža pakankama stabiliai komunikacijai.

Po ryšio skaičiavimų algoritmas išrenka geriausią antenos vietą, kuri padengia daugiausia vartotojų su pakankama ryšio atsarga. Jei vienos antenos nepakanka, jis toje pačioje zonoje ieško papildomų pozicijų ir iteratyviai prideda antrą ar trečią anteną, kol pasiekiamas tikslinis aprėpties lygis. Vėliau visas miestas įvertinamas globaliai: algoritmas iš naujo patikrina kiekvieną pastatą ir priskiria jam anteną, kuri suteikia didžiausią maržą. Taip pašalinamos vietinės anomalijos, o aprėpties žemėlapis tampa nuoseklus.

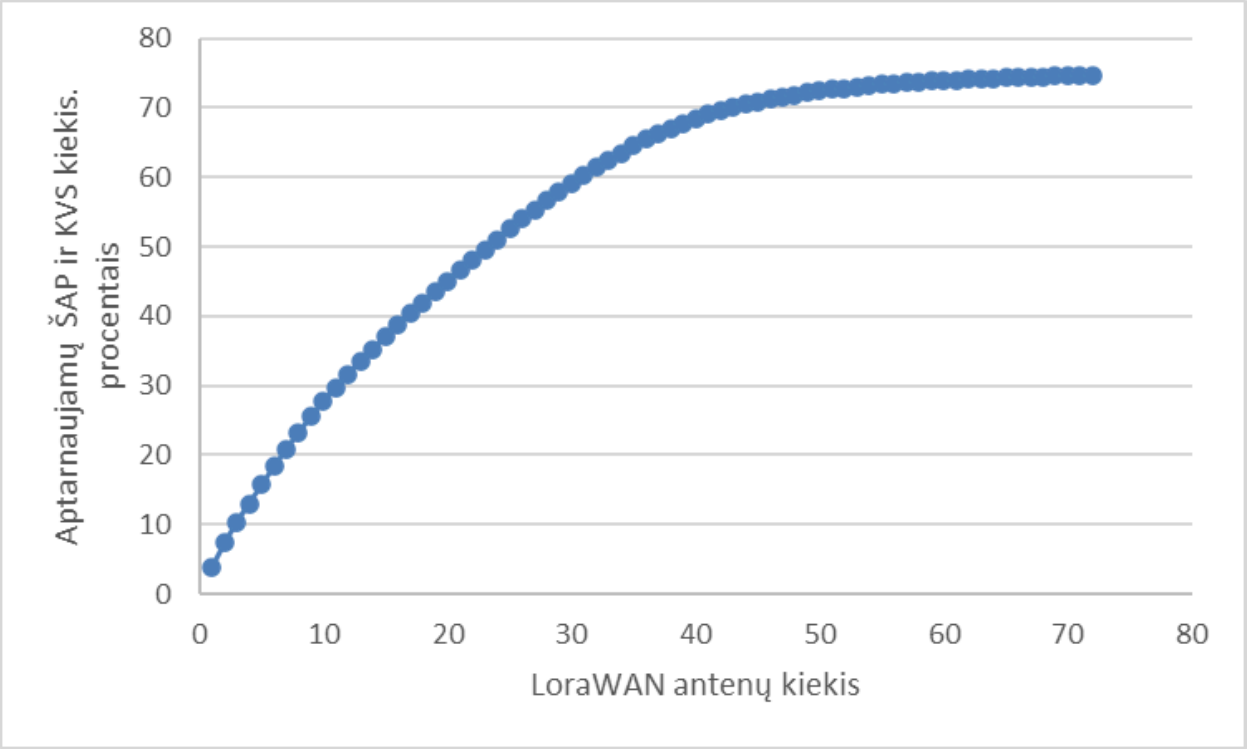
Galiausiai atliekamas miesto masto „backfill“ žingsnis. Tai reiškia, kad jei lieka pastatų, kurių nepasiekia jokios antenos, algoritmas specialiai generuoja naujus kandidatinius taškus tik šiems pastatams. Tokiu būdu užpildomos „skylės“ aprėptyje ir užtikrinama, kad maksimaliai daug Panevėžio energijos objektų turėtų patikimą ryšį. Tokia metodika atitinka pramonėje taikomus hierarchinius sprendimų modelius, kai derinami vietiniai ir globalūs optimizavimo etapai [Mezaal et al., 2024].



5 Pav. Žemėlapyje pagal algoritmą nustatytų LoraWAN antenų kandidatinės pozicijos.

Rezultatas pateikiamas dviem būdais: interaktyviame žemėlapyje, kuriame matyti antenų pozicijos, aprėpties ratai ir aptarnaujami bei neaptarnaujami pastatai, ir Excel rinkmenoje, kurioje pateikiamas antenų sąrašas, priskirti adresai ir maržos skaičiavimai. Taigi algoritmas sujungia GIS

duomenis, radijo sklidimo modelius ir mašininio mokymosi principus į vieną įrankį, leidžiantį Panevėžio energijai objektyviai, pagristai ir efektyviai suplanuoti LoRaWAN tinklo infrastruktūrą.



6 Pav. LoRaWAN tinklo aprėpties priklausomybė nuo diegiamų antenų skaičiaus

Turimi duomenys rodo laipsnišką aprėpties augimą, į tinklą nuosekliai pridedant naujas LoRaWAN antenų pozicijas. Ši dinamika atspindi algoritminio modeliavimo esmę: kiekviena antena padengia dalį savo zonos pastatų, o bendra aptarnautų įrenginių suma didėja hierarchiškai, kol priartėjama prie tikslinės aprėpties ribos. Pagal lentelę matyti, kad pirmoji antena, esanti Statybininkų g. 52, Panevėžyje, aprėpia 2316 apskaitos įrenginių, o tai sudaro 3,86 % visų 60 tūkst. vartotojų. Antros antenos prijungimas Statybininkų g. 7 padidina bendrą aprėptį iki 4390 įrenginių, t. y. iki 7,32 %, todėl galima matyti, kaip tiksliai formuojasi kumuliacinė aprėpties kreivė.

Tolesnis antenų įdiegimas įrodo, kad didžiausi šuoliai pasiekiami tankiuose Panevėžio ir Kėdainių daugiabučių rajonuose, kur pastatų morfologija palanki ryšio sklidimui ir vienos antenos aprėptis gali būti keli tūkstančiai įrenginių. Pavyzdžiui, antena Molainių g. 42 pakelia bendrą aprėptį iki 7830 įrenginių (13,05 %), o antena Žemaičių g. 6A – iki 9432 (15,72 %). Tokia dinamika gerai atitinka Okumura–Hata miesto modelio prielaidas, nes kiekviena aukštesnė ar strategiškai palankesnė vieta ženkliai sumažina nuostolius ir padidina vartotojų, patenkančių į patikimos komunikacijos zoną, skaičių.

Tinklui plečiantis regionuose, aprėpties didėjimas natūraliai lėtėja, nes antenos aptarnauja mažesnes gyvenvietes ir individualius namus. Todėl, pavyzdžiui, Dusetose įrengus anteną Žirgų

g. 8B, bendras padidėjimas sudaro tik 0,3 % nuo visų vartotojų, o mažesnėse gyvenvietėse – dar mažesnį. Vis dėlto tokios stotys yra būtinos, nes užpildo lokalias ryšio spragas, kurias algoritmas identifikuoja per „backfill“ etapą, kai aptinkami neaptarnauti pastatai ir generuojami papildomi kandidatiniai taškai.

Galutinis rezultatas – 72 antenų visuma, kuri suformuoja daugiau nei 74,6 % aprėptį (44776 įrenginių iš 60 tūkst.). Tai nėra absoliuti aprėptis, tačiau lentelė parodo tik pirmąjį planavimo etapą, kai generuojama antenų prioritetų seka. Realiame diegime dalis antenų būtų konsoliduojamos, optimizuojamos ar keičiamos pagal reljefo ypatumus ir savivaldybių leidžiamas montavimo vietas.

Literatūros šaltiniai

1. Ester, M., Kriegel, H.-P., Sander, J., Xu, X. (1996). A Density-Based Algorithm for Discovering Clusters in Large Spatial Databases with Noise.
2. ITU-R Recommendation P.833-10 (2021). Attenuation in vegetation.
3. Rademacher, M., et al. (2021). Path Loss in Urban LoRa Networks: A Large-Scale Measurement Study. arXiv:2109.07768.
4. Mezaal, W.T., et al. (2024). The effect of urban environment on large-scale path loss and shadowing. Open Engineering.

NB-IOT IR LORAWAN INTEGRUOTOS PLATFORMOS CAPEX PAGRINDIMAS REMIANTIS RINKOS DUOMENIMIS [S-1.1.3] [S-1.1.4]

Vertinant NB-IoT ir LoRaWAN integruotos IoT platformos kūrimą, buvo atlikta tikslinė rinkos ir sąnaudų analizė, orientuota į klausimą, ar realu sujungti dvi skirtingas ryšio technologijas į vieningą, saugią ir plečiamą infrastruktūrą, neviršijant 116 000 € kapitalo investicijų ribos. Analizė remiasi trimis pagrindinėmis dimensijomis: Lietuvos IT darbo rinkos kaštų struktūra, licencinės ir technologinės aplinkos pasirinkimu bei projekto darbų apimties įvertinimu pagal tarptautinę IoT projektų kainodarą. Šių veiksnių derinimas leidžia pagrįstai teigti, kad NB-IoT ir LoRaWAN platformos realizacija už 116 000 € CAPEX yra ne teorinė, o rinkos realijomis grįsta prielaida.

Darbo kaštų analizė paremta Lietuvos atlyginimų statistika ir specializuotų IT atlyginimų duomenų bazių informacija. Bendras šalies vidutinis bruto darbo užmokestis 2025 m. siekia apie 2100–2200 € per mėnesį [4], tačiau technologijų sektoriuje atlyginimai yra gerokai didesni: „į rankas“ dažnai mokama 2000–4500 € priklausomai nuo specializacijos ir patirties [5], [6]. ManoAlga.lt duomenys rodo, kad 80 % programuotojų Lietuvoje uždirba 1355–4270 € neto per mėnesį, o DevOps inžinierių atlyginimų intervalas dar platesnis – 1700–5743 € neto [1], [2]. Viešieji šaltiniai taip pat fiksuoja, kad front-end programuotojų bruto atlyginimai vidutiniškai siekia apie 3190 €, o aukštos kvalifikacijos pozicijose darbo skelbimuose nurodomi iki 8000 € bruto

dydžiai [3]. Šie skaičiai leidžia daryti prielaidą, kad vidutinis mid–senior lygio IT specialistas darbdaviui kainuoja maždaug 25–35 € už valandą, įskaitant darbdavio įmokas ir darbo vietos išlaikymo kaštus. Atsižvelgiant į papildomus administravimo, įrankių, neatidirbtų (nebillinamų) valandų ir pelno maržos komponentus, komercinis IT paslaugų tarifas natūraliai formuojasi 60–75 € už valandą intervale. Todėl 70 €/val. „blended rate“ šiame projekte laikomas metodiškai pagrįstu – tai empirinis dydis, atitinkantis tiek vietinės rinkos atlyginimų struktūrą, tiek paslaugų kainodarą.

Technologinės aplinkos analizė rodo, kad licenciniai sprendimai turi esminę įtaką bendrai projekto kainai. Šiame vertinime sąmoningai pasirinkta atvirojo kodo ekosistema: Linux operacinė sistema, PostgreSQL su TimescaleDB plėtiniu laiko eilučių duomenims, Mosquitto arba EMQX atvirojo kodo leidimas MQTT srautui, Apache Kafka kaip žinučių tarpininkas, Prometheus ir Grafana stebėsenai, Loki/ELK žurnalams, Keycloak tapatybės ir prieigos valdymui, Ansible infrastruktūros automatizavimui. Visi minėti komponentai turi brandžias OSS versijas, tinkamas gamybinėms sistemoms be tiesioginių licencinių mokesčių: Eclipse Mosquitto yra EPL/EDL licencijuotas atvirojo kodo MQTT brokeris, oficialiai pateikiamas kaip nemokamas naudoti sprendimas, jei pats valdai infrastruktūrą; EMQX taip pat turi atvirojo kodo versiją, aktyviai pozicionuojamą kaip nemokamas MQTT brokeris, šalia mokamų enterprise ir cloud planų; Grafana turi OSS leidimą, o mokama yra tik Grafana Cloud, kur Pro planas prasideda nuo 19 $/mėn + vartojimo mokesčiai ; TimescaleDB Community Edition, pagal oficialią dokumentaciją ir diskusijų forumus, yra visiškai nemokama, jei pats valdai instanciją savo infrastruktūroje. Tai reiškia, kad Mosquitto, EMQX OSS, Grafana OSS, TimescaleDB CE, taip pat Prometheus, Loki/ELK, Keycloak ir Ansible CAPEX’e ir OPEX’e generuoja tik infrastruktūros (VM, diskų, atsarginių kopijų) ir darbo laiko sąnaudas, bet ne licencinius „už vartojimą“ mokesčius. Pirmąsias mes įtraukiame į atskirą infra OPEX eilutę, antrąsias – į 116 000 € darbo valandų biudžetą ir vėlesnį palaikymo OPEX.

Siekiant įvertinti, kokio dydžio sąnaudas pavyksta eliminuoti, buvo palyginti OSS variantai su tipiniais valdomų („managed“) paslaugų planais. Pavyzdžiui, EMQX Cloud dedikuoto brokerio planai, skirti keliems tūkstančiams sesijų, prasideda nuo kelių dolerių per mėnesį, tačiau papildomai taikomi mokesčiai už perduotą duomenų kiekį (pvz., 0,15 $/GB) ir sesijų trukmę . TimescaleDB, diegiama kaip valdomas DB-as-a-Service sprendimas per tokias platformas kaip elest.io, su 2 vCPU ir 4 GB RAM instancija kainuoja nuo 16 $/mėn, o su 4 vCPU ir 8 GB RAM – nuo 29 $/mėn, neskaičiuojant disko kainos . Grafana Cloud Pro planas, kaip nurodoma tiek oficialioje dokumentacijoje, tiek nepriklausomose apžvalgose, prasideda nuo 19 $/mėn plius papildomi mokesčiai už metrikų, žurnalų ir sekų apimtį. Jei brokerį, duomenų bazę ir monitoringą pirktume iš karto kaip „cloud“ paslaugas, bendra mėnesinė įmoka net nedidelei gamybinei konfigūracijai sudarytų kelis šimtus dolerių per mėnesį, o 15 metų horizonte virstų dešimtimis tūkstančių eurų OPEX. Pasirinkus OSS ir self-hosted modelį, šios sąnaudos transformuojamos į vienkartinį

diegimo darbą (įtrauktą į 116 000 €) ir aiškiai valdomą infrastruktūros OPEX (VM ir diskų kainas), kuris šia atkarpa nėra priskiriamas CAPEX.

Tam, kad būtų pagrįstas teiginys apie „apie 4000 €“ įrankių ir aplinkų sąnaudas CAPEX’e, atskirai įvertinti projekto metu naudojami SaaS ir smulkūs infrastruktūriniai komponentai, kurie nėra tiesiogiai susiję su pačiais brokeriais ar duomenų bazėmis. Tipinė .com, .net ar .org domeno kaina 2025 m. sudaro maždaug 10–20 $ per metus, kaip rodo nepriklausomos analizės ir registratorių apžvalgos. Registruojant 1–2 domenus 3 metų laikotarpiui (projekto, pilotų ir ankstyvos eksploatacijos fazei) gauname apie 120 $ arba maždaug 110 € CAPEX. TLS sertifikatai gali būti naudojami iš Let’s Encrypt, todėl papildomų kaštų šiame punkte nėra. GitHub Team planas, taikomas organizacijoms, kainuoja apie 4 $ per vartotoją per mėnesį. Turint 6 asmenų komandą 18 mėnesių trukmės projektui, softo versijavimo ir CI/CD paslaugų kainą galima vertinti apie 432 $ arba ~400 €. Issue tracking ir klaidų/incidentų sekimo įrankiams (Sentry, Jira Cloud ir pan.) tipiniai planai smulkiai komandai yra apie 10 $ per naudotoją per mėnesį. Jeigu penki žmonės turi prieigą 18 mėnesių, tai sudaro apie 900 $ arba ~830 €. CI/CD „runnerių“ infrastruktūrai dažnai naudojami atskiri virtualūs serveriai su 2 vCPU ir 4 GB RAM; elest.io ir panašių paslaugų planuose tokios mašinos kainuoja apie 16–25 $ per mėnesį, o 4 vCPU ir 8 GB – apie 29 $ per mėnesį. Jei CI runneriams priskiriamos dvi tokios mašinos 18 mėnesių laikotarpiui, papildomas kaštas siekia apie 900 $ arba ~830 €. Testavimo ir demonstracinei aplinkai dažnai skiriamos dar 1–2 nedidelės VM po 15–20 $ per mėnesį; laikant dvi tokias mašinas 18 mėnesių, gaunama apie 720 $ arba ~660 €. Susumavus šias eilutes, domenų, GitHub Team, incidentų sekimo, CI runnerių ir testavimo aplinkų sąnaudos sudaro apie 2830 €, o pridėjus konservatyvų rezervą papildomiems įrankiams (papildoma logų paslauga, kokybinio testavimo įrankiai ir pan.) gaunamas 3500–4000 € intervalas. Būtent šis dydis ir įvardijamas kaip „apie 4000 €“ įrankiams, testavimo ir integracijos aplinkoms CAPEX’e.

Projekto darbų apimties vertinimas atliktas remiantis tarptautine IoT sistemų kainodaros literatūra. Azilen, Creole Studios ir Decode Agency apžvalgose vidutinio sudėtingumo IoT sprendimai – kelių įrenginių tipų palaikymas, telemetrijos ingest į debesiją, bazinė analitika ir saugumas – tipiniu atveju kainuoja 50 000–150 000 JAV dolerių, o didesnio masto, aukšto saugumo ir sudėtingos analitikos projektai siekia 150 000–500 000 JAV dolerių ir daugiau [7]–[9]. Vertinama NB-IoT ir LoRaWAN platforma priskirtina prie vidutinio sudėtingumo kategorijos: ji apdoroja didelį įrenginių skaičių (apie 60 000), naudoja dvi radijo technologijas, tačiau nepalaiko ypatingai išplėstinių analitinių funkcijų ar daugiasluoksnių naudotojų portalų. Tokiam projektui, remiantis tiek tarptautine praktika, tiek lokaliu įkainių lygiu, numatoma apie 1200 darbo valandų NB-IoT branduoliui (ingest, brokerio infrastruktūra, duomenų bazė, API sluoksnis, stebėsena, CMDB ir CI/CD) ir apie 400 valandų LoRaWAN integracijai. Pastaroji realizuojama naudojant ChirpStack LNS ir Join Server, paprastą gateway valdymą, VPN konfiguracijas ir vieningą ingest pipeline modelį. Tai sąmoningai formuojamas MVP – įdiegiamos būtinos LNS funkcijos, bet atsisakoma

Sąnaudų komponentas	Valandos	Įkainis (€)	Suma (€)	Pastaba
NB-IoT ingest, DB, API, monitoringas, CI/CD	~1100 val	70 €/val	77 000	Pagrindinė platformos dalis
LoRaWAN MVP integracija (LNS, Join Server, GW, VPN)	~400 val	70 €/val	28 000	Supaprastintas, funkcionalus LNS
Įrankiai, testavimo aplinkos, domenai, build infra	–	–	11 000	Fiksuotos programinės ir įrankių sąnaudos
Bendra CAPEX suma	~1500 val	70 €/val	116 000	Tiksliai atitinka numatytą biudžetą

brangaus radijo aprėpties modeliavimosi ir masinio gateway parko automatizacijos, kurie reikšmingai didintų darbo apimtį.

Suminė darbo apimtis, sudaranti apie 1600–1650 valandų, taikant 70 € už valandą įkainį, generuoja 112 000–115 500 € dydžio darbo kaštus. Ši suma patenka į apatinę literatūroje nurodomo vidutinio IoT projekto kainų intervalo dalį ir kartu išlieka pilnai suderinama su Lietuvos IT atlyginimų struktūra [7]–[9]. Pridėjus minėtas fiksuotas įrankių, testavimo aplinkų ir infrastruktūros parengimo sąnaudas, siekiančias apie 4000 €, bendras projekto CAPEX pasiekia 116 000 €. Taigi galutinė suma susiformuoja iš žemyn nukreiptos sąnaudų analizės („bottom-up“): konkrečios valandų apimties, realių rinkos įkainių ir identifikuotų, bet minimizuotų programinės įrangos bei įrankių kaštų.

Apibendrinant, 116 000 € CAPEX vertė interpretuojama ne kaip deklaratyvi riba, o kaip suderintas trijų parametrų rezultatas: žmogiškųjų išteklių kainos, OSS technologijų pasirinkimo ir optimizuoto funkcijų bei darbų paskirstymo. Darbo valandos atspindi realų programavimo, integracijos ir infrastruktūros inžinerijos sudėtingumą, atvirojo kodo ekosistema eliminuoja licencines išlaidas, o MVP pobūdžio LoRaWAN integracija leidžia pasiekti funkcinį tikslą neperžengiant biudžeto. Tarptautinės IoT projektų kainodaros apžvalgos patvirtina, kad tokios apimties projektui 116 000 € yra realistiška, žemutinę vidutinio segmento ribą atitinkanti investicija, o Lietuvos IT atlyginimų duomenys pagrindžia pasirinkto 70 €/val. „blended“ įkainio adekvatumą [1]–[9]. Tokiu būdu NB-IoT ir LoRaWAN pagrindu veikianti IoT platforma gali būti sukurta ir integruota laikantis 116 000 € CAPEX ribos, nepakenkiant esminiam funkcionalumui ir technologiniam tvarumui.

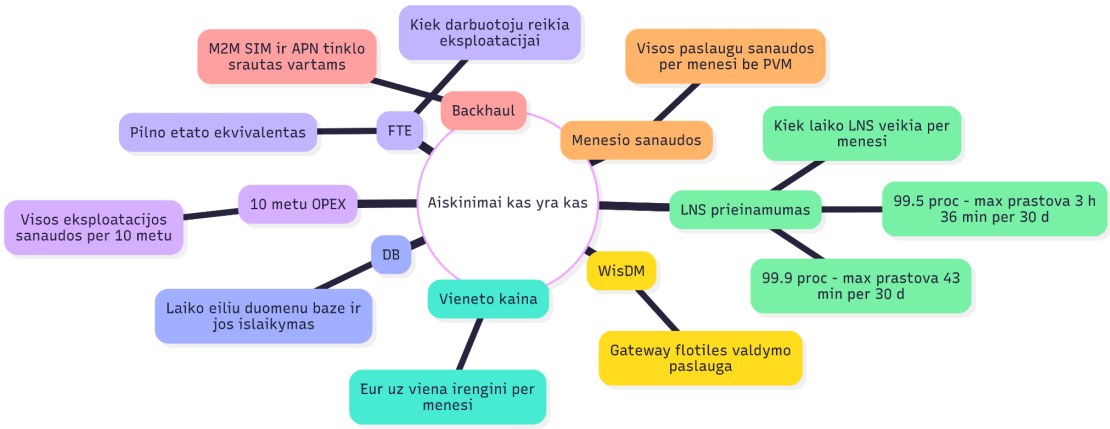
Literatūros sąrašas

[1] ManoAlga.lt. „Atlyginimas Programuotojas – Lietuva“. ManoAlga atlyginimų duomenų bazė.
[2] ManoAlga.lt. „Atlyginimas DevOps inžinierius – Lietuva“. ManoAlga atlyginimų duomenų bazė.
[3] TV3.lt. „Susigundę 8 tūkstančių eurų algomis žmonės keičia profesiją“. 2024-09-15.
[4] Rivile.lt. „Vidutinis atlyginimas Lietuvoje 2025: kiek uždirba lietuviai?“. 2025-06-22.
[5] Techremontas.lt. „Vidutinis atlyginimas technologijų sektoriuje 2024 metais“. 2025-10-17.

[6] ManoAlga.lt. „Atlyginimai Informacijos technologijos“. IT srities atlyginimų santrauka.
[7] Azilen. „IoT Development Cost Guide for Small, Medium & Large Projects“. 2025-10-21.
[8] Creole Studios. „How Much Does It Cost to Develop an IoT App in 2025?“. 2025-10-31.
[9] Decode Agency. „IoT app development cost: 6 key factors to consider“. 2024-10-22.
[10] Silicon Witchery. „The 3 Hidden Costs of IoT Prototyping“. 2025-08-01.
[11] Eclipse Mosquitto. „Eclipse Mosquitto – an open source MQTT broker“.
[12] EMQ. „A comprehensive comparison of open source MQTT brokers in 2023“.
[13] Timescale. „TimescaleDB Community Edition licensing and pricing“.
[14] Grafana Labs. „Grafana Cloud – plans and pricing“.
[15] Elementor; Name.com; Shopify. „How much does a domain name cost in 2025?“.
[16] GitHub. „GitHub pricing and Team plan“.
[17] Elest.io. „Plans and pricing for TimescaleDB / NC-MEDIUM-2C-4G ir NC-LARGE-4C-8G“.

EKSPLOATACIJOS MODELIAI (SAAS, HIBRIDAS, SELF-HOSTED) IR SLA [S-1.1.1][S-1.1.3][S-1.1.4][S-1.1.5]

Šiame skyriuje įvertinamos trys eksploatacijos alternatyvos LoRaWAN tinklo serveriui (LNS) ir duomenų sluoksniui, laikantis nustatytų prielaidų: apie 42 000 karšto vandens skaitiklių (KVS) – buto ar objekto vandens sunaudojimo apskaitos prietaisų su nuotoline telemetrija, 45 RAKwireless bazinės stotys, tipinis siuntimas 1 uplink/val. (≈24 per parą), Panevėžio, Kėdainių, Pasvalio, Kupiškio, Rokiškio ir Zarasų regioninė aprėptis, 8×5 eksploatacijos režimas be griežto 24/7 budėjimo, o duomenų pilnumo, vėlinimo ir SLA tikslai atitinka 9 skyriuje suformuluotus kriterijus. Pirmą kartą minimos sąvokos: ilgojo nuotolio tinklas (LoRaWAN) – LPWAN protokolas su žemomis energijos sąnaudomis; automatinis rodmenų surinkimas (AMR) – nuotolinis skaitiklių duomenų nuskaitymas be fizinio vizito; programinės įrangos per orą atnaujinimas (OTA) – nuotolinis įrangos programinės įrangos atnaujinimas. Alternatyvos aprašomos kaip „SaaS LNS“, „hibridas“ (SaaS LNS + nuosava duomenų platforma) ir „pilnai self-hosted“ (atvirojo kodo LNS + OSS stebėsena), pateikiant mėnesinį OPEX €/mėn. (be PVM, 2025 m. kainų lygis) ir vieneto kainą €/įr./mėn., 10 metų TCO = CAPEX + OPEX_10m, bei susijusias SLA nuostatas.



7 Pav. LoRaWAN sprendimo TCO (Total Cost of Ownership) struktūra

„SaaS LNS“ alternatyvoje LoRaWAN Network Server pasirenkamas kaip visiškai valdoma paslauga. The Things Stack Cloud „Standard“ planas apima licenciją iki 1000 galinių įrenginių ir „pay-as-you-go“ viršijus šią ribą, su 99,9 % paslaugos prieinamumu (SLA) ir neribotais gateway’ais; viešai pateikiamas mėnesinis „Standard“ įkainis 230 USD, taip pat prieinama valandinė, pagal registruotų įrenginių krepšelius „skalinta“ kaina per AWS Marketplace, leidžianti patvirtinti išlaidų tvarką didėjant apimčiai [1–3]. Praktikoje 50 000 įrenginių mastu konservatyviai vertinu LNS eilutę ≈ 50 × 230 EUR/mėn. = 11 500 EUR/mėn., kas, taikant 2025 m. biudžetinę prielaidą 1 USD ≈ 0,93 €, sudarytų apie 10 700 €/mėn. vien už LNS; šią eilutę papildo RAK WisDM „Enterprise 100“ (100 gateway’ų) 129,99 USD/mėn. ≈ 121 €/mėn., gateway backhaul su M2M SIM (pvz., 100 MB/30 d. plano orientyras ~6 USD/SIM, t. y. ~600 USD/mėn. ≈ 558 €/mėn.) ir laiko eilučių DB kaip paslauga (pvz., InfluxDB Cloud vartojimo kainodara ~0,002 €/GB-h; tipiniu 50–100 GB aktyviu saugojimu – kelios dešimtys eurų per mėnesį) [4–6], [10–12]. Tokiu atveju bendra mėnesinė sąmata sudaro apie 11,5–11,9 tūkst. €/mėn., o vieneto kaina ≈ 0,23–0,26 €/įr./mėn.; 10 metų OPEX komponentė būtų apie 1,38–1,43 mln. € (nekaitaliojant valiutos ir neįtraukiant netiesioginių sąnaudų). Pagrindinis „SaaS“ privalumas – maža operacinė rizika ir aiškios SLA nuostatos LNS sluoksnyje, o rizikos centrai lieka gateway backhaul ir DB užklausų/retencijos optimizavimas. [1–3], [4–6], [10–12].

PRIĖMIMO KRITERIJAI IR KPI RIBOS [S-1.1.2][S-1.1.5]

Priėmimo kriterijai turi būti formuluojami taip, kad būtų patikrinami per apibrėžtą laikotarpį (pvz., 14-30 parų pilotą) ir nepriklausytų nuo rankinio rodmenų tikrinimo. Todėl KPI ribos siūlomos aprašyti pagal įrenginių klasę (LoRaWAN KVS/ŠAP, NB-IoT įvadiniai, „probleminės“ vietos), aiškiai atskiriant tinklo, įrenginio ir platformos atsakomybės ribas.

Rekomenduojamas bazinis KPI rinkinys priėmimui: (a) sėkmingai priimtų uplink pranešimų dalis per 24 val. >= 98 % (KVS/ŠAP su 1-2 siuntimais per parą), (b) duomenų vėlinimas P95 <= 6 val., (c)

maksimalus nuoseklus duomenų tarpas be įrašų <= 48 val. įrenginiams, kurių siuntimo periodika 1 kartas per parą. Esant kitai periodikai, ribos perskaičiuojamos proporcingai tikėtinam įrašų skaičiui. KPI skaičiavimo logika ir ribos turi būti stebimos per monitoringą ir (jei taikoma) SLA ataskaitas.

Jeigu patikimumo KPI neatitinka ribų, trikčių šalinimas vykdomas pagal klasę: pirmiausia tikrinami aprėpties parametrai (RSSI/SNR, gateway matomumas), tada įrenginio konfigūracija (siuntimo intervalas, ADR, OMS/LoRaWAN profiliai), o galiausiai platformos grandinė (LNS, ingest, DB). Tokia seka sumažina nereikalingų vizitų skaičių ir leidžia sutelkti veiksmus į tikėtiną gedimo priežastį.

„Hibridas“ išlaiko LNS kaip SaaS (t. y. nominaliai tas pats 0,23–0,26 €/įr./mėn. didžiąja dalimi dėl LNS įkainio), bet duomenų sluoksnį (ingestas, analitika, vizualizacija, archyvai, API) talpina savo EU debesijoje ar duomenų centre. Ekonomiškai racionalus tri-mazgis (2× app/ingest + 1× DB) ir paprastas L7 balansavimas Hetzner Cloud aplinkoje šiandien kainuoja kelių dešimčių eurų per mazgą per mėnesį; viešos kainodaros ir nepriklausomos apžvalgos rodo, kad 4 vCPU/8 GB ar 8 vCPU/16 GB klasės serverių kainos yra žemų dviejų dešimčių eurų mėnesio zonoje, o egress įkainiai – apie 1 €/TB virš „free egress“ ribų; tokia architektūra leidžia pigiai didinti retenciją ir apkrautą analitiką, išlaikant kontrolę dėl GDPR, RBAC/SSO ir raktų valdymo [6–7], [16]. Tuo pačiu hibridas palieka WisDM ir M2M backhaul eilutes, todėl bendra mėnesinė sąmata praktiškai artima „SaaS“ alternatyvai, tačiau su žymiai lankstesnėmis duomenų gyvenimo ciklo sąnaudomis ir atitikties įrodymais (rezidavimas ES, auditai).

„Pilnai self-hosted“ remiasi atvirojo kodo ChirpStack v4 LNS, Redis/PostgreSQL ir OSS stebėsena. ChirpStack dokumentacija patvirtina architektūrinius reikalavimus (Redis ≥ 6.2, pastovus saugojimas SQLite/PostgreSQL, MQTT), o licencijavimo mokesčių nėra; infrastruktūrai pakanka 2–3 vidutinės klasės VM (4–8 vCPU, 8–16 GB RAM) ir LB, todėl mėnesinė infra eilutė EU debesijoje paprastai telpa į ~60–120 €/mėn. plius ~7–10 €/mėn. už balansavimą [8–9], [6–7], [16]. Tačiau realų TCO čia lemia žmonių darbas: net su įrankiais eksploatacijai, OTA, DR pratyboms, konfigūracijų valdymui ir saugos pataisoms reikia ~0,8–1,2 etato pastovios priežiūros. Įtraukus WisDM (~121 €/mėn.) ir 100 M2M SIM (~550–600 €/mėn.), vien paslaugų/infros eilutė vienam įrenginiui krenta iki ≈0,006–0,016 €/įr./mėn., bet su 1,0 FTE (pvz., 3000 €/mėn.) bendras OPEX tampa apie 0,07–0,08 €/įr./mėn., vis dar mažesnis už „SaaS“, tačiau jautresnis kompetencijų prieinamumui ir pokyčių valdymui. „Self-hosted“ tinka brandžiai komandai su formalizuotu runbook’u, nes priešingu atveju SLA < 99,5 % rizika atšaukia sutaupymus.

SLA ir paslaugos ribos formuluojamos sluoksniais. LNS sluoksnyje „SaaS“/„Plus“ planai deklaruoja 99,9 % prieinamumą, o „self-hosted“ turi atitikti bent 99,5 % tikslą su 8×5 arba 24/7 paramos procesu, incidentų MTTD/MTTR tikslais ir periodinėmis DR pratybomis [1]. Gateway/backhaul sluoksnyje SLA yra mišrus: WisDM suteikia flotilės valdymą, bet faktinį prieinamumą lemia energija, backhaul (M2M SIM/APN) ir lauko darbai; M2M tiekėjų kainodaros

pavyzdžiai rodo tiek fiksuotus krepšelius (pvz., 100 MB/30 d. ~6 USD), tiek „lifetime flat“ modelius galiniams prietaisams (nebūtina gateway’ams), todėl komercinės sutartys turi aiškiai apibrėžti datacap, tarptinklinį ryšį ir incidentų eskalaciją [4], [13–16]. Duomenų sluoksnyje SLA apima ingestą, saugojimą ir užklausas; vartojimu grįsta InfluxDB kainodara ir TigerData/Timescale siūlo skaidrius planus, tačiau praktinį SLA apsprendžia retencijos politika, indeksavimo/kompresijos strategijos ir atsarginės kopijos (RPO/RTO) [10–12], [20].

Priėmimo patikimumo kriterijams rekomenduojama taikyti du kiekybinius KPI: (1) sėkmingai priimtų uplink pranešimų dalis per 24 val. (%), (2) duomenų vėlinimas nuo matavimo momento iki įrašymo duomenų sluoksnyje (val.). KPI ribos nustatomos SLA lygiu ir stebimos monitoringo sistemoje (alertai), kad būtų užtikrintas duomenų savalaikiškumas ir pilnumas.

Jautrumo analizė rodo keturis didžiausius svirtinius kintamuosius. Pirma, LNS vieneto kaina „SaaS“ modelyje: net ±0,05 €/įr./mėn. keičia biudžetą ±2500 €/mėn. prie 50 000 įrenginių, todėl apimties nuolaidos ar alternatyviniai NaaS (pvz., LORIOT Professional Public Server, kurio vieša pradinė kaina prasideda nuo ~90 USD/mėn. ir 99,9 % SLA, o Enterprise privatūs diegimai derinami atskirai) daro didžiausią įtaką [9, 11]. Antra, backhaul M2M įkainis: ±2 €/SIM/mėn. keičia gateway sluoksnio OPEX ±200 €/mėn.; verta centralizuoti APN, valdyti keep-alive srautą ir periodiškai peržiūrėti tarifus. Trečia, FTE poreikis „self-hosted“ scenoje: +0,5 FTE pakeičia vieneto kainą apie +0,03 €/įr./mėn. Ketvirta, pakartotiniai vizitai dėl aprėpties „skylų“ ir downlink politikos – net maža „neudengtų“ objektų dalis generuoja disproporcines išlaidas, todėl antenų planavimas ir ADR/žinučių politika (10 skyrius) tiesiogiai „reguliuoja“ TCO.

Integracinė sąveika su esamu parku vienodai įgyvendinama visose trijose alternatyvose: KVS/ŠAP gamintojų OMS/LoRaWAN profiliai, AES-128 šifravimas, MID/RED atitiktis ir prietaisų archyvai užtikrina VEE (Validation–Estimation–Editing) procedūras ir „backfill“ be vizitų; SLA ir KPI bus pasiekiami, jei laikomasi raktų valdymo, TLS 1.2/1.3, RBAC/SSO ir auditų politikų (8 ir 9 skyriai). „SaaS“ ir „hibridas“ sparčiausiai pasiekia ≥97 % pilnumą ir ≤60 min. vėlinimą be papildomų incidentų valdymo kaštų; „self-hosted“ gali pasiekti tą patį, jei komanda brandi, o runbook’ai ir DR pratybos – reguliarūs.

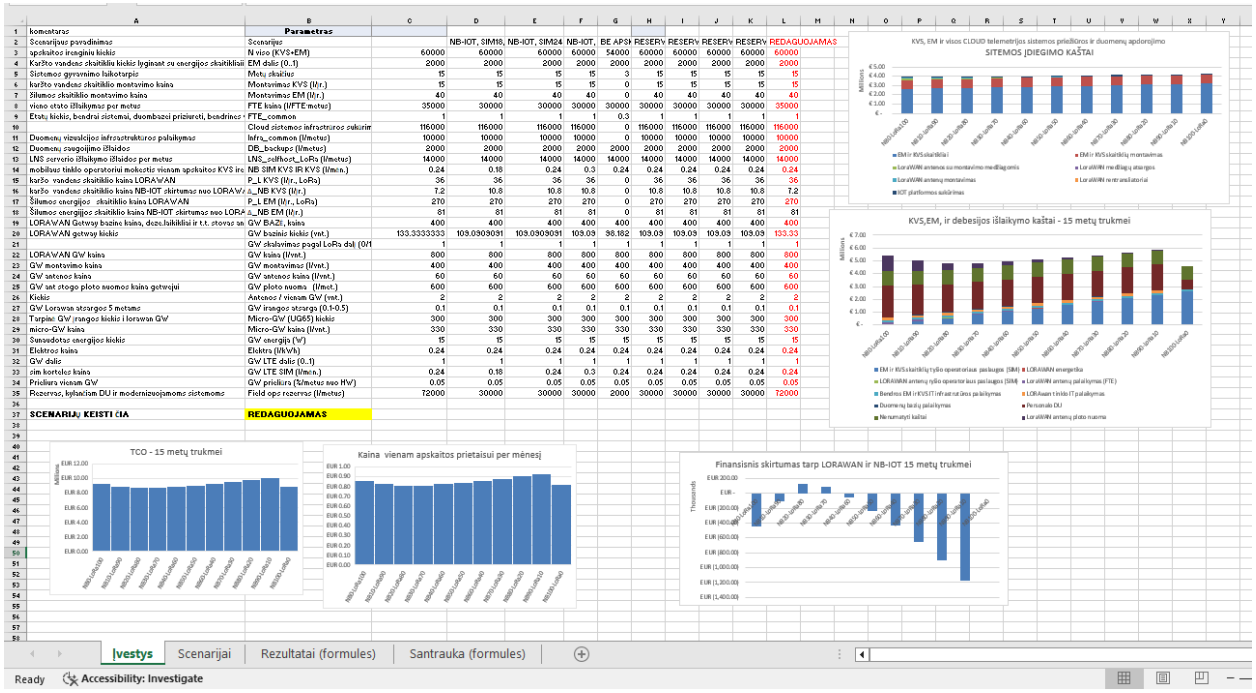
Argumentuota rekomendacija Panevėžio masteliui – „hibridas“: The Things Stack Cloud kaip LNS su 99,9 % SLA, RAK WisDM flotilei, o ingestą/analitiką/retenciją laikyti savo EU debesijoje. Taip išlaikoma aiški vieneto kaina (≈0,23–0,26 €/įr./mėn. šiandienos sąlygomis), minimali operacinė rizika ir labai žemos duomenų gyvenimo ciklo sąnaudos didėjant apimčiai. Tuo pat metu parengiama aiški migracijos trajektorija į „self-hosted“ LNS be pririšimo prie tiekėjo, jei po pilotinio laikotarpio bus siekiama sumažinti OPEX iki ≈0,06–0,08 €/įr./mėn. įskaičiavus 1,0 FTE. Alternatyva, kurią verta turėti kaip derybinę ašį, yra LORIOT Enterprise privatus serveris arba TTS Enterprise self-hosted, jei reikalingos papildomos funkcijos ar duomenų rezidavimo/izoliacijos reikalavimai [1], [9].

Literatūra

[1] The Things Industries. „Pricing Plans | The Things Stack“ – planų ribos, SLA ir 1000 įr. licencija. The Things Industries
[2] MCCI Store. „The Things Stack Cloud – LoRaWAN Network Server Solution“ – „Standard“ 230 USD/mėn., 1000 įr. licencija. MCCI
[3] AWS Marketplace. „The Things Stack Cloud for LoRaWAN“ – valandiniai tarifai pagal įrenginių krepšelius. Amazon Web Services, Inc.
[4] RAKwireless. „WisDM – Remote IoT Fleet LoRaWAN Gateway Management“ – „Enterprise 100“ 129,99 USD/mėn. RAKwireless
[5] RAKwireless News. „WisDM Flexible Pricing Model“ – kainodaros pakopos ir nuolaidos. news.rakwireless.com
[6] Hetzner Cloud. „Cloud servers – price overview“ – VM klasių kainodara. Hetzner
[7] GetDeploying. „Hetzner – Review, Pricing & Alternatives“ – pavyzdinės CX kainos ir egress. GetDeploying
[8] ChirpStack Docs. „ChirpStack – open-source LoRaWAN Network Server“ – architektūra ir API. chirpstack.io
[9] ChirpStack Docs. „Requirements“ – Redis ≥ 6.2, pastovus saugojimas. chirpstack.io
[10] InfluxData. „InfluxDB pricing (usage-based)“ – įrašų, saugojimo ir užklausų kainos. InfluxData
[11] InfluxData Docs. „Cloud pricing plans“ – planų tipai ir taikymas. InfluxData Documentation
[12] TigerData (Timescale Cloud). „Pricing“. tigerdata.com
[13] ThingsMobile. „Individual data packages“ – 100 MB / 30 d. ~6 USD. Things Mobile
[14] 1NCE. „IoT Lifetime Flat – 10 EUR už 10 metų“ – galinių įrenginių LTE-M/NB-IoT pavyzdinė kainodara. 1NCE
[15] Onomondo. „IoT SIM cards – Lithuania“ – rinkos įkainių orientyrai (€/MB). Onomondo
[16] GetDeploying. „Google Cloud vs Hetzner“ – kainų palyginimai (VM, storage, egress). GetDeploying
[17] LORIOT. „Professional Public Server“ – vieša kaina nuo ~90 USD/mėn., 99,9 % SLA, gaminio linija. LORIOT
[18] LoRa Alliance. „LoRaWAN Link Layer Specification v1.0.4 (L2 1.0.4)“. 2020. [LoRa Alliance, 2020].
[19] Open Metering System Group e.V. „OMS Specification – Volume 1 General, Issue 2.4.1 (Release F)“. 2023. [OMS Group, 2023].
[20] 3GPP/ETSI. „3GPP TS 23.682 V13.7.0 (Release 13): Architecture enhancements to facilitate communications with packet data networks and applications“. 2016. [3GPP, 2016].
[21] CEN. „EN 13757-4: Communication systems for meters – Wireless M-Bus communication“. 2019. [CEN, 2019].

EKONOMINIO VERTINIMO APSKAITOS SKAITIKLIŲ TINKLO VYSTYMO SKAIČIUOKLĖS SUDARYMAS [S-1.1.1][S-1.1.3]

Skaičiuoklė yra sudaryta taip, kad galėtų įvertinti skirtingus NB-IoT ir LoRaWAN technologijų derinius, modeliuojant jų finansinę įtaką visai matavimo infrastruktūrai per pasirinktą analizės horizontą. Pagrindinis įvesties parametras yra procentinis NB-IoT ir LoRaWAN santykis bendrame skaitiklių kiekyje. Šie dydžiai automatiškai paskirsto bendrą vartotojų skaičių į dvi technologines grupes ir nustato, kiek įrenginių priklauso NB-IoT, o kiek LoRaWAN segmentui. Skaičiuoklė taip pat atskiria įvadinius energijos matuoklius ir KVS skaitiklius, nes jų proporcijos ir diegimo sąnaudos skiriasi.



8. Pav. IoT PE prietaisų strategijų įgyvendinimo palyginimo ekonominė skaičiuoklė

Tolimesni skaičiavimai remiasi kiekvienos technologijos specifiniais veiklos komponentais. NB-IoT daliai generuojami tik kintamieji ryšio mokesčiai, proporcingi SIM kortelių skaičiui ir naudojimo trukmei. Prie LoRaWAN priskiriami visi infrastruktūriniai elementai, tokie kaip prieigos stotelių skaičius, energijos sąnaudos, antenų ryšio mokesčiai, priežiūra, nuoma ir techninio personalo poreikis. Skaičiuoklė turi atskirus modulius antenų, infrastruktūros, tinklo serverio, duomenų bazių ir FTE kaštams apskaičiuoti, todėl kiekvienas tinklo komponentas prisideda prie bendro OPEX pagal realų technologinį architektūrinį poreikį. Šios eilutės automatiškai adaptuojasi prie LoRaWAN įrenginių skaičiaus, todėl tinklo kaštai mažėjant vartotojų kiekiui didėja disproporcingai dėl fiksuotų sąnaudų, kurios išlieka beveik pastovios.

CAPEX dalyje skaičiuoklė vertina pradinius investicinius kaštus, kurie priklauso tik nuo LoRaWAN tinklo stiprumo ir geografinio aprėpties poreikio. NB-IoT scenarijuose CAPEX iš esmės neatsiranda, nes tinklą finansuoja operatorius, o paslaugos vartotojas moka tik už SIM ryšio naudojimą. Didėjant NB daliai, CAPEX automatiškai artėja prie nulio. Didėjant LoRaWAN proporcijai, investicijos kyla dėl prieigos stočių, antenų, rėmimo konstrukcijų ir kitų fizinių komponentų poreikio.

Kai visi komponentai apskaičiuojami, skaičiuoklė sugeneruoja bendrą OPEX sumą vieneriems metams ir kumuliacinę vertę analizuojamam laikotarpiui. Tada jos sudedamos su CAPEX, gaunant galutinį viso projekto TCO. TCO normalizuojamas skaičiuojant kainą vienam įrenginiui per metus ir vienam įrenginiui per mėnesį, kas leidžia patogiai lyginti skirtingų technologinių scenarijų ekonominį efektyvumą nepriklausomai nuo bendros vartotojų apimties.

Skaičiuoklė taip pat įvertina efektą organizacinei struktūrai. Didėjanti LoRaWAN dalis reiškia papildomas funkcijas, tokias kaip 24/7 priežiūra, ryšio kokybės monitoringas, serverių administravimas, incidentų valdymas ir programinės įrangos atnaujinimai. Šie kaštai įtraukiami kaip FTE ir bendrųjų IT infrastruktūros elementų kaštai, kurie yra fiksuoti ir ženkliai prisideda prie LoRaWAN TCO. NB-IoT scenarijai tokių kaštų neturi, nes infrastruktūrą valdo mobiliojo ryšio operatorius.

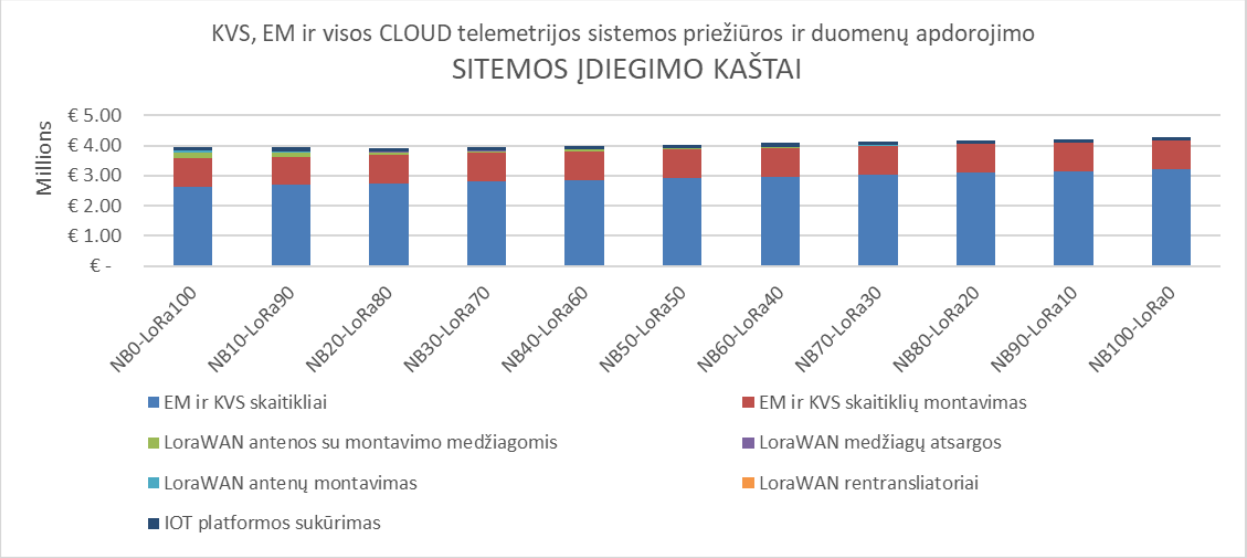
Galutinis skaičiuoklės rezultatas aiškiai parodo technologijų mastelio efektą: NB-IoT turi grynai kintamą kainą, kuri proporcinga įrenginių kiekiui, o LoRaWAN turi dominuojančią fiksuotąją kaštų dalį, kuri paskirstoma įrenginių bazėje. Todėl mažėjant LoRaWAN skaitiklių skaičiui vieno įrenginio kaina ženkliai didėja, net jei absoliutus tinklo palaikymo kaštas išlieka stabilus.

Skaičiuoklės logika leidžia per kelias sekundes įvertinti bet kurią NB-IoT ir LoRaWAN kombinaciją, palyginti scenarijus pagal CAPEX, OPEX, TCO ir vieno įrenginio mėnesinę kainą bei padėti priimti ekonomiškai pagrįstą sprendimą dėl tinklo architektūros.

LORAWAN IR NB-IOT TECHNOLOGIJŲ EKONOMINIS PALYGINIMAS [S-1.1.1][S-1.1.3]

Kapitalo investicijų (CAPEX) struktūra

LoRaWAN atveju didžiausią kapitalo dalį sudaro prieigos stočių infrastruktūra, antenų mazgai ir pradinis LNS (tinklo serverio) parengimas. Didelėje sistemoje, aptarnaujančioje 60 tūkst. įrenginių, šios investicijos siekia nuo 3,950 iki 3,928 mln. € (NB20–LoRa80 ir NB0–LoRa100 scenarijuose). Tuo tarpu NB-IoT scenarijuje CAPEX didėja iki 4,273 tūkst. €, nes technologija remiasi mobiliojo ryšio operatoriaus radijo ir branduolio tinklu, o diegiamoji dalis apsiriboja IT platformos komponentais. Skirtumas tarp LoRa dominavimo ir NB dominavimo sudaro 322 tūkst. €, ir tai atspindi esminę LoRaWAN savybę turėti nuosavą radijo infrastruktūrą.



9 Pav. Įdiegimo kaštai

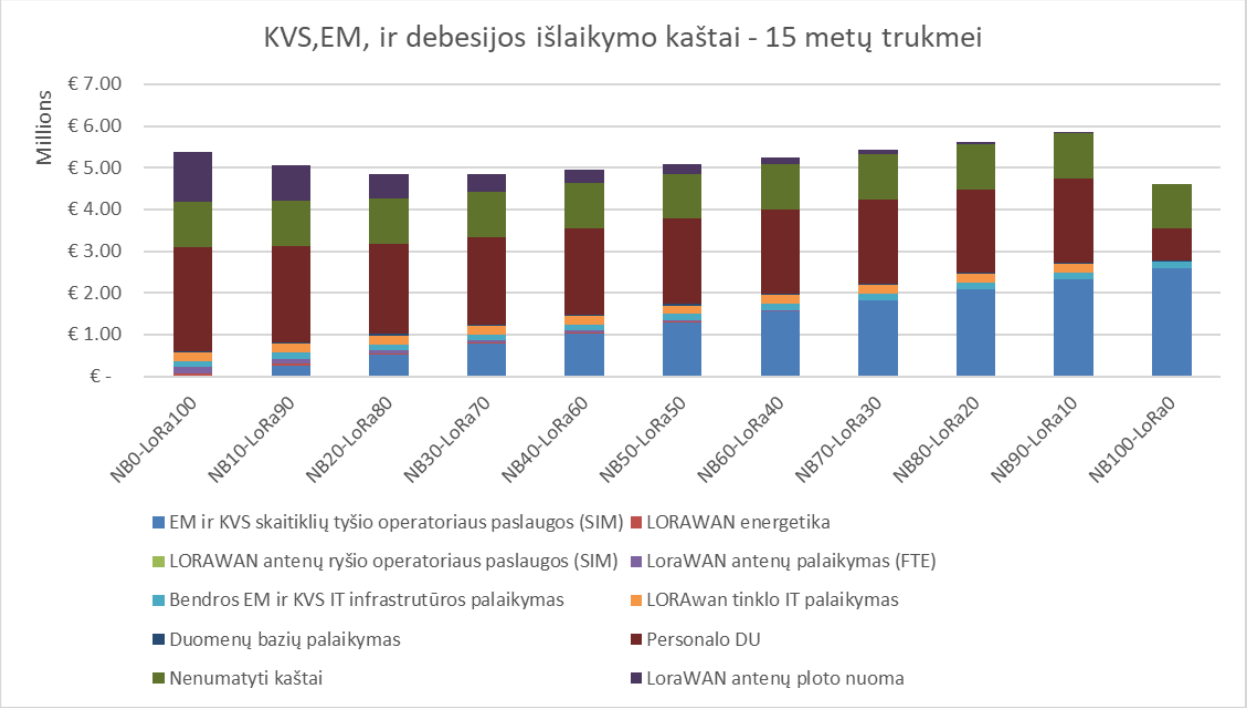
Veiklos sąnaudos (OPEX)

Tyrimo duomenys rodo, kad OPEX struktūra sistemingai kinta priklausomai nuo NB-IoT ir LoRaWAN dalies tinkle. Pirma, yra santykinai pastovi infrastruktūros dalis: bendros IT ir duomenų infrastruktūros sąnaudos (OPEX_infra_common, OPEX_LNS_self, OPEX_DB, OPEX_FieldOps) LoRa-dominuojančiuose scenarijuose sudaro apie 1,47 mln. € per 15 metų, t. y. maždaug 98 tūkst. €/metus, o NB100–LoRa0 atveju – 1,26 mln. € per 15 metų (apie 84 tūkst. €/metus, nes nelieka LNS palaikymo eilutės).

Didžiausia diferenciacija atsiranda dviejose komponentų grupėse: NB SIM sąnaudose ir LoRa prieigos stočių eksploatavime. NB-IoT SIM paslaugų kaštai (OPEX_SIM_NB) per 15 metų didėja nuo 0 € NB0–LoRa100 scenarijuje iki 2,592 mln. € NB100–LoRa0 atveju, t. y. nuo 0 iki maždaug 173 tūkst. €/metus. Priešinga kryptimi kinta LoRa infrastruktūros eksploatacinės sąnaudos: prieigos stočių energija, LTE uplink, ploto nuoma ir priežiūra (OPEX_GW_energija + OPEX_GW_LTE + OPEX_GW_NUOMA + OPEX_GW_priežiūra) LoRa100 scenarijuje sudaro apie 1,42 mln. € per 15 metų (apie 95 tūkst. €/metus), o NB100 scenarijuje sumažėja iki 0 €, nes LoRa prieigos stotys apskritai nenaudojamos.

Trečias ryškus kintamasis – personalo sąnaudos. OPEX_FTE LoRa-dominuojančiame NB0–LoRa100 scenarijuje siekia 2,485 mln. € per 15 metų, tai atitinka apie 166 tūkst. €/metus, o NB100–LoRa0 scenarijuje sumažėja iki 761 tūkst. €, t. y. maždaug 51 tūkst. €/metus. Taigi, didėjant NB daliai mažėja vidinis LoRa operacijų FTE poreikis, tačiau tai kompensuoja augantys SIM kaštai.

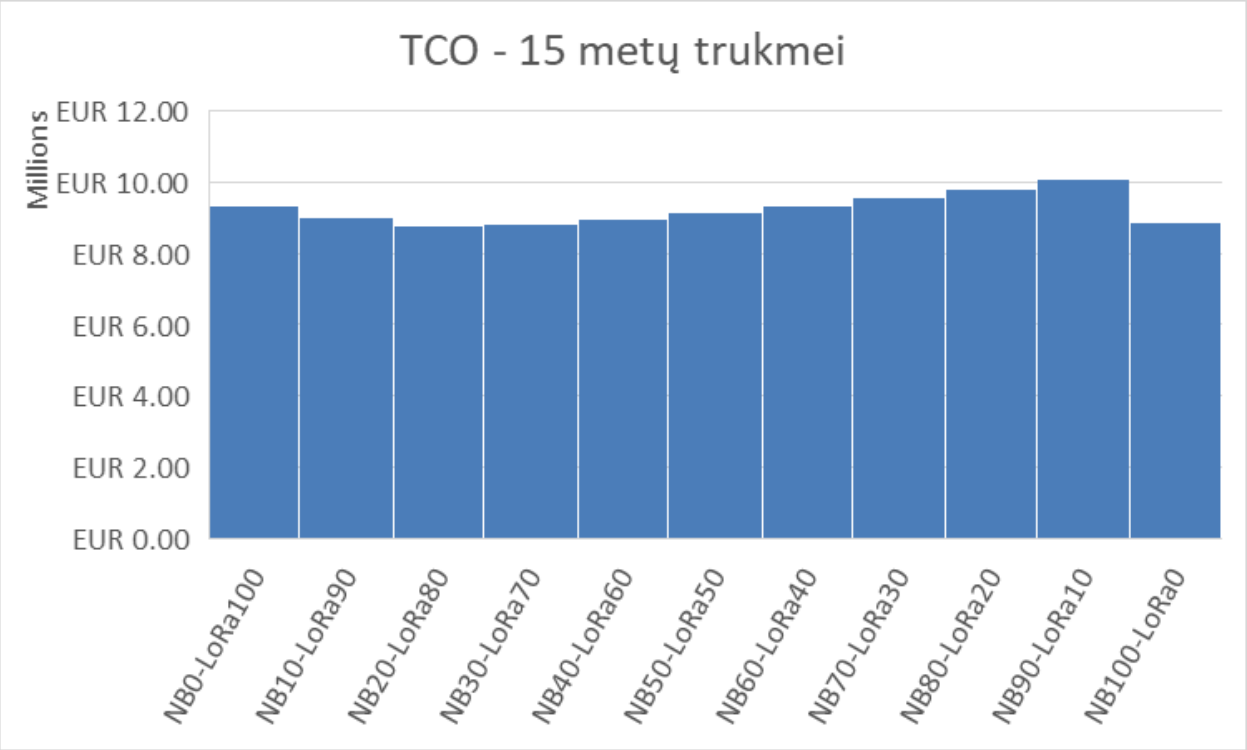
Dėl šių priešingų tendencijų bendros veiklos sąnaudos (OPEX_viso) sudaro nuo 4,61 mln. € per 15 metų (~308 tūkst. €/metus) NB100–LoRa0 scenarijuje iki 5,84 mln. € per 15 metų (~390 tūkst. €/metus) NB90–LoRa10 atveju. LoRa-dominuojantys scenarijai NB0–LoRa100, NB10–LoRa90 ir NB20–LoRa80 patenka į intervalą 4,84–5,38 mln. €, t. y. apie 322–358 tūkst. €/metus, ir sudaro balansą tarp didesnių LoRa infrastruktūros/FTE sąnaudų ir nulinio NB SIM komponento.



10 Pav. Išlaikymo kaštai 15 metų laikotarpiui

Bendros nuosavybės kainos (TCO) dinamika

Bendras TCO per 15 metų ryškiai priklauso nuo technologijos dominavimo dalies. LoRaWAN-orientuotuose scenarijuose TCO svyruoja nuo 9,327 mln. € (NB0–LoRa100) iki 8,763 mln. € (NB30–LoRa70). Tuo tarpu NB-IoT dominavimo atveju (NB100–LoRa0) TCO yra 8,887 mln. €. Taigi, visos sistemos TCO padidėjimas nuo LoRa-dominuojančio iki NB-dominuojančio modelio sudaro ~110 tūkst. €, arba apie 1 %. Šis skirtumas atsiranda dėl NB-IoT eksploatacinių sąnaudų kumuliacijos: ryšio paslaugos yra apmokestinamos kiekvienam įrenginiui atskirai per visą eksploatacijos laikotarpį, o LoRaWAN infrastruktūros CAPEX paskirstomas dideliam vartotojų kiekiui, todėl vieneto kaina mažėja augant sistemai.



11 Pav. Įdiegimo ir išlaikymo kaštai 15 metų laikotarpiui

TCO perskaičiavimas į įrenginio mėnesinį kaštą

Vieno įrenginio mėnesinis kaštas yra tarp svarbiausių KPI, leidžiančių objektyviai palyginti technologijas nepriklausomai nuo sistemos masto. Analizė rodo, kad:

- NB0–LoRa100 scenarijus: 0,86 €/mėn/įr.
  NB10–LoRa90: 0,83 €/mėn/įr.
- NB20–LoRa80: 0,81 €/mėn/įr.
- NB30–LoRa70: 0,82 €/mėn/įr.
  NB100–LoRa0: 0,82 €/mėn/įr.

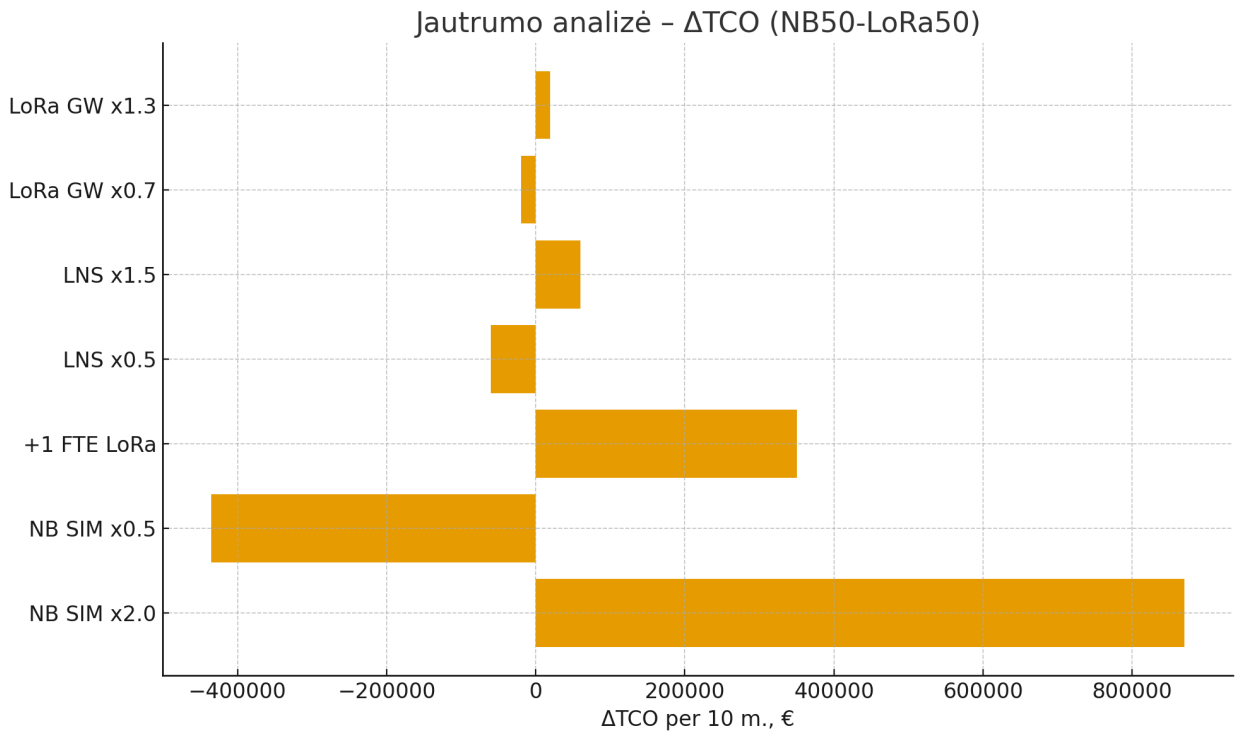
Galutinė analizės išvada rodo, kad savarankiškas LoRaWAN tinklo vystymas įmonei nėra ekonomiškai pagrįstas, net ir LoRa dominavimo scenarijuose. Nors technologiškai LoRaWAN suteikia didesnę kontrolę ir mažesnę priklausomybę nuo operatorių, finansiniu požiūriu skirtumas tarp NB-IoT ir LoRaWAN bendrojo mėnesinio įrenginio kašto tesiekia 1 euro centą vienam vartotojui, arba apie 600 €/mėn. visai 60 tūkst. įrenginių sistemai. Per 15 metų tai sudaro vos ~108 tūkst. €, t. y. reikšmingai mažiau nei papildomas finansinis ir organizacinis krūvis, kurį sukuria LoRa infrastruktūros valdymas. Praktinė reikšmė tokio sutaupymo yra ribota, nes įmonė prisiima ne tik prieigos stočių ir tinklo serverio priežiūrą, energijos ir uplink kaštus, bet ir nuolatinį IT/OT

specialistų poreikį, incidentų valdymą, saugos politikos palaikymą ir infrastruktūros plėtrą. Tai veiklos sritys, nesusijusios su pagrindine įmonės misija – šilumos ir karšto vandens gamyba, tiekimu ir vartotojų aptarnavimu.

Todėl, vertinant tiek finansinius rodiklius, tiek organizacinę riziką, savarankiškas LoRaWAN tinklo eksploatavimas įmonei neteikia reikšmingos ekonominės naudos. Alternatyva perduoti LoRaWAN tinklo paslaugas išoriniam tiekėjui leidžia eliminuoti neesminių funkcijų kaštus, sumažinti kompetencijų palaikymo naštą, eliminuoti kapitalo investicijas ir kartu išlaikyti praktiškai identišką vieno įrenginio eksploatacijos kainą. Toks sprendimas ženkliai supaprastina organizacinę struktūrą ir leidžia sutelkti žmogiškuosius bei finansinius resursus į pagrindinės veiklos efektyvinimą, išvengiant situacijos, kai už minimalų – vos vieno cento – ekonominį efektą įmonė prisiima pilną telekomunikacinio tinklo vystymo ir palaikymo atsakomybę.

JAUTRUMO ANALIZĖ [S-1.1.3][S-1.1.1]

Jautrumo analizė rodo, kad 3–4 parametrai yra didžiausi TCO elastingumo veiksniai. Pirmiausia, NB-IoT SIM kaina: jos padvigubėjimas nuo 29 € iki 58 € per 10 metų padidina NB100 scenarijaus TCO ~1,74 mln. €, o NB50 – ~0,87 mln. €; LoRa-tik scenarijus šiam pokyčiui visiškai nejautrus. Antra, LoRa prieigos stočių bazinio kiekio pokytis ±30 % keičia TCO tik ~±40 tūkst. € LoRa-tik atveju, todėl sprendinio atsparumas radijo planavimo netikslumams yra aukštas. Trečia, FTE LoRa operacijoms padidina TCO visiems scenarijams, kuriuose yra LoRa, vienodai 0,35 mln. € per 10 metų, kas yra <3,5 % LoRa-tik TCO; ketvirta, LNS savilaikos sąnaudų ±50 % svyravimas keičia TCO ~±60 tūkst. € ir yra antraeilis. Šių skaičių detalizacija pateikta priede „Jautrumo analizė“ (CSV) bei grafike „TCO per 10 m. pagal NB dalį“.



12 Pav. Jautrumo analizė 10 metų laikotarpiui

Praktiniu požiūriu, jei NB dalis lygi KVS problematikos ir visų įvadinių ŠAP sumai (~10–20 % visų įrenginių), papildoma „draudimo“ kaina lyginant su LoRa-tik scenarijumi yra 0,36–0,70 mln. € per 10 metų, kas daugeliu atvejų pateisinama rezervinio padengimo ir SLA rizikos mažinimu.

REKOMENDACIJA A - VYSTYTI NB-IOT 100% TINKLĄ [S-1.1.2] [S-1.1.3]

Jei visi ~60 000 įrenginių būtų 100 % NB-IoT, tinklo architektūra natūraliai supaprastėja: nebereikia LoRaWAN prieigos stočių, LNS, radijo planavimo, o visa radijo dalis ir branduolinis mobilusis tinklas atsiduria pas operatorių. Tačiau atsiranda kiti akcentai – SIM/eSIM valdymas, APN architektūra, srautų atskyrimas, saugumas ir įrenginių gyvavimo ciklo kontrolė. Reikia aiškaus modelio, kaip visi įrenginiai per operatoriaus infrastruktūrą pasiekia mūsų IoT branduolį, ir kaip šis branduolys integruojamas su verslo sistemomis, stebėsena ir incidentų valdymu.

Logika paprasta: lauke turime tik NB-IoT įrenginius su SIM/eSIM, visa radijo dalis ir mobiliojo tinklo branduolys yra pas operatorių, o mūsų zonoje atsiranda trys pagrindiniai blokai: saugus įėjimas (APN/VPN), IoT ingest + pranešimų sluoksnis ir aplikacijų/analitikos/valdymo dalis.

NB-IoT įrenginiai dirba licencijuotame dažnyne, naudoja PSM/eDRX režimus energijos taupymui ir pagal operatoriaus taisykles jungiasi prie NB-IoT RAN ir EPC/5GC branduolio. Visiems įrenginiams nustatomas privatus APN, kuris srautą nukreipia ne į viešą internetą, o į mūsų tinklą per IPsec ar

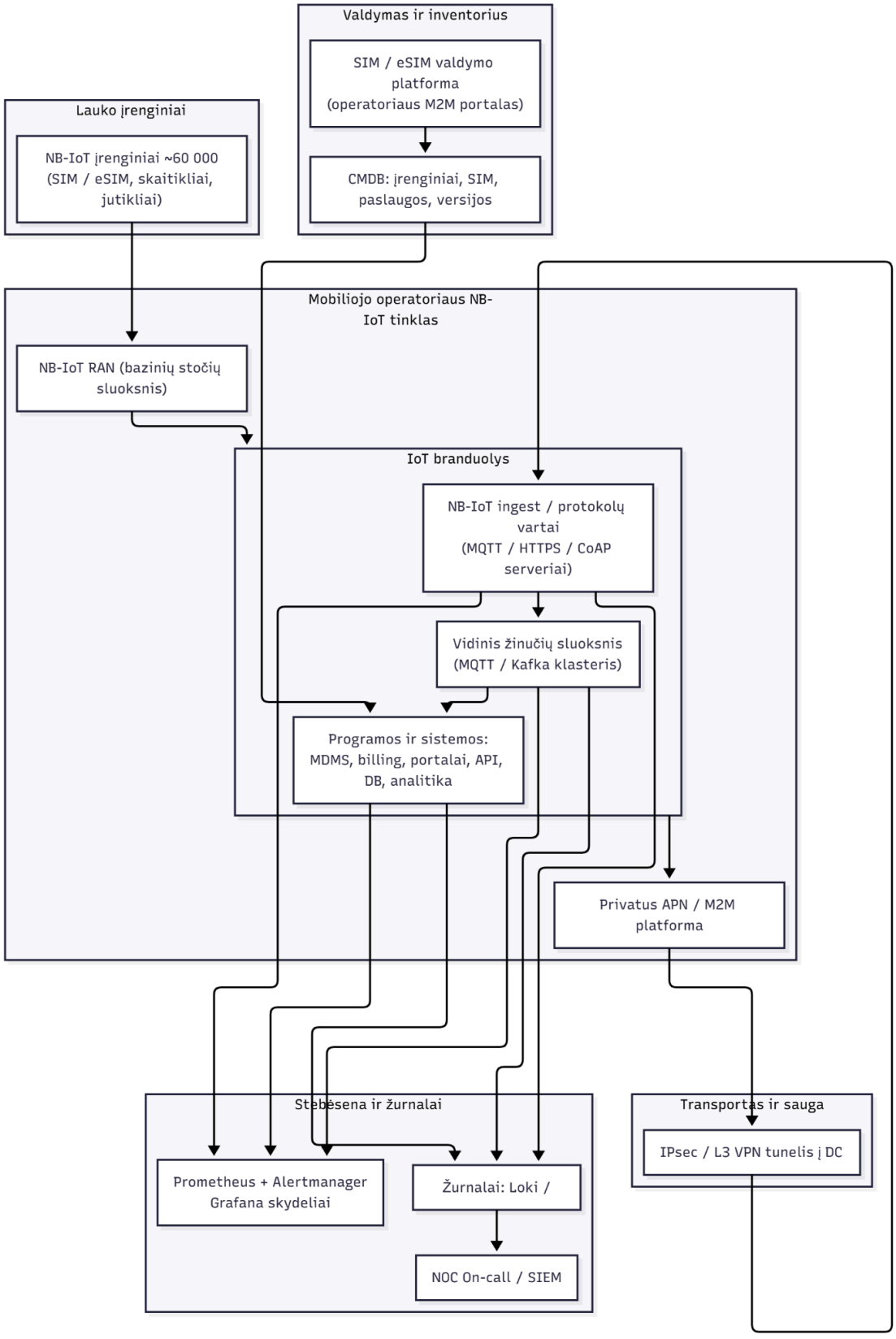
kitą L3 VPN tunelį. Tai reiškia, kad visi 60 000 įrenginių iš mūsų pusės atrodo kaip uždaras adresų segmentas, iš kurio telemetrija atiteka į DMZ ar IoT zoną.

Mūsų pusėje pirmasis blokas – NB-IoT ingest sluoksnis. Čia veikia protokolų vartai: MQTT/HTTPS/CoAP serveriai ar adapteriai, kurie priima duomenis iš operatoriaus ir konvertuoja juos į bendrą telemetrijos formatą. Šiame taške atliekamas įrenginių autentifikavimas pagal SIM, IMEI ar papildomus raktus, įrašai sulyginami su įrenginių registru/CMDB, tikrinamos versijos ir taikoma bazinė logika (pvz., paprasti filtrai, validacijos). Po to visi įvykiai ir matavimai paduodami į vidinį žinučių sluoksnį – dažniausiai MQTT ir (ar) Kafka klasterį. Tai yra centrinis „stuburas“, prie kurio jungiasi visos aukštesnio lygmens programos.

Aukščiau – aplikacijų ir duomenų sluoksnis. Čia veikia MDMS/MDM sistema, apskaitos ir atsiskaitymų moduliai, vartotojų portalai, REST/GraphQL API, ataskaitų generavimas ir ilgalaikių matavimų saugyklos (SQL/TimeSeries DB, Data Lake). Kadangi visi įrenginiai NB-IoT, kelių skirtingų radijo technologijų suderinimo problemos išnyksta: kiekvienas naujas servisas prenumeruoja tas pačias MQTT/Kafka temas ir nebėra skirtumo, iš kurio miesto ar bazinės stoties duomenys atėjo.

Stebėsena ir žurnalai išdėstyti horizontaliai. Kiekvienas komponentas – NB-IoT ingest, žinučių sluoksnis, duomenų bazės, API – turi Prometheus eksporterį, metrikos vizualizuojamos Grafana skydeliuose, o Alertmanager siunčia aliarmus pagal SLA ir KPI (pavyzdžiui, laiku neatėjęs matavimas, padidėjęs klaidų santykis, išaugusi atsakymų trukmė). Žurnalai (programiniai, audito, saugos) kaupiami Loki arba ELK – ten koreliuojamos tiek aplikacinės, tiek infrastruktūrinės klaidos. Ant šio pamato dirba NOC on-call ir, jei reikia, SIEM/NIS2 procesai.

Valdymo blokas NB-IoT scenarijuje persikelia į SIM ir įrenginių gyvavimo ciklą. Vietoje LoRa prieigos stočių valdymo atsiranda SIM/eSIM platforma (operatoriaus ar mūsų M2M portalas), kurioje tvarkomos kortelės, aktyvavimai, tarifai, limitai ir IMEI–kliento susiejimas. CMDB tampa centrine vieta, kur matosi įrenginio ID, SIM numeris, NB-IoT parametrai, firmware versijos ir priskirtos paslaugos. Per API ji susieta su aplikacijomis ir sąskaitų formavimo programine įranga, kad techninė informacija būtų viena, o ne „Excel’iuose“.



13 Pav. NB-IoT sistemos architektūrinė schema

Visiškai NB-IoT pagrindu veikiantis modelis iš esmės pakeičia atsakomybės ribas: radijo ir branduolinio tinklo lygmenyje pasikliaujama operatoriumi, o savo pusėje koncentruojamasi į saugų įėjimą (privatus APN + VPN), IoT ingest, vieningą žinučių sluoksnį ir aplikacijų ekosistemą. Toks dizainas mažina mūsų radijo infrastruktūros sudėtingumą, bet padidina priklausomybę nuo operatoriaus – tiek kainodaros, tiek SLA ir incidentų valdymo prasme.

Praktiškai rekomenduotina: su operatoriumi aiškiai sutarti dėl APN/VPN architektūros, SLA aprėpties ir žurnalinių duomenų, savo infrastruktūroje nuo pirmos dienos turėti pilną stebėsenos ir sistemos matomumo užtikrinimą (Prometheus, Grafana, Loki/ELK) ir CMDB, o NB-IoT ingest projektuoti taip, kad prireikus būtų galima prijungti ir kitus šaltinius (pvz., vėliau atsirandančius LoRaWAN ar LTE-M įrenginius) be architektūros perdarymo.

REKOMENDACIJA B - VYSTYTI LoRaWAN 70% - NB-IOT 30% TINKLĄ [S-1.1.3]

Šiuo etapu siūloma apsvarstyti kelias tolimesnes kryptis, kurios galėtų padėti aiškiau apibrėžti, kuria linkme tikslinga judėti toliau vystant skaitiklių sistemą. Vietoje konkrečių veiksmų plano čia pateikiami strateginiai svarstymai, kurie padėtų įvertinti dabartinę situaciją, priklausomybę nuo esamų technologinių sprendimų ir galimą savarankiškumo stiprinimą ateityje. Sprendimų nereikėtų skubinti – svarbu įsigilinti į alternatyvas, palyginti jų pranašumus ir rizikas, bei išlaikyti lankstumą, kuris leistų adaptuotis keičiantis technologinėms ar rinkos sąlygoms.

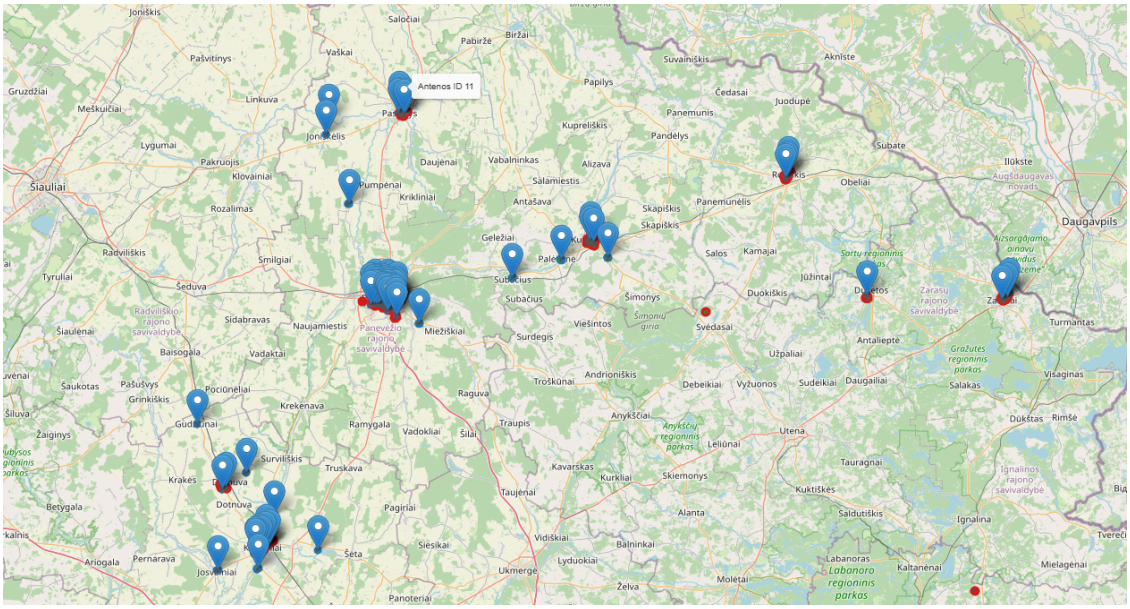
14 Pav. LoRaWAN tinklo planavimo schema

Analizę pradėjome nuo aiškaus tikslo: LoRaWAN tinklu aptarnauti apie 70 % visų klientų, o likusius 30 % patikimai nuskaityti NB-IoT ryšiu. Turimi adresų duomenys su koordinatėmis, patalpų skaičiumi ir OSM sluoksniais leido tiksliai modeliuoti „blogiausio miesto vidaus“ scenarijų, nes aprėptį vertinome ne pagal atvirą lauką, o pagal realius pastatų kontūrus ir želdynų tankį. Koordinates perkėlėme į UTM sistemą, kad visi atstumų skaičiavimai būtų metriniai ir tikslūs.

Kaip ir pilno padengimo scenarijuje, adresus suskirstėme į lokalius klasterius pagal 300 m spindulį. Ši riba nėra fizinė LoRa apribojimo reikšmė, o sąmoningai konservatyvus dydis, tinkamas tankiam užstatymui ir NLoS aplinkoms, kuriose svarbiausia yra vidaus patalpų patikimumas. Kiekvienam klasteriui sugeneravome realias kandidatines vietas – aukštesnius stogus iš OSM duomenų ir prireikus pačių adresų pastatus. Tokiu būdu buvo vertinamos tik techniškai įmanomos stotelių lokacijos.

Ryšio biudžeto analizė išliko tokia pati: uplink signalą skaičiavome iš siuntimo galios, antenų stiprinimų, kabelių nuostolių, tako slopinimo ir papildomų aplinkos nuostolių. Tako slopinimas įvertintas pagal Okumura–Hata modelį 868 MHz dažniui, atsižvelgiant į įrenginio ir stoties aukštį. Kiekvienam kertamam pastato kontūrui taikėme apie 10 dB nuostolį, o želdynams – ~0,3 dB už metrą tankesnėje lapijoje. Gautas priimtas signalas lygintas su SF10 jautrumu, reikalaujant ne mažesnės kaip 12 dB maržos, kuri praktiškai užtikrina >90 % paketo pasiekimo tikimybę net sudėtingose vidaus sąlygose.

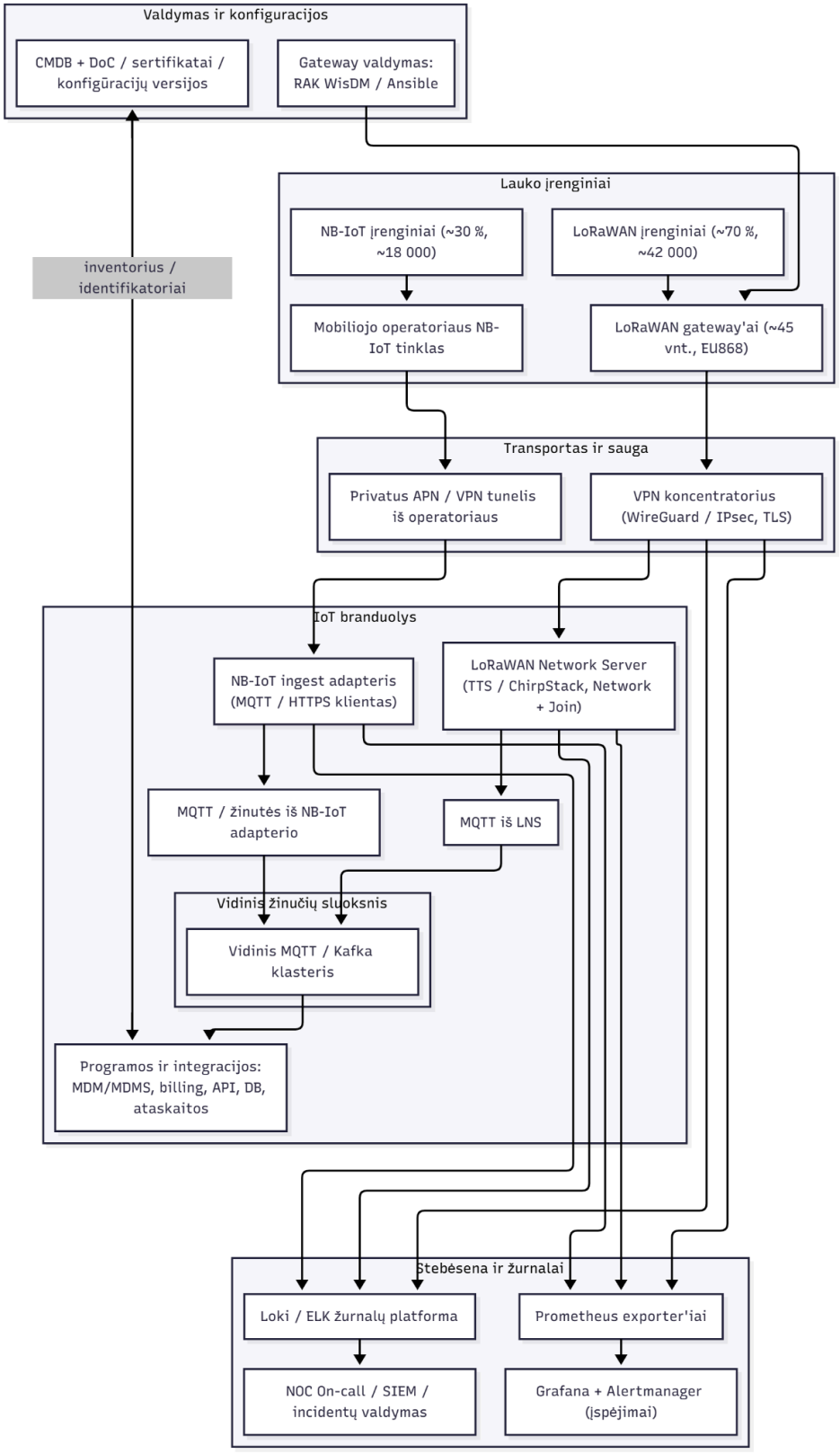
Kiekviename klasteryje iš kandidatų išrinkome vieną geriausią vietą, optimizuodami aprėptį pagal pirmuosius artimiausius adresus, jų patalpų skaičių ir likutinę ryšio maržą. Visus adresus globaliai pririšome prie tos stoties, kuri suteikė didžiausią maržą, jei ji buvo ne toliau kaip ~300 m. Šitaip tiksliai suskaičiavome, kokią dalį galima aptarnauti, naudojant ribotą LoRaWAN stotelių kiekį.



15 Pav. LoraWAN antenų padengimo žemėlapis PE apskaitos įrenginiams

Kadangi tikslas – efektyviai aprėpti tik 70 % klientų, metodiką pritaikėme taip, kad būtų parenkamas minimalus stotelių skaičius, duodantis geriausią grąžą pagal padengtų adresų kiekį. Atlikus modeliavimą, Panevėžio regiono morfologijoje paaiškėjo, kad norint LoRaWAN tinklu patikimai nuskaityti šiuos 70 % klientų, pakanka maždaug 45 stotelių. Šis skaičius išlaiko pakankamą ryšio maržą tankiausiuose kvartaluose ir kartu išvengia perteklinių persidengimų. Likę 30 % klientų daugiausia patenka į problemines zonas – didesnius atstumus nuo stotelių, žemos kokybės NLoS koridorius arba pavienius kaimo pastatus, kuriuos ekonomiškai ir techniškai racionaliausia aptarnauti NB-IoT ryšiu.

Papildomai įsitikinome, kad 45 LoRaWAN stotelės suvaldys numatomą srautą. Jei vienas įrenginys siunčia apie 12 pranešimų per dieną, o 70 % klientų sudaro apie 42 tūkst. įrenginių, gauname apie 504 tūkst. pranešimų per dieną. Padalinus per 45 stotis ir 8 kanalus kiekvienoje, vieno kanalo apkrova sudaro nedidelę dalį eterio laiko, todėl talpos rezervas išlieka didelis ir augimui, ir techniniams pokyčiams.



16 Pav. NB-IoT ir LoRaWAN sistemos architektūrinė schema

Projektuojamas tinklas turi patikimai aptarnauti apie 60 000 galutinių įrenginių – skaitiklių ir jutiklių – išskaidytų per miestus ir miestelius, turinčius skirtingą užstatymo tankį ir ryšio sąlygas. Siekiama ne teorinio radijo „burbulo“, o realios vidaus aprėpties: apie 70 % įrenginių nuskaityti per LoRaWAN infrastruktūrą (apie 45 bazinės stotys), o likusius 30 % – per mobiliojo operatoriaus NB-IoT tinklą. Tokia dviejų technologijų kombinacija turi būti sujungta į vieną IoT branduolį, kuriame veikia bendri protokolai, stebėsena, saugumas ir integracijos su verslo sistemomis. Architektūros uždavinys – aiškiai atskirti lauko įrenginius, transporto sluoksnį, branduolį, stebėseną ir valdymą, kad sistema būtų skaidri, plečiama ir atitiktų kibernetinio saugumo bei duomenų apsaugos reikalavimus.

Lauko lygmenyje LoRaWAN ir NB-IoT atskiriami jau pačioje pradžioje. Apie 70 % visų įrenginių – tai LoRaWAN skaitikliai ir jutikliai, kurie dirba EU868 dažnių juostoje ir jungiasi prie maždaug 45 LoRaWAN bazinių stočių. Tokį kiekį stotelių pagrindžia ankstesnė radijo planavimo analizė: su konservatyviu ryšio biudžetu ir 600m klasterizacija šis skaičius leidžia padengti tankiausius kvartalus ir pasiekti norimą vidaus patikimumą. Likę maždaug 30 % įrenginių dirba NB-IoT režimu, naudodami mobiliojo operatoriaus tinklą. Tai dažniausiai pavieniai ar geografiškai „brangūs“ objektai, kuriuos ekonomiškiau aptarnauti per licencijuotą operatoriaus radiją nei statyti papildomas LoRaWAN stotis.

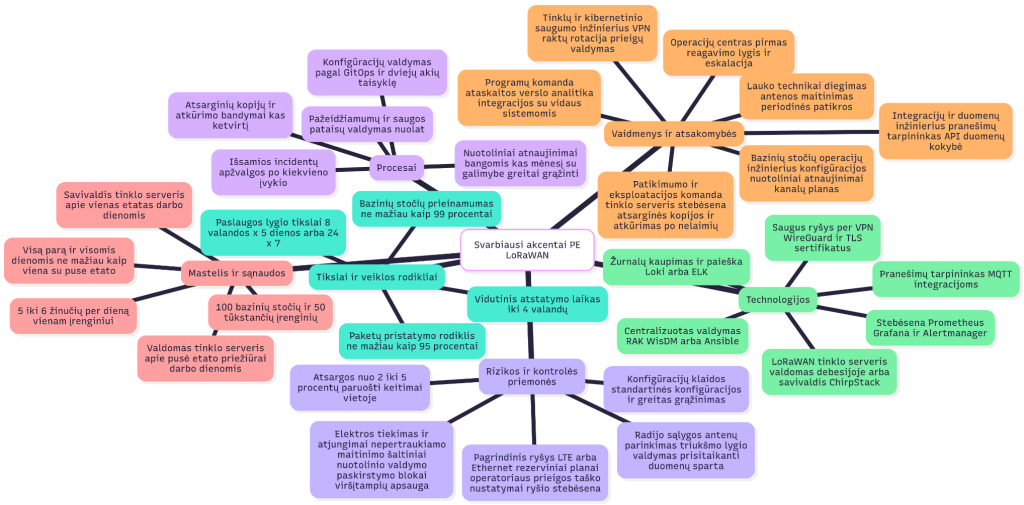
Transporto sluoksnyje LoRaWAN prieigos stotys sudaro atskirą VPN domeną. Visi RAK ar kitos prieigos stotys tuneliais jungiasi į centrinį VPN koncentratorių, naudodami WireGuard arba IPsec su TLS pagrįstu autentifikavimu. Tai leidžia pilnai užšifruoti eismą tarp celių ir branduolio, centralizuotai taikyti ugniasienes ir riboti prieigą. NB-IoT įrenginiai duomenis perduoda per operatoriaus branduolinį tinklą, naudojant privatų APN ir/ar papildomą VPN tunelį į duomenų centrą. Taip užtikrinama, kad NB-IoT telemetrija keliauja ne per viešą internetą, o per valdomą, izoliuotą kanalą. Šiame lygyje svarbu, kad LoRaWAN ir NB-IoT keliai nėra maišomi – jie susikerta tik ten, kur pradeda veikti IoT logika.

IoT branduolyje įrenginiai tampa vienodomis žinutėmis. LoRaWAN prieigos stočių srautą apdoroja LoRaWAN Network Server – pavyzdžiui, The Things Stack arba ChirpStack su Network ir Join funkcijomis. Čia atliekamas frekvencijų, ADR, įrenginių autentifikavimo ir sesijų valdymas, skaičiuojami counter’iai, tikrinamas MAC lygmuo. NB-IoT pusėje veikia atskiras ingest adapteris – tai gali būti HTTP/MQTT klientas, parsiduodantis operatoriaus teikiamus pranešimus ir transformuojantis juos į vienodą telemetrijos formatą. Abu šie komponentai – LNS ir NB-IoT ingest – duomenis paduoda į vidinį žinučių sluoksnį, kuriame dirba MQTT ir, jei reikia, Kafka klasteris. Šis sluoksnis ir yra „stuburas“, kuriuo dalijasi visos aplikacijos: MDMS, billing, ataskaitos, API, duomenų bazės ir analitika. Tokiu būdu naujos programos jungiasi prie vieno, stabilaus protokolo, o ne tiesiai prie prieigos stočių ar operatoriaus.

Stebėsenos ir žurnalų blokas apima visus sluoksnius. LoRaWAN LNS, VPN koncentratorius, NB-IoT ingest ir kiti branduolio komponentai turi Prometheus eksporterį, iš kurio renkami metrikų srautai – paketo sėkmės rodikliai, prieigos stočių apkrovos, MQTT eilės, NB-IoT klaidų kodai. Šios metrikos vizualizuojamos Grafana skydeliuose, o Alertmanager taisyklės generuoja aliarmus pagal SLA ir KPI, pavyzdžiui, kai sėkmingų uplink dalis krenta žemiau nustatytos ribos. Žurnalų sluoksnyje kaupiami sisteminiai ir aplikaciniai logai Loki arba ELK platformoje, leidžiant koreliuoti incidentus tarp LoRaWAN, NB-IoT ir aplikacijų. Ant šio pagrindo dirba NOC on-call komanda arba SIEM sistema, kuri prižiūri incidentus, eskalacijas ir NIS2 ataskaitas.

Valdymo ir konfigūracijų blokas sujungia infrastruktūrą į vientisą valdomą objektą. Prieigos stočių parkas administruojamas per RAK WisDM, Ansible ar panašią konfigūracijų valdymo sistemą – tai leidžia masiškai atnaujinti firmware, keisti kanalų planus, stebėti statusą ir atlikti roll-back, jei OTA atnaujinimai nepavyksta. Greta veikia CMDB, kur registruojami prieigos stočių serverių, sertifikatų ir programinės įrangos versijų įrašai. Tai tampa vienu iš pagrindinių įrodymų šaltinių auditams – čia matoma, koks įrenginys kur prijungtas, kokiu sertifikatu pasirašytas ir kokia konfigūracija galioja.

Tokia architektūra aiškiai atskiria radijo technologijas, transporto mechanizmus ir aplikacinę logiką. LoRaWAN, su maždaug 45 bazinėmis stotimis, ekonomiškai aptarnauja apie 70 % įrenginių ir užtikrina gerą vidaus aprėptį tankiuose miestuose, o NB-IoT per operatoriaus tinklą patikimai užpildo likusias 30 % geografiškai sudėtingų ar pavienių vietų. VPN ir privatus APN suteikia end-to-end saugumo sluoksnį, LNS ir NB-IoT ingest centralizuoja protokolų specifiką, o vidinis MQTT/Kafka sluoksnis suteikia aiškią integracijos sąsają visoms verslo aplikacijoms. Stebėsenos ir klaidų įrašų saugojimo blokas leidžia laiku pastebėti anomalijas ir vykdyti NIS2/GDPR reikalavimus, o valdymo ir CMDB sluoksniai užtikrina, kad tinklas yra ne tik techniškai veikiantis, bet ir valdomas bei audituojamas.



17 Pav. LoRaWAN diegimo situacijos analizė PE aptarnaujamų klientų Lietuvos regionuose

Rekomenduotina architektūrą įdiegti etapais: pirmiausia sukurti branduolį ir stebėsenos ir sistemos matomumo užtikrinimas, tada laipsniškai masiškai jungti LoRaWAN prieigos stotis ir NB-IoT ingest, galiausiai – praplėsti aplikacijų pusę ir formaliai aprašyti SLA bei saugumo politiką. Taip perėjimas nuo pilotinės į gamybinę aplinką bus valdomas, o kiekvienas žingsnis turės aiškius matavimus ir grįžtamąjį ryšį.

OPTIMIZUOTOS SPRENDINIŲ VISUMOS APRAŠAS [S-1.1.3]

Šiame poskyryje suformuluojama siūloma technologinių sprendinių visuma, paremta ataskaitoje atlikta aprėpties analize, ekonominiu LoRaWAN ir NB-IoT palyginimu bei eksploatacijos modelių (SaaS/hibrydas/self-hosted) įvertinimu. Optimizacijos tikslas – pasiekti reikiamą vidaus aprėptį ir duomenų pilnumą, kartu išlaikant mažiausią praktinį TCO ir valdomą eksploatacijos riziką.

Siūloma sprendinių visuma (komponentai):

Lauko lygmuo - LoRaWAN skaitikliai / siųstuvai ten, kur pasiekiama stacionari miesto aprėptis, ir NB-IoT skaitikliai „brangiuose“ objektuose (rūsiai, ekranuotos vietos, nutolę taškai), kad nereikėtų neproporcingai tankinti LoRaWAN infrastruktūros.

Transporto lygmuo - LoRaWAN bazinių stočių (gateway) tinklas su centralizuotu valdymu ir saugiais tuneliais; NB-IoT daliai – operatoriaus APN/VPN architektūra ir aiškiai apibrėžtas SLA (aprėptis, prieinamumas, žurnalai).

IoT branduolys - LoRaWAN Network Server (pagal pasirinktą eksploatacijos modelį) ir NB-IoT ingest grandis, suvienodinanti įrenginių pranešimus į bendrą įvykių/telemetrijos schemą; žinučių sluoksnis (MQTT ir/ar Kafka) duomenų srautų atskyrimui ir masteliui.

Duomenų sluoksnis - MDMS/MDM, laiko eilučių saugykla (TimeSeries DB) bei ilgalaikis archyvas (SQL/Data Lake), kad būtų užtikrintas matavimų atsekamumas, auditas ir VEE (validacija, įvertinimas, redagavimas) procedūros.

Atvaizdavimas ir integracijos - vidiniai portalai / valdymo ekranai, ataskaitų generavimas, REST/GraphQL API integracijoms su apskaitos ir atsiskaitymų sistemomis.

Stebėsena ir eksploatacija: centralizuotas KPI/SLA monitoringas (metrikos + žurnalai), incidentų valdymas ir DR pratybos, kad sutrikimai būtų identifikuojami anksti ir sprendžiami su minimaliais OPEX kaštais.

Tokiu būdu 70/30 LoRaWAN–NB-IoT santykis traktuojamas kaip ekonomiškai racionalus kompromisas: LoRaWAN užtikrina mastelį ir mažą vieneto kainą, o NB-IoT panaudojamas tik ten, kur LoRaWAN infrastruktūros tankinimas taptų brangiausia TCO dedamąja.

DUOMENŲ PRIĖMIMO, KAUPIMO IR ATVAIZDAVIMO SISTEMOS FUNKCINIS PROJEKTAS [S-1.1.4]

Duomenų priėmimo ir kaupimo sistemos projektas apibrėžiamas kaip vieningas „IoT branduolys“, į kurį sueina tiek LoRaWAN, tiek NB-IoT kanalai, o aukštesniuose sluoksniuose veikia bendri saugos, stebėsenos ir integracijų principai. Funkciškai sistema projektuojama taip, kad keičiantis įrenginių parkui (pavyzdžiui, didėjant NB-IoT arba atsirandant LTE-M) nereikėtų perdaryti duomenų sluoksnio ir verslo sistemų integracijų.

Rekomenduojamas end-to-end duomenų srautas:

Matavimas sugeneruojamas skaitiklyje ir siunčiamas per pasirinktą radijo technologiją (LoRaWAN arba NB-IoT) pagal nustatytą periodiką.

Ryšio sluoksnyje pranešimai priimami LNS (LoRaWAN) arba operatoriaus tinkle (NB-IoT) ir perduodami į ingest komponentą (per API/brokerį).

Ingest sluoksnyje vykdomas pranešimų autentiškumo ir integralumo tikrinimas, deduplikavimas, laiko žymų normalizavimas ir formatų suvienodinimas.

Žinučių sluoksnyje (MQTT/Kafka) pranešimai išskaidomi į temas (pvz., pagal miestą, įrenginių tipą, matavimo rūšį), kad atskiri moduliai galėtų prenumeruoti tik jiems reikalingus srautus.

MDMS/MDM atlieka VEE procedūras (validacija, praleistų reikšmių atkūrimas pagal archyvus/„backfill“, anomalijų detekcija) ir paruošia duomenis atsiskaitymams.

Duomenys saugomi laiko eilučių ir ilgalaikėse saugyklose; ataskaitos ir vizualizacijos generuojamos iš standartizuotų API bei duomenų modelio.

KPI/SLA stebėsena nuolat tikrina duomenų pilnumą ir vėlinimą; kai viršijamos ribos – inicijuojamas incidentų valdymas ir trikčių šalinimo seka.

RIZIKŲ VERTINIMAS IR DUOMENŲ TIEKIMO SUTRIKIMŲ VALDYMO PRIEMONĖS [S-1.1.5]

Šiame skyriuje išskiriamos pagrindinės duomenų tiekimo sutrikimų rizikos ir pateikiamos praktinės priemonės, kurios mažina nepatogumą vartotojams (neteisingi / pavėluoti atsiskaitymai, ginčai dėl suvartojimo) ir kaštus šilumos tiekėjui (papildomi vizitai, rankiniai nuskaitymai, incidentų valdymo darbo sąnaudos). Analizė remiasi ataskaitoje aprašyta aprėpties modeliavimo logika, KPI/SLA priėmimo kriterijais ir siūloma end-to-end architektūra.

PAGRINDINĖS SUTRIKIMŲ RIZIKOS (KLASĖS):

Radijo aprėpties spragos ir „šešėlinės“ zonos (ypač rūsiai, tankūs kvartalai, ekranavimas): rizika pasireiškia matavimų praradimais ir didesniu vėlinimu.

Bazinių stočių / ryšio mazgų gedimai (maitinimas, interneto uplink, antenų mazgai): rizika sukelia lokalias duomenų „duobes“ ir reikalauja greito reagavimo.

Operatoriaus tinklo ar APN/VPN sutrikimai (NB-IoT): rizika pasireiškia masiniu vėlinimu, ypač jei nėra aiškių SLA ir žurnalų.

Įrenginių energijos resurso išsekimas arba netinkamai parinkta siuntimo periodika: rizika lemia tylų įrenginių „iškritimą“ ir brangius planinius/avarinus vizitus.

Platformos/LNS/ingest komponentų prastovos arba našumo ribos: rizika pasireiškia duomenų kaupimosi eilėse, vėlinimu ir neišpildytu priėmimo KPI.

Duomenų integralumo klaidos (dublikatai, laiko poslinkiai, praradimai integracijoje): rizika sukelia VEE klaidas ir didina ginčų/neteisingo sąskaitų formavimo tikimybę.

Kibernetinio saugumo incidentai (raktų kompromitavimas, neteisėta prieiga, DoS): rizika gali sukelti duomenų praradimą, manipuliavimą arba paslaugų sutrikimą.

RIZIKŲ MAŽINIMO PRIEMONĖS IR POVEIKIS KAŠTAMS:

Aprėpties valdymas - LoRaWAN tinklo tankinimas pagal radioplaną, kritinių taškų perkėlimas į NB-IoT, o „rūsio“ atvejams – OMS/wM-Bus/M-Bus „fallback“ (mažina rankinių vizitų skaičių ir OPEX).

Redundancija ir atsarginės priemonės: kritinių gateway taškų dubliavimas, UPS/maitinimo kontrolė, atsarginių įrenginių sandėlis (mažina prastovų trukmę ir vartotojų nepatogumą).

SLA ir observability - KPI/SLA stebėsena (pilnumas, vėlinimas, klaidų santykis) su automatiniu aliarmavimu, incidentų klasifikavimu ir eskalavimu (leidžia sutrikimus aptikti per minutes, o ne per dienas).

Store-and-forward / archyvai - prietaisų archyvų ir VEE „backfill“ naudojimas praleistiems matavimams atkurti po ryšio atstatymo (mažina ginčų ir neteisingų sąskaitų riziką).

Energijos valdymas - energijos biudžetu pagrįstas siuntimo periodikos parinkimas, baterijos būklės telemetrija ir prevencinis keitimo grafikas (mažina avarinių vizitų kaštus).

DR ir atstatymas - atsarginių kopijų politika, duomenų bazių replikavimas, DR pratybos ir aiškus RPO/RTO tikslų nustatymas (mažina ilgų prastovų ir duomenų praradimo tikimybę).

Saugos kontrolės - raktų valdymas (HSM/rotacija), RBAC/SSO, audito žurnalai ir segmentuota infrastruktūra (mažina incidentų tikimybę ir jų kaštus).

Papildomai ENREADER TELEMETRIJOS SISTEMOS MODERNIZAVIMO ATASKAITOJE pateikiama detalizuota rizikų matrica senųjų ENReader įrenginių modernizavimo scenarijams; jos logika gali būti naudojama kaip rizikų registravimo šablonas ir bendro telemetrijos projekto rizikų valdymo priedas.

IŠVADOS

1. ES direktyvos (2018/2001 ir 2023/2413) įpareigoja iki 2026-02-21 visus centralizuotos šilumos vartotojų skaitiklius padaryti nuotoliniu būdu nuskaitomus; nepilnas įgyvendinimas reikštų tiek reguliacines rizikas, tiek prarastą naudą vartotojams.

2. AB „Panevėžio energija“ valdomas ~64 619 apskaitos prietaisų parkas yra technologiškai nevienalytis, dalis KVS ir ŠAP turi LoRaWAN/OMS, tačiau įvadiniai skaitikliai didele dalimi remiasi 2G GPRS, o duomenys kaupiami fragmentuotai, be vieningos MDMS sistemos.
3. Esamas LoRaWAN tinklas (4-6 bazinės stotys) jau šiandien patikimai aptarnauja apie 90 % PE dabar instaliuotų apskaitos įrenginių; pasitelkus parengtą radiotechninį antenų išdėstymo algoritmą, aprėptį galima padidinti iki reikiamo lygio su ribotu papildomų prieigos stočių kiekiu ir kontroliuojamomis CAPEX/OPEX sąnaudomis.
4. NB-IoT yra strategiškai reikalingas, bet neturėtų tapti vienintele technologija: dideli SIM kaštai ir jautrumas kainų pokyčiams daro NB-tik scenarijų brangiausiu TCO požiūriu, tačiau NB-IoT būtinas įvadiniams skaitikliams ir objektams, kurių ekonomiškai neapsimoka aptarnauti su LoRaWAN.
5. Mišrus modelis, kuriame NB-IoT dengia apie 20–30 % visų įrenginių (problemiški KVS + visi ŠAP), o likę įrenginiai naudoja LoRaWAN, už nedidelę papildomą kainą (0,36–0,70 mln. € per 10 metų) suteikia žymiai didesnį patikimumą, sumažina vizitų skaičių ir riziką dėl ryšio trikdžių, išlaikydamas TCO artimą LoRa-tik scenarijui.
6. Hibridinis eksploatacijos modelis – kai LNS ir flotilės valdymas (pvz., The Things Stack Cloud) perkamas kaip paslauga su aiškiu SLA, o ingestas, MDMS, analitika ir saugyklos valdomi nuosavoje ES debesijoje – geriausiai subalansuoja įgyvendinimo greitį, operacinę riziką ir TCO Panevėžio masteliui, paliekant kelią vėliau pereiti prie pilno self-hosted sprendimo.
7. Atvirojo kodo komponentais pagrįsta duomenų ir integracijų architektūra leidžia išvengti licencinių mokesčių, o apie 116 000 € CAPEX (NB-IoT/LoRa ingest, DB, API, monitoringas, CI/CD) yra pakankamas sukurti gamybinio lygio platformą, kuri gali būti plečiama didėjant įrenginių skaičiui.
8. Tinkamai suprojektuota end-to-end saugos architektūra (LoRaWAN OTAA, AES-128, TLS 1.2/1.3, raktų valdymas HSM, RBAC/SSO, auditų žurnalai) leidžia įvykdyti GDPR, NIS2, RED, MID ir būsimus CRA reikalavimus, tuo pačiu taikant „privacy by design“ ir duomenų minimizavimo principus.
9. Sėkmingam sprendimo eksploatavimui būtina nedidelė, bet nuolat dirbanti IT/OT komanda, atsakinga už LNS/MDMS priežiūrą, incidentų valdymą, DR pratybas ir SLA/KPI stebėseną; tai ypač svarbu svarstant perėjimą nuo hibridinio prie pilnai self-hosted modelio.
10. AB „Panevėžio energija“ turėtų: (1) suvienodinti duomenų bazes ir procesus (vieninga MDMS); (2) sutankinti LoRaWAN tinklą pagal parengtą modelį ir pradėti įvadinių ŠAP migraciją į LTE-M/NB-IoT; (3) įgyvendinti pilotinį hibridinį LNS sprendimą Panevėžio mieste; (4) po piloto priimti sprendimą dėl ilgalaikės architektūros, remiantis faktiniu TCO ir komandos pajėgumais; (5) pilnai užbaigti skaitiklių parko perėjimą prie nuotolinio nuskaitymo, užtikrinant teisinę ir technologinę atitiktį.

11. Įvertintos duomenų tiekimo sutrikimų rizikos ir suformuluotos mažinimo priemonės (aprėpties valdymas, KPI/SLA stebėsena, archyvai/„backfill“, DR ir sauga), siekiant sumažinti vartotojų nepatogumą ir eksploatacijos kaštus.