

RĪGAS TEHNISKĀ UNIVERSITĀTE
Energētikas un elektrotehnikas fakultāte
Industriālās elektronikas un elektrotehnikas institūts

Anatolijs ZABAŠTA

Doktora studiju programmas „Elektrotehnoloģiju datorvadība” doktorants

**DATORVADĪBAS METOŽU UN PIEEJU IZSTRĀDE KRITISKO
INFRASTRUKTŪRU SAVSTARPĒJĀS IETEKMES ANALĪZEI**

Promocijas darbs

Zinātniskais vadītājs
Dr. sc. ing., asoc. profesore
N. Kuņicina

Rīga 2014

Zabašta A. Kritiskās infrastruktūras datorvadības metožu izstrāde. Promocijas darbs. - R.:
RTU Izdevniecība, 2014.- 155 lpp.



Šis darbs izstrādāts ar Eiropas Sociālā fonda atbalstu projektā “Atbalsts RTU doktora studiju īstenošanai”.

PATEICĪBAS

Izsaku pateicību visiem, kuri ir atbalstījuši šā promocijas darba izstrādi. Vislielākā pateicība Industriālas Elektronikas un Elektrotehnikas institūta zinātniekiem: akadēmiķim profesoram Leonīdam Ribickim, profesoram Ivaram Raņķim un promocijas darba zinātniskajai vadītājai, asociētai profesorei Nadeždai Kuņicinai par konsultācijām tehniskajos un praktiskajos jautājumos, kā arī par atbalsta sniegšanu studiju laikā un promocijas darba izstrādē.

Pateicos RTU Doktorantu studiju daļas un Doktorantūras skolas darbiniekiem, Doktorantu studiju daļas vadītājam Laurim Biseniekam un projektu vadītājai Alīnai Galkinai par atbalstu un padomiem doktorantūras studiju laikā.

Pateicos profesoram Emiliano Casaliccio no universitātes "Roma Tor Vergata" un profesoram Jevgeņijam Osipovam no Lulea Tehnoloģijas Universitātes par atbalstu un padomiem zinātnisko misiju laikā.

Pateicos TELE2 radio tīkla vadītājam Artim Apinim un zinātņu doktoram, Augstsprieguma Tīkla AS elektroapgādes sistēmu inženierim Aleksandram Ļvovam par konsultācijām tehniskos jautājumos.

Izsaku pateicību saviem kolēģiem, ar kuriem es sadarbojos pētījumos un projektos: RTU doktorantam Kasparam Kondratjevam, Latvijas Interneta Asociācijas izpilddirektoram Viesturam Šeļmanovam - Plešam, Ventspils Augstskolas Inženierzinātņu institūta VSRC direktoram Valdim Avotiņam, Ventspils SIA Ūdeka Tehniskajam vadītājam Viesturam Otomeram.

Pateicos savai mīļai sievai par pacietību, sapratni un atbalstu visu studiju gadu garumā un promocijas darba izstrādē.

ANOTĀCIJA

Promocijas darba mērķis ir izstrādāt modeli, metodes un metrikas, kas ļautu kvantitatīvi novērtēt elektroapgādes un telekomunikāciju kritisko infrastruktūru ietekmi uz ūdensapgādes kritisko infrastruktūru un pārbaudīt izstrādātās pieejas pareizību ar reālās infrastruktūras piemēru.

Promocijas darba pirmajā nodaļā formulēta uzdevuma nostādne un analizētas zinātniskajā literatūrā aprakstītās dažādās pieejas, kuras izmanto, lai modelētu kritisko infrastruktūru savstarpējo atkarību.

Promocijas darba otrajā nodaļā tiek veikts kritisko infrastruktūru modelēšanai un imitācijai veltīto pētījumu pārskats. Minētajā nodaļā tiek izvērtētas pētījumos un projektos pielietotās metrikas un to saistība ar izvēlēto modeli un atkarības veidu.

Promocijas darba trešajā nodaļā tiek pētīti kritisko infrastruktūru mijiedarbības kvantitatīvie raksturojumi un veikta metriku analīze un klasifikācija.

Promocijas darba ceturtajā nodaļā tiek veikta metriku aprobācija, izpētot triju infrastruktūru (elektroapgādes, telekomunikāciju un ūdensvada tīkls) savstarpējo ietekmi, pielietojot imitācijas modeli. Nodaļa atspoguļo veikto imitācijas rezultātu analīzi un izdarītos secinājumus par izmantotajām metrikām un par iespēju veikt infrastruktūru parametru optimizāciju, lai samazinātu savstarpējās ietekmes negatīvo efektu.

Promocijas darba piektajā nodaļā analizētas problēmas, ieviešot praksē kritisko infrastruktūru datorvadības metodes, pielietojot bezvadu sensoru tīklus, un aprakstīti tehniskie risinājumi, kuri izstrādāti projektos.

Promocijas darbs uzrakstīts latviešu valodā uz 155 lpp., satur ievadu, piecas nodaļas, secinājumus, piecus pielikumus, 57 attēlus un 8 tabulas. Izmantotās literatūras sarakstā ir atsauces uz 91 informācijas avotu.

ABSTRACT

The goal of the PhD thesis is to develop a model, methods and metrics that enable quantitative evaluation of electric power and telecommunications infrastructure critical impact on the water supply infrastructure, and to verify the correctness of the approach developed for a real infrastructure example.

In the first chapter, the task approach is defined and the literature that describes different approaches used to simulate the critical infrastructure interdependencies is analysed.

In the second chapter of the thesis, a research on carried out of critical infrastructure modelling and simulation studies is made, furthermore, applied metrics and their relationships with the model chosen and the type of dependencies, applied in research and projects, are evaluated.

The third chapter of the thesis examines the quantitative characteristics of the critical infrastructures interaction and performs the analysis and classification of metrics.

In the fourth chapter metrics approbation is done, exploring a specific example of the three infrastructures interdependences (electricity, telecommunications and water supply network), using the simulation model. The chapter conducts simulation analysis of the results and conclusions of the use of metrics and of possibility of the infrastructure parameters optimization to minimize the negative impact of the interdependencies.

The fifth chapter analyses the challenges faced implementing critical infrastructures computer control methods, using wireless sensor networks, and describes the technical solutions that are tailored in the reviewed projects.

The thesis is written in Latvian on 155 pages, contains an introduction, five chapters, conclusions, five annexes, 58 pictures and 8 tables. The bibliography contains references to 91 source of information.

АННОТАЦИЯ

Целью диссертации является разработка модели, методов и метрик, которые позволяют количественно оценить критическое влияние электроэнергетической и телекоммуникационной инфраструктуры на критическую инфраструктуру водоснабжения и проверить правильность подхода на реальном примере.

В первой главе определяется постановка задачи и проводится анализ научной литературы, описывающей различные подходы, используемые для моделирования взаимозависимости между критическими инфраструктурами.

Во второй главе диссертации сделан обзор исследований, посвященных моделированию и симулированию взаимодействия критических инфраструктур, и оценивается применение метрик.

В третьей главе диссертации исследуются количественные показатели взаимодействия критических инфраструктур и проводится анализ и классификация метрик.

В четвертой главе производится апробация метрик, когда с помощью имитационной модели исследуется взаимозависимость между тремя критическими инфраструктурами, анализируются результаты и делаются выводы об оптимизации параметров для минимизации взаимного негативного влияния между инфраструктурами.

В пятой главе анализируются проблемы реализации компьютерных методов контроля критических инфраструктур с использованием беспроводных сенсорных сетей и описываются технические решения, разработанные в рассмотренных проектах.

Диссертация написана на латышском языке на 155 страницах, содержит введение, пять глав, выводы, 5 приложений, 57 рисунков и 8 таблиц. В списке использованной литературы перечислен 91 источник информации.

SATURA RĀDĪTĀJS

Ievads.....	10
1. Metodes un pieejas kritisko infrastruktūru savstarpējās mijiedarbības analīzei.....	18
1.1. Uz topoloģiju balstīta pieeja.....	22
1.2. Holistiskā pieeja	23
1.3. Jauktā holistiskā – redukcionistiskā pieeja	24
1.4. Analītiskā pieeja.....	25
1.5. Imitācijas pieeja.....	26
1.6. Metriku loma	27
1.7. Secinājumi par pirmo nodaļu	27
2. Kritisko infrastruktūru mijiedarbības modeļu analīze	28
2.1. Uz topoloģiskās pieejas balstītais modelis	28
2.2. Uz analītiskās pieejas balstītais modelis	29
2.2.1. Analītiskā modeļa piemērs	30
2.3. Pakalpojumu dekompozīcijas modelis	32
2.3.1. Metodoloģija	32
2.3.2. Savstarpēju mijiedarbību modelēšana, izmantojot UML	35
2.3.3. Elektroapgādes, telekomunikācijas un ūdens apgādes infrastruktūras mijiedarbības modelēšanas piemērs Talsu teritorijā	36
2.4. Uz imitācijas pieejas balstītie modeli	39
2.4.1. Uz pakalpojumiem bāzētie modeli (SimCIP).....	40
2.4.2. Programmu aģentu modeli un federatīvie modeli (DIESIS).....	42
2.4.3. Piedāvājuma un pieprasījuma tipa modeļi (I2SIM)	43
2.5. Secinājumi par otro nodaļu.....	44
3. Metrikas kritisko infrastruktūru analīzei.....	46
3.1. Metriku izvēles pieejas	46
3.2. Atkarības novērtēšanas metrikas	48
3.3. Secinājumi par metriku izvēli	51
4. Elektroapgādes, telekomunikāciju un ūdensapgādes tīklu mezglu mijiedarbības modeļa izveide un simulācija.....	53
4.1. Scenārija pamatojums un apraksts	53
4.2. Modeļa parametru izvēle un pamatojums	55
4.2.1. Ūdensapgādes tīkla mezglu parametrus noteikšana	55
4.2.2. Elektroapgādes tīkla mezglu parametru izvēles pamatojums.....	57

4.2.3. Telekomunikācijas (GSM) tīkla mezglu parametru izvēles pamatojums...	58
4.3. Modeļa apraksts	59
4.4. Eksperimenta rezultātu polinomiāla aproksimācija.....	63
4.5. Secinājumi par ceturto nodaļu	65
5. Kritiskas infrastruktūras datorvadības metodes, pielietojot bezvadu sensoru tīklus.....	67
5.1. Talsu novada datorizētas ūdenssaimniecības vadības kontroles sistēmas apraksts	68
5.2. Rīgas Situms pilot-projekta sistēmas apraksts.....	72
5.2.1. Risinātie problēmjautājumi.....	74
5.2.2. Datu pārraide	74
5.2.3. Rezerves barošana	76
5.2.4. Mērījumu datu integrācijas ar esošām IT sistēmām	77
5.3. Bezvadu sensoru tīkla tehnoloģijas pētījumi un eksperimenti Ventspilī.....	78
5.3.1. Ūdensvada izmēģinājuma tīkla segmenta izvēle	78
5.3.2. Sensori - transiveri.....	81
5.3.3. Retranslācijas princips	82
5.3.4. Antenas dizains pilsētvidei	84
5.3.5. Ethernet vārteja - koncentrators.....	86
5.3.6. Izmēģinājuma tīkla galīgais variants	92
5.3.7. “Smārt Meter” informācijas sistēmas arhitektūra.....	93
5.3.8. Noplūžu meklēšanas metožu izpēte.....	95
5.3.9. E-pakalpojumi sistēmas lietotājiem.....	99
5.4. Secinājumi par piekto nodaļu	100
Darba kopējie secinājumi	102
Izmantota literatūra	104
Pielikumi... ..	110

DARBĀ LIETOTIE SAĪSINĀJUMI

AMI – Progresīva mērīšanas infrastruktūra (*Advanced Metering Infrastructure*)

AMR – Automātiskā mērītāju nolasīšana (*Automatic Meter Reading*)

CAIDI – Klientu vidējā pārtraukuma ilguma indekss (*Customer average interruption duration index*)

EKI – Eiropas kritiskās infrastruktūras

FAK – Fiziskās atkarības koeficients

FRI – Fiziskās atkarības relatīvais ilgums

IEEE – *Institute of Electrical and Electronics Engineer*

KI – Kritiskā infrastruktūra

KIS – Kritiskās infrastruktūras sistēma

MDA – Uz modeļiem balstīta arhitektūra (*Model Driven Architecture*)

MTTF – Vidējais laiks starp bojājumiem (*Mean Time to Failure*)

RBDL – Rezerves barošanas avota darbības laiks

RBNL – Rezerves barošanas avota nomainīšanas laiks

SAIDI – Sistēmas vidējais pārtraukuma ilguma indekss (*System Average Interruption Duration Index*)

SAIFI – Sistēmas vidējais pārtraukuma biežuma indekss (*System Average Interruption Frequency Index*)

SCADA – Uzraudzība, pārvaldīšana un datu iegūšana (*Supervisory Control and Data Acquisition*)

SOA – Uz pakalpojumiem orientēta arhitektūra (*Service-Oriented Architecture*)

ŪMDL – Ūdensvada tīkla mezglu vidējais dīkstāves laiks

UML – Vienota modelēšanas valoda (*Unified Modeling Language*)

ŪST – Ūdensvada sadales tīkls

VDL – Vidējais dīkstāves laiks

XML – Paplašināma iezīmēšanas valoda (*Extensible Markup Language*)

IEVADS

“Kritiskās infrastruktūras” jēdziens atbilstoši EK direktīvai 2008/114/EC [27] tiek definēts šādi: „Kritiskās infrastruktūras ir objekti, sistēmas vai tās daļas, kuras ir būtiskas, lai nodrošinātu svarīgu sabiedrības funkciju darbību, cilvēku veselības aizsardzību, drošumu, cilvēku ekonomisko vai sociālo labklājību, un kuru darbības traucējumi vai iznīcināšana būtiski ietekmētu attiecīgo valsti, jo tā nespētu turpmāk nodrošināt šo funkciju īstenošanu”.

Kritiskās infrastruktūras sistēmu (KIS) uzraudzība, vadība un drošība kļuvusi svarīga, jo sistēmas kļūst arvien lielākas, sarežģītākas un arvien vairāk ietekmē viena otru. Sakarā ar informāciju un komunikāciju tehnoloģijas pielietošanu tādas KIS kā *elektroapgādes, telekomunikācijas, ūdens apgādes un transporta vadības sistēmas* kļuvušas savstarpēji atkarīgas un vairāk pakļautas bojājumiem, dabas stihijām un kibernetiskiem uzbrukumiem [58].

Kritisko infrastruktūru drošība, stabilitāte un uzticamība ir cieši saistīta ar *savstarpējās mijiedarbības* fenomenu. Tiešās atkarības mehānismus ir salīdzinoši viegli noteikt, modelēt un analizēt, gadījumos, kad infrastruktūru apjomi ir pietiekami mazi. Tomēr, ja mijiedarbojas vairākas liela mēroga kritiskās infrastruktūras, tad tiešās saites starp tās elementiem veido atgriezeniskās saites, kas var radīt savstarpējas ietekmes. Šādas savstarpējas ietekmes ir sarežģīti formalizēt, un tās kļūst aprakstāmas tikai tad, kad kritiskā infrastruktūra tiek izpētīta un modelēta [71].

Literatūrā var atrast vairākas definīcijas jēdzieniem "*atkarība*" (“dependence”) un "*savstarpējā atkarība*” (*savstarpējā ietekme*) (“interdependence”), tomēr biežāk tiek lietotas šādas definīcijas: *atkarība (ietekme)* ir infrastruktūras spēja ietekmēt citas infrastruktūras stāvokli. Infrastruktūra A ir atkarīga no infrastruktūras B, ja izmaiņas vismaz vienā infrastruktūras “B” daļā ir spējīgas ietekmēt un mainīt stāvokli (darbību, raksturlielumus, īpašības u.c.) “A” infrastruktūrā. Šāds fenomens tiek saukts par *vienvirziena ietekmi*.

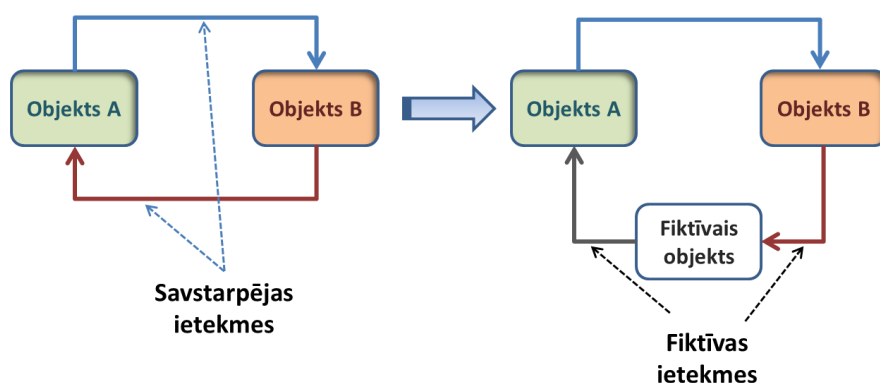
Jēdziens *savstarpējā atkarība (savstarpējā ietekme)* reprezentē divvirzienu ietekmi starp divām vai vairākām infrastruktūrām gadījumos, ja katras infrastruktūras stāvoklis ir ietekmējams vai ir korelējams ar citas infrastruktūras stāvokli.

Jēdzienu „*atkarība*” formulē arī kā ietekmes virzienu (pievienojot, piemēram, kavēšanās vai latentuma laiku) un tā lielumu, līdzīgi kā vektoru. Formalizējot ietekmes, jāņem vērā tas, ka eksistē vairāki apslēptie ietekmju virzieni, kas nav definēti, tāpēc parasti tiek novērtētas tikai *skaidras un tiešas atkarības*. Šajā darbā uzmanība ir vērsta tikai uz parādībām, kas ir saistītas ar kritisko infrastruktūru *pakalpojumu kvalitātes un/vai funkcionalitātes degradāciju*.

Šajā pētījumā tiek pielietots pieņēmums, kuru definēja darbā [30]. Proti, „*savstarpējās atkarības*” definīcija rada loģisku cēloņu un sekū pretrunu, līdz ar to tā tika vienkāršota,

aizvietojot katru savstarpējo ietekmi ar vienkāršām ietekmēm, ieviešot fiktīvas saites (skat. 1. attēlu, kur orientētās saites fiktīvajā kontūrā attēlo papildus vienkāršās ietekmes). Līdz ar to turpmāk savstarpējās ietekmes tiks izskatītas, ņemot vērā 1.attēlu. Tādēļ dažos gadījumos ir jāpaļaujas uz kādu abstraktu parametru, korelējot analizējamo objektu stāvokli, lai novērtētu ietekmes stiprumu. Citos gadījumos, lai novērtētu ietekmes, būtu iespējams tikai varbūtības apraksts. Atsevišķos gadījumos pilnīgs matemātiskais apraksts var tikt izveidots, tāpēc ietekme (atkarība) būs skaidri definēta.

Visbeidzot, ir lietderīgi atzīmēt, ka jēdziens *atkarība* atšķiras no jēdziena *risks*. Bieži vien tiek jaukta šo divu jēdzienu izmantošana: *ievainojamības analīze* un *riska analīze* tiek uzskatīta par līdzvērtīgu jēdzienam *atkarības analīze*. Tomēr jāuzsver, ka *risks* ir saistīts ar notikuma sekām un tā varbūtību, bet *atkarība* ir saistīta ar notikumu izplatīšanās cēloņiem. Turklāt spēcīga savstarpējā atkarība nenozīmē vienmēr lielu risku un otrādi [30].



1. att. Vienkāršota savstarpējas ietekmes shēma (pārveidota shēma no [30])

1. attēlā redzamajā otrajā blokā attēlotais viens fiktīvais loģiskais mezgls un divas fiktīvās saites ir izmantotas, lai novērstu loģisko nekoncekvenci.

Vēl viena svarīga teorētiska konstrukcija, kas ir pielietota, [51, 30] ir savstarpējās atkarības *kārtība*. Parasti analizējamais notikums ir notikumu ķēdes galīgais rezultāts. Lai gan „īsta” vai sākotnēja cēloņa meklēšana ir svarīga, tomēr šā pētījuma uzdevums ir identificēt konkrētu notikumu kopu, kura veidojas ķēdes reakcijas rezultātā. Šāda vienkāršu notikumu kopa īsteno atkarības kārtību. Bieži vien tikai pirmās kārtas atkarības, tas ir tiešas atkarības, tiek izmantotas analīzei.

Tēmas aktualitāte

Kritisko infrastruktūru aizsardzība mūsu laikos nozīmē ne tikai aizsardzību pret uzbrukumiem, bet arī pakalpojumu sniegšanas nodrošināšanu un dīkstāvju risku samazināšanu katrā infrastruktūrā. Ir zināmi vairāki piemēri, kad avārijas kādā no kritiskajām infrastruktūrām ir radījušas problēmas citās infrastruktūrās.

2003. gadā 14. augustā kļūdas vadības sistēmas programmatūrā kļuva par vienu no ievērojamākās elektroapgādes avārijas cēloņiem ASV ziemeļaustrumos, rietumdaļā un Kanādā, Ontārio provincē [21]. Neskatoties uz to, ka daži nozīmīgi pakalpojumi turpināja funkcionēt, smagi bija cietuši mobilie telefona sakari, ūdens apgādes sistēmas un dzelzceļu transporta sistēma.

2003. gada 25. janvārī datora vīruss „SQL Slammer warm” [80] sāka izplatīties visā pasaulē, inficējot vairāk nekā 75000 datorus jau pirmajās 10 minūtēs, tādējādi radot haosu internetā.

2007. gadā notika viens no lielākajiem „Distributed Denial of Service” (DDoS) uzbrukumiem Igaunijā [19], piespiežot valdību slēgt vairākus no savām galvenajām IT sistēmām.

Saskaņā ar Latvijas Informācijas tehnoloģiju drošības incidentu novēršanas iestādes datiem (CERT) aptuveni 3300 IP adreses tika inficētas 2011. gadā. Šajā gadā CERT nācās izskatīt vairāk nekā 15000 drošības incidentu [38].

Apzinoties topošos riskus, Eiropadome 2004. gada jūnijā pieņēma lēmumu par kritisko infrastruktūru aizsardzības stratēģijas sagatavošanu. 2008. gada Eiropadome sagatavoja direktīvu ar mērķi veicināt Eiropas kritiskās infrastruktūras (turpmāk EKI) aizsardzības uzlabojumus. Direktīva aicina izstrādāt vienotu metodiku, ar ko identificētu un klasificētu apdraudējumus un draudus infrastruktūras objektiem un to neaizsargātību [27]. Savukārt 2009. gadā Eiropas Komisija pieņēma paziņojumu par informācijas kritiskās infrastruktūras aizsardzību pret atteikumiem un uzbrukumiem un izstrādāja rīcības plānu ar mērķi pastiprināt taktisko un operatīvo sadarbību starp ES valstīm [28].

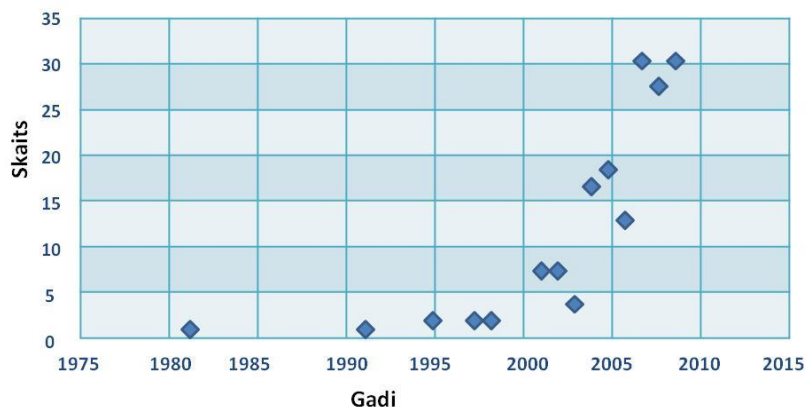
Mūsdienās elektroapgādes, siltumapgādes un ūdensapgādes nozarēs informācijas un komunikācijas tehnoloģijas (IKT) tiek izmantotas galvenokārt, lai informētu klientus par tarifiem vai nodrošinātu avārijas un klientu apkalpošanas dienestus. Sakarā ar automatizētu mērījumu datu nolasīšanas sistēmu attīstību ūdens un siltuma sadales tīklos un viedo elektrības mērītājus uzstādīšanu pie klientiem IKT nozīme strauji pieaug. Piemēram, internets tiek izmantots ne tikai kā mājaslapa klientu informēšanai, bet arī kā tīmekļa saskarne, lai piekļūtu mērījumu datiem un pakalpojumiem, un tādēļ sistēmas lietotāju skaits strauji pieaug. Sakarā ar augošo pārraidīto datu apjomu palielinājas atkarība no telekomunikāciju un interneta pakalpojumu sniedzējiem, tāpēc datu drošība un integritāte kļūst par ļoti svarīgu aspektu komunālajiem dienestiem un enerģijas piegādātājiem [81]. Šādos apstākļos pieaug nepieciešamība pēc metodēm un rīkiem, kas ļautu infrastruktūras pārvaldītājiem izvērtēt un prognozēt savas kritiskās infrastruktūras darbību

apstākļos, kad citās saistītajās infrastruktūrās notiek kļūmes, avārijas vai pakalpojumu kvalitātes pazemināšanās.

Šajā pētījumā aprakstītā metode palīdzēs kritisko infrastruktūru pārvaldītājiem, kas darbojas kopējā teritorijā, novērtēt savstarpējo infrastruktūru ietekmi un plānot riska samazināšanas pasākumus. Piemēram, ja elektroapgādes operators ir informēts par savas infrastruktūras ietekmi uz telekomunikāciju, transporta vai ūdens apgādes kritiskajām infrastruktūrām, tas var noteikt atjaunošanas pasākumu prioritātes ārkārtas situācijās. Vai ūdens piegādātājs, apzinoties elektroapgādes pārtraukumu riskus, var pieņemt lēmumu par rezerves barošanu ūdens apgādes tīkla mezgliem.

Literatūras apskats

Zinātniskā un praktiskā interese par infrastruktūru savstarpējo ietekmi aug pēdējos gados. Ka redzams 2. attēlā, publicēto dokumentu apjoms šajā jomā ir ievērojami palielinājies kopš 2001. gada, sasniedzot maksimālu līmeni laika posmā no 2007. gada - 2009. gadam. Faktiski, 95% no visiem dokumentiem, kas pēta infrastruktūru savstarpējo atkarību, ir publicēti pēdējo 10 gadu laikā [68].



2.att. Publikāciju skaits, kas ir veltīts kritisko infrastruktūru savstarpējas atkarības jautājumiem, G. Satumtira et al [68].

Galvenie jautājumi, kas būtu jārisina, lai veiktu korektu kontroli un pārvaldību, ir infrastruktūru identifikācija, uzvedības prognozēšana, optimizācija, savlaicīga reaģēšana uz izmaiņām, koordinācija un sadarbība starp KI operatoriem, kā arī defektu lokalizācija un novēršana [80].

No infrastruktūru savstarpējās atkarības viedokļa enerģētika, telekomunikācijas, bankas un finanšu institūcijas, transports un loģistika, kā arī citas infrastruktūras kļūst arvien vairāk pārslogotas, un arvien vairāk ievainojamas pret kļūmēm, kas izplatās caur un starp tām.

Galvenais uzdevums ir izvairīties no kļūmju plašas izplatīšanas lavīnveida un interaktīvas ietekmes efekta dēļ [21].

Kiberuzbrukumu seku analīze rāda, ka ir nepieciešams modelēt un analizēt savstarpējās attiecības, kas pastāv infrastruktūrās un starp infrastruktūrām [33]. Šīs atkarības bieži vien ir netiešas, slēptas un slikti saprotamas infrastruktūras īpašniekiem un operatoriem, kā arī attiecīgas jomas speciālistiem. Turklāt, palielinoties kritiskās infrastruktūras modelēšanas sistēmas detalizācijas pakāpei, šādu modeli kļūst grūtāk apstiprināt galvenokārt tādēļ, ka trūkst kvantitatīvu un atbilstošas detalizācijas datu [61]. Tas nav pārsteigums, kāpēc pēdējos gados daudzi pētnieki ir koncentrējušies uz savstarpēji atkarīgu infrastruktūru modelēšanu un analīzi [70].

Casalichio at al. savā rakstā [16], iepazīstina ar taksonomiju, kas klasificē savstarpējās atkarības metrikas, pamatojoties uz to informācijas saturu, lēmumu atbalstu un riska analīzes spējas un izrēķināšanas izmaksām. Rinaldi [63], ierosināja klasifikāciju, pēc kuras atkarības tiek klasificētas: fiziskā, kibernetiskā, ģeotelpiskā un temporālā atkarība.

Strukturēta pieeja infrastruktūras uzticamībai, kas balstās uz draudu, kļūmju un traucējumu novērtējumu, ka arī atribūti un metodes šādas uzticamības novērtēšanai, ir izpētīta darbā [4]. Uz risku novērtēšanu balstīta metodoloģija, kuras mērķis ir uzraudzīt savstarpēji atkarīgus pakalpojumus, pamatojoties uz vispārīgu risku un nodrošināšanas līmeņiem, kas ļauj noteikt kritiskās infrastruktūras pakalpojumu drošības stāvokli, ir izstrādāta darbā [2].

Viens no MICIE projekta uzdevumiem bija metodoloģiju, algoritmu un rīku izstrāde, kas ļautu veikt kvantitatīvu risku un apdraudējumu novērtējumu, kas izriet no kritisko infrastruktūru savstarpējās ietekmes [22].

Kritiskās infrastruktūras un to savstarpējā atkarība tiek analizēta, un dažādas piemērotas modelēšanas metodes ir apskatītas darbā [63]. Metodes, lai labāk novērtētu un uzraudzītu kritiskās infrastruktūras un to mijiedarbību un lai prognozētu iespējamus riskus, ir izstrādātas darbā [69].

KI drošības modelēšanas pieeja ir apskatīta [2, 3]. Pieejas mērķis ir pārvērst reāli eksistējošas infrastruktūras informāciju par vispārinātu, abstraktu, ar riskiem saistītu informāciju. Risku novērtēšanas metodoloģija, kuras mērķis ir uzraudzīt savstarpēji saistītus pakalpojumus, pamatojoties uz vispārējiem riskiem un nodrošināšanas līmeņiem, izmantojot drošības īpašības: konfidencialitāti, integritāti un pieejamību, tika demonstrēta [82].

Bagheri [7] ierosināja izmantot „Unified Modeling Language” (UML), lai definētu modeli KI atkarības pētījumiem, kas veidotu labu pamatu kritisko infrastruktūru modelēšanai un

simulācijai ar programmu aģentu rīkiem. UML programmu aģentu modelis, kas atspoguļo ūdens sadales tīkla statisko struktūru un dinamiskās īpašības, tika aprakstīts [45].

Darba [40] autori piedāvā drošības aprēķināšanas metodes mūsdienu enerģētisko sistēmu plānošanai, tomēr autori neizskata enerģētisko sistēmu ietekmi uz kaimiņu kritiskajām infrastruktūrām gadījumā, ja notiek drošības rādītāju pasliktināšanās. Pilsētas vidējā sprieguma barošanas tīkla drošības novērtēšanas metodes un algoritmi ir pētīti [41]. Autori ir izstrādājuši metodes, kas apraksta elektriskās sadales tīkla un slodzes modeļus, kritērijus un formulas, lai aprēķinātu drošības līmeni, tomēr arī šis darbs nesniedz atbildi, kas notiek atkarīgajā kritiskajā infrastruktūrā, kad drošības līmenis degradē elektriskās sadales tīklu.

Zimmerman et al. viens no pirmajiem pētniekiem piedāvāja metrikas, lai kvantitatīvi mērītu savstarpējās ietekmes [78, 79]. Savā darbā [79] autori piedāvā metrikas kaskādes efekta noteikšanai saistībā ar elektroapgādes kļūmēm, piemēram, kaskādes relatīvo ilgumu.

Darbā [13], kritisko infrastruktūru modeļus klasificēja saistot ar datu pieejamību (detalizācijas pakāpi): topoloģiskais, analītiskais un imitācijas modelis. Papildus citām priekšrocībām imitācijas pieeja ļāva modelēt kritisku infrastruktūru sakabes un ietekmes daudz detalizētāk. Turklāt darbā [13] tika demonstrētās jaunas KI savstarpējās atkarības metrikas un to izmantošana topoloģiskā, analītiskā un imitācijas modelī.

Lai definētu savstarpējās atkarības indeksu, darbā [62] tiek izmantots abstrakts jēdziens „*neoperējamība*” un piedāvātas metrikas, kas ļauj matemātiski aprakstīt infrastruktūras *neoperējamības* aspektus.

Apskatītie piemēri rāda, ka, lai gan atsevišķas kritiskās infrastruktūras darbības izpēte ir kļuvusi par nobriedušu pētniecības jomu un ir pieejami analīzes rīki, spējīgi raksturot infrastruktūras darbību atbilstošā laika mērogā un ar dažādas abstrakcijas pakāpi, tomēr metodes un instrumenti, ar kuriem var analizēt neviendabīgas un savstarpēji saistītas kritiskās infrastruktūras, ir lielā mērā neattīstīti. Turklāt trūkst piemēru no reālās pasaules prakses, kur šādas metodes un instrumenti būtu pielietoti. Var nosaukt tikai atsevišķus pētījumus, kuros ir izpētītas vismaz divu infrastruktūru savstarpējās atkarības, piemēram, IRRIS (2006-2008.g) projekts, kurā tika izpētīta mijiedarbība starp elektrotīkliem un telekomunikācijas tīkliem; projekts DIESIS (2008.g), kurā tika imitēts Romas plūdu scenārijs no iepriekš minētā IRRIS projekta, un MIA (2010. g.) projekts, kurā tika izpētīta mijiedarbība starp elektrotīkliem un telekomunikācijas tīkliem.

Pētījuma mērķis

Promocijas darba mērķis ir izstrādāt modeli, metodes un metrikas, kas ļautu kvantitatīvi novērtēt elektroapgādes un telekomunikācijas kritisko infrastruktūru ietekmi uz ūdensapgādes

kritisko infrastruktūru gadījumos, kad servisa līmenis vai pakalpojumu pārtraukšana elektroapgādes un telekomunikācijas infrastruktūrā apdraud ūdens apgādes infrastruktūras darbību, un pārbaudīt izstrādātās pieejas pareizību ar reālas infrastruktūras piemēru.

Pētījuma uzdevumi

1. Izpētīt kritisko infrastruktūru savstarpējās ietekmes novērtēšanas metodes un piedāvāt metodi, kas ļautu novērtēt elektroapgādes un telekomunikācijas kritisko infrastruktūru ietekmi uz ūdens apgādes kritisko infrastruktūru pilsētās.
2. Piedāvāt metrikas, kas ļautu kvantitatīvi novērtēt elektroapgādes, telekomunikācijas un ūdens apgādes kritisko infrastruktūru savstarpējo ietekmi.
3. Izstrādāt simulācijas modeli, kas ļautu novērtēt elektroapgādes un telekomunikācijas kritisko infrastruktūru ietekmi uz ūdens apgādes kritisko infrastruktūru pilsētās gadījumos, kad servisa līmenis vai pakalpojumu pārtraukšana elektroapgādes un telekomunikācijas kritiskajā infrastruktūrā apdraud ūdens apgādes kritiskās infrastruktūras darbību.
4. Izmantojot imitācijas modeli un izstrādātās metrikas, kvantitatīvi novērtēt elektroapgādes un telekomunikācijas kritiskās infrastruktūras mezglu ietekmi uz ūdens apgādes kritiskās infrastruktūras mezgliem vienā Latvijas pilsētā.
5. Izpētīt tehniskos risinājumus, tehnoloģijas un veidus, kā tiek kontrolēts ūdens apgādes tīkla mezglu stāvoklis, izmantojot bezvadu sensoru tīklus.

Zinātniskā novitāte

1. Darbā ir izpētītas kritisko infrastruktūru savstarpējās ietekmes novērtēšanas metodes un tiek piedāvātas specifiskās metrikas, kas ļauj kvantitatīvi novērtēt elektroapgādes, telekomunikāciju un ūdens apgādes kritisko infrastruktūru savstarpējo ietekmi.
2. Darbā ir izstrādāts imitācijas modelis, kas ir balstīts uz moderno teoriju un tehnoloģijām, ar mērķi izpētīt kritisko infrastruktūru savstarpējo ietekmi.
3. Izmantojot imitācijas modeli, darbā ir eksperimentāli pārbaudīta jauna metode, kas ļauj izpētīt ūdensvada tīkla mezglu vidējā dīkstāves laika atkarību no rezerves barošanas avota darbības laika un rezerves barošanas avota nomainīšanas laika savstarpējas korelācijas noteikto parametru robežās, apstākļos, kad notiek elektroapgādes un telekomunikācijas tīkla dīkstāves.
4. Darbā izpētīti un izstrādāti jauni tehniskie risinājumi, kas ļauj kontrolēt ūdens apgādes tīkla mezglu stāvokli, izmantojot bezvadu sensoru tīklus.

Šis pētījums ir pirmais Latvijā un arī Baltijā, kur ir izstrādāts un eksperimentāli pārbaudīts modelis, kas imitē triju kritisko infrastruktūru savstarpējo ietekmi un kvantitatīvi mēra savstarpējās mijiedarbības.

Pētījuma metodes

Pētījuma gaitā tika izmantotas šādas zinātniskās metodes un paņēmieni: problēmas analīze, risinājumu hipotēzes izvirzīšana, analīze un sintēze, holistiskā – redukcionistiskā pieeja un modelēšana, infrastruktūru mijiedarbības modelēšana ar UML līdzekļiem, datormodelēšana un mijiedarbības imitācija MatLab[®] Simulink[®] vidē, vairāku kritēriju optimizācijas metode, matemātiskās statistikas metode, eksperimentu plānošana un apstrāde datorprogrammā EDAOpt.

Pētījuma gaitā bija jāņem vērā ierobežojumi: pirmkārt, nebija pieejami komerciālie mijiedarbības imitācijas riski, tāpēc modelēšanai un imitācijai tika izmatots inženieru – tehniskais modelēšanas rīks MatLab[®] Simulink[®]. Otrkārt, ierobežota pieeja datiem, kas raksturo elektroapgādes un telekomunikācijas tīkla servisa līmeni.

Darba rezultāti tika prezentēti un apspriesti deviņās starptautiskās zinātniskās konferencēs (skat. 1.Pielikumu).

Promocijas darba struktūra

Promocijas darbā ir piecas nodaļas.

Promocijas darba 1. nodaļā ir analizētas zinātniskajā literatūrā aprakstītās dažādās pieejas, kuras tiek izmantotas, lai modelētu kritisko infrastruktūru savstarpējo atkarību, ņemot vērā tādus faktorus, kādi ir visbūtiskākie attiecībā uz konkrētu infrastruktūru un izvēlēto modeli.

2. nodaļa atspoguļo kritisko infrastruktūru modelēšanai un imitācijai veltīto pētījumu pārskatu. Minētajā nodaļā tiek izvērtētas pētījumos un projektos pielietotās metrikas un to saistība ar izvēlēto modeli un atkarības veidu.

3. nodaļā autors pēta kritisko infrastruktūru mijiedarbības kvantitatīvos raksturojumus un ar šo mērķi veic metriku analīzi un klasifikāciju. Šīm nolūkam autors izmanto 2. nodaļā veikto modeļu analīzi un to izmantotās metrikas.

4. nodaļā tiek veikta metriku aprobācija, izpētot triju infrastruktūru (elektroapgādes, telekomunikācijas un ūdensvada tīkls) savstarpējo ietekmi, pielietojot imitācijas modeli. Nodaļā tiek veikta imitācijas rezultātu analīze un izdarīti secinājumi par izmantotām metrikām un par iespēju veikt infrastruktūru parametru optimizāciju, lai samazinātu savstarpējās ietekmes negatīvo efektu, tas ir “neoperējamības” fenomenu.

Promocijas darba piektajā nodaļā pētījuma autors analizē problēmas, ar kurām sastopas tehniskie speciālisti un pētnieki, kas ievieš praksē kritisko infrastruktūru datorvadības pārvaldības metodes, pielietojot bezvadu sensoru tīklus, un apraksta tehniskos risinājumus, kuri tiek izstrādāti apskatītajos projektos.

1. METODES UN PIEEJAS KRITISKO INFRASTRUKTŪRU SAVSTARPĒJĀS MIJIEDARBĪBAS ANALĪZEI

Šajā darbā tiek izmantota Rinaldi [61] ierosināta klasifikācija, pēc kuras atkarības tiek klasificētas šādi: *fiziskā, kibernetiskā, ģeotelpiskā un temporālā*:

- **Fiziskā** savstarpējā atkarība, ir tāda, kad vienas infrastruktūras izejas rezultāti kļūst par ieejām citai infrastruktūrai, piemēram, materiālu vai pakalpojumu ražošanas procesā.
- **Kibernetiskā** savstarpējā atkarība rodas, kad infrastruktūras statuss ir atkarīgs no datiem, nosūtītiem caur informācijas infrastruktūru.
- **Ģeotelpiskā** savstarpējā atkarība rodas, kad divas vai vairākas infrastruktūras ir ģeotelpiski savstarpēji atkarīgas, ja vietējās vides notikums var izraisīt vienlaicīgu stāvokļa maiņu visām infrastruktūrām. Piemēram, katastrofālie notikumi pilsētas teritorijā var izveidot korelētus traucējumus citās infrastruktūrās, tādās kā telekomunikāciju un elektroapgādes sistēmās.
- **Temporālās savstarpējās atkarības** jēdziens ir izmantots, lai kvantitatīvi izmērītu vienas infrastruktūras ietekmi uz otru, novērtējot pārtraukuma vai zaudējumu posma ilgumu un atbilstoši atjaunošanās posma ilgumu ietekmētajā infrastruktūrā. Šādi laika posmi var atšķirties no sekundēm (piemēram, elektroapgādes sistēmas darbības pārtraukumi), līdz stundām (attiecībā uz darbībām, kas ir saistītas ar ūdens piegādi, gāzes vai transporta sistēmām).

Lai arī atsevišķas infrastruktūras modelēšana ir pētīta un ir pieejami analīzes rīki, kas spētu aprakstīt konkrētās infrastruktūras darbību dažādos mērogos un ar dažādu abstrakcijas pakāpi, tomēr attiecībā uz heterogēnu infrastruktūru savstarpējās ietekmes analīzi izpētes rīki lielā mērā vēl nav attīstīti. Turklāt nav tik daudz piemēru, kur šādas teorijas un instrumenti būtu pielietoti reālajā praksē.

Atsaucoties uz minēto promocijas darba ievaddaļā, uzmanība ir vērsta tikai uz parādībām, kas ir saistītas ar kritisko infrastruktūru *pakalpojumu kvalitātes un/vai funkcionalitātes degradāciju*. Citiem vārdiem sakot, infrastruktūru ietekme un savstarpējā atkarība tiek raksturotas, pamatojoties uz to, ka kļūme (nejaušs notikums vai ļaunprātīgs uzbrukums) vienā infrastruktūrā vai tās sastāvdaļā izraisa funkcionalitātes degradāciju citā infrastruktūrā un tās sastāvdaļās.

Lai noteiktu savstarpējās atkarības indeksu, turpmāk tiks izmantots abstrakts jēdziens „*neoperējamība*”. *Neoperējamība* nozīmē infrastruktūras vai tās sastāvdaļas nespēju izpildīt tai paredzēto funkciju.

Darbā [22] tika piedāvātas metrikas, kas ļauj matemātiski aprakstīt infrastruktūru *neoperējamības* aspektus. Turpmāk *neoperējamības* efekts tiks apzīmēts ar burtu μ un atbilstoši *neoperējamības* līmenis ar x . Konkrēti, $x_\mu = 0$ nozīmē, ka infrastruktūras elements vai sastāvdaļa ir pilnībā funkcionējoša, savukārt $x_\mu = 1$ nozīmē, ka tas ir pilnīgi nespējīgs nodrošināt savu funkciju izpildīšanu.

Pamatojoties uz savstarpējās atkarības definīciju, var secināt, ka *neoperējamības* pozitīvais pieaugums vienā infrastruktūrā veicina *neoperējamības* pieaugumu otrā infrastruktūrā, kas tiek izteikts ar (1.1) [22]

$$\frac{A \Leftarrow B}{\mu_{A,i}^T, \mu_{B,j}^T} \rightarrow \Delta x_A(t) = \phi(t, x_A^0, x_B^0, \Delta x_B^0), \quad (1.1)$$

kur mainīgais $t \in [t_0, t_0+T]$, bet x_A^0 izsaka infrastruktūras A *neoperējamības* līmeni, kuru mēra ar metriku $\mu_{A,i}$ sākuma posmā pirms ietekmes no infrastruktūras B ; x_B^0 izsaka infrastruktūras B *neoperējamības* līmeni, kuru mēra ar metriku $\mu_{B,i}$ sākuma posmā pirms *neoperējamības* rašanas. Δx_A ir *neoperējamības* līmeņa izmaiņas infrastruktūrā A saistībā ar *neoperējamības* līmeņa palielinājumu infrastruktūrā B . Laiks t_0 ir moments, kad tika izraisīta *neoperējamība* infrastruktūrā B ; savukārt T ir laikposms, kurā tika novērots *neoperējamības* efekts.

Saskaņā ar šo definīciju, ir vienkārši nodefinēt ***atkarības indeksu***: *atkarības indekss* ir attiecība starp *neoperējamības* pieaugumu atkarīgajā infrastruktūrā pret *neoperējamības* pieaugumu ietekmējošajā infrastruktūrā. Tad indekss (1.2) ir mērāms kā *atkarības* pakāpe starp divām infrastruktūrām, kas reaģē uz *neoperējamības* izraisīšanu vienā no infrastruktūrām:

$$\delta_{A,B}^T = \left(\int_{t_0}^{t_0+T} \Delta x_A(\tau) d\tau \right) / \left(\int_{t_0}^{t_0+T} \Delta x_B(\tau) d\tau \right). \quad (1.2)$$

Jāņem vērā, ka *atkarības indekss* ir atkarīgs no liela parametru kopuma (1.3):

$$\delta_{A,B} = \delta_{A,B}(x_A^0, x_B^0, \Delta x_B^0, \Delta x_A, \eta_{A,i}, \eta_{B,j}, t_0, T). \quad (1.3)$$

Neoperējamības līmeņa izmaiņas infrastruktūrā A var izteikt attiecībā uz atkarību no infrastruktūras sastāvdaļām q . Infrastruktūra A ir atkarīga no sastāvdaļām q , respektīvi, kad pieaug *neoperējamības* līmenis šādās sastāvdaļās q , tad palielinās *neoperējamības* līmenis infrastruktūrā A kopumā:

$$\Delta x_A(t) = \phi(x_A^0, x_q^0, \Delta x_q^0) \quad \text{kur } t \in [t_0, t_0+T]. \quad (1.4)$$

Šeit q var piederēt gan infrastruktūrai A , gan citai infrastruktūrai B . Var secināt, ka *atkarības indekss* raksturo atkarības pakāpi infrastruktūrā A attiecībā uz visiem n komponentiem infrastruktūrā B . Tātad *atkarības indekss* tiks definēts šādi:

$$\begin{aligned} \left\langle \delta_{A,B(q)}^T \right\rangle_W &= \frac{1}{n} \sum_{i=1}^n w_i \left[\int_{t_0}^{t_0+T} \Delta x_A(\tau, q_i) d\tau \right] / \left[\int_{t_0}^{t_0+T} \Delta x_B(\tau, q_i) d\tau \right] = \\ &= \frac{1}{n} \sum_{i=1}^n w_i \left[\int_{t_0}^{t_0+T} \phi_A(\tau, x_A^0, x_B^0, \Delta x_{q_i}^0) d\tau \right] / \left[\int_{t_0}^{t_0+T} \phi_B(\tau, x_A^0, x_B^0, \Delta x_{q_i}^0) d\tau \right], \end{aligned} \quad (1.5)$$

kur w_i ir katra komponenta q īpatsvars ar $w_i \in [0,1]$.

Atšķirīga pieeja kritisko infrastruktūru savstarpējai atkarībai ir atspoguļota darbos [16, 78], kur piedāvā indeksu *relatīvais ilgums* $R_{i,j}$, kas mēra lavīnveida efektu, kuru izraisa kļūmes ietekmējošā infrastruktūrā.

$R_{i,j} = T_j / T_i$ ir definēts kā attiecība starp dīkstāves ilgumu T_j infrastruktūrā J un dīkstāves ilgumu T_i infrastruktūrā I , kuras kļūmes kļūst par iemeslu dīkstāvēm J infrastruktūrā.

Darbā [79] ir piedāvāta „formas” metrika $R_{i,j}$, kura kvantitatīvi mēra ietekmi uz infrastruktūru J . Šeit $R_{i,j}$ ir aprakstīta kā funkcija $f(\cdot)$, kurai par argumentiem kalpo laiks t un konkrētu nozaru metriku kopa M_j , kuru izmanto, lai noteiktu infrastruktūras J efektivitātes līmeni vai darba spējas:

$$R_{i,j} = f(t, m_j^1, m_j^2, \dots, m_j^p), \text{ kur } m_j^k \in M_j \quad (1.6)$$

Atbilstoši [16], ja $R_{i,j} < 1$, infrastruktūra J ir spējīga reaģēt uz izraisītajām kļūmēm (piemēram, izolēt bojājumu vietas, pārstrukturēt savus pakalpojumus). Pretējā gadījumā, ja $R_{i,j} > 1$, tad infrastruktūra J ir lielā mērā atkarīga no kļūmēm infrastruktūrā I , un tai ir nepieciešams zināms laiks, lai atjaunotu tās pakalpojumus pēc tam, kad beidzas dīkstāves I infrastruktūrā.

Literatūrā var atrast atšķirīgas pieejas, kā izpētīt savstarpējo infrastruktūru atkarību. Piemēram, [22] aprakstītā pieeja balstās uz modeļu detalizācijas pakāpi, un tā nosaka trīs galvenās kategorijas. Pirmā kategorija pārstāv vienkāršus modeļus, kas spēj nodrošināt kvalitatīvu informāciju par parādībām, kuru nosauc kā holistisku. Otrajā kategorijā ietilpst detalizētāki un jutīgāki modeļi, kuru mērķis ir analizēt infrastruktūru topoloģiskās īpašības (topoloģiska pieeja un topoloģiskais modelis), bet trešajai kategorijai ir attiecināmi imitācijas rīki, kuru darbība ir spējīga reproducēt infrastruktūras sastāvdaļu uzvedību un kuriem ir detalizēta, uz operatīvo darbību orientēta pieeja (imitācijas pieeja un imitācijas modelis).

Savukārt [13], pētot infrastruktūru atkarību, par prioritāti izvirza datu pieejamību un granularitāti un piedāvā holistisku, topoloģisku, analītisku un imitācijas pieeju un tām atbilstošus modeļus. Vairāki pētnieki [17, 22] piedāvā arī jauktu holistisku – redukcionistisku pieeju, kas izmanto infrastruktūru pakalpojumu dekompozīcijas modeli.

Nenoliedzot citu pieeju pamatotību, par pamatu tiek izvēlēts [13] deklarētais princips, kas balstās uz *datu pieejamību un granularitāti* un kas ļauj turpmāk izskatīt vairākus

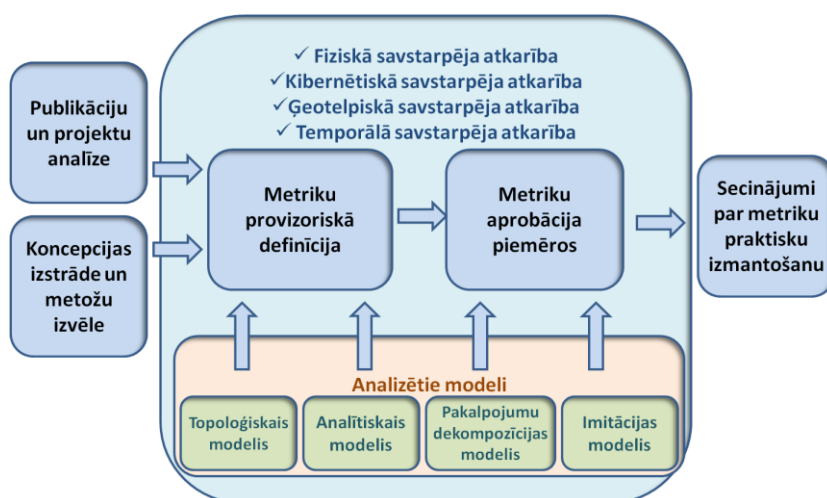
infrastruktūru mijiedarbības modeļus. Savukārt šī pētījuma autors papildina darbos [16, 14, 13] piedāvātas pieejas vēl ar “Holisistisko – redukcionistisko” pieeju, kas paredz lielu kritisko infrastruktūru sistēmu dekompozīciju uz mazākām sastāvdaļām un holistisko pakalpojumu sadali uz apakšpakalpojumiem [82]. *Holisistiskā – redukcionistiskā* pieeja atbilst *datu pieejamības un granularitātes* principam un papildus dod iespēju izpētīt kritisko infrastruktūru mijiedarbību, izmantojot pakalpojumu dekompozīcijas modeli.

Ņemot vērā minēto, šajā darbā tiek izskatītas šādas pieejas:

1. Topoloģiskā pieeja.
2. Holistiskā pieeja. Pētījumā netiek izskatīti uz holistisko pieeju balstīti modeļi, jo, kā atzīmēts vairākos pētījumos, tiem trūkst praktiskā pielietojuma.
3. Holisistiskā - redukcionistiskā pieeja.
4. Analītiskā pieeja.
5. Imitācijas pieeja.

Lai sasniegtu pētījuma mērķus, promocijās darbā ir izmantota šāda metode (skat. 1.1.att.): vispirms tiek veikta publikāciju un projektu analīze, tiek precizētas „kritiskās infrastruktūras”, „savstarpēja atkarība” un citu jēdzienu definīcijas, pēc tam tiek precizēti pētījuma rāmji un ierobežojumi, proti, tiek pētītas šādas KI atkarības: fiziskā, kibernetiskā, ģeotelpiskā un temporālā. Nosauktās KI atkarības ir analizētas, izmantojot četrus modeļus: topoloģisko, analītisko, pakalpojumu dekompozīcijas un imitācijas modeli, turklāt katram modelim autors piedāvā atbilstošas provizoriskās metrikas KI ietekmes un atkarības kvalitatīvajam un kvantitatīvajam novērtējumam.

Nākamajā solī tiek veikta metriku aprobācija, izpētot konkrētu piemēru, proti, triju infrastruktūru (elektroapgādes, telekomunikācijas un ūdensvada tīkls) savstarpējo ietekmi, pielietojot imitācijas modeli. Nobeigumā tiek veikta imitācijas rezultātu analīze un tiek izdarīti secinājumi par izmantotajām metrikām un par iespēju veikt infrastruktūru parametru optimizāciju, lai samazinātu savstarpējās ietekmes negatīvo efektu, tas ir, neoperējamības fenomenu.



1.1. Uz topoloģiju balstīta pieeja

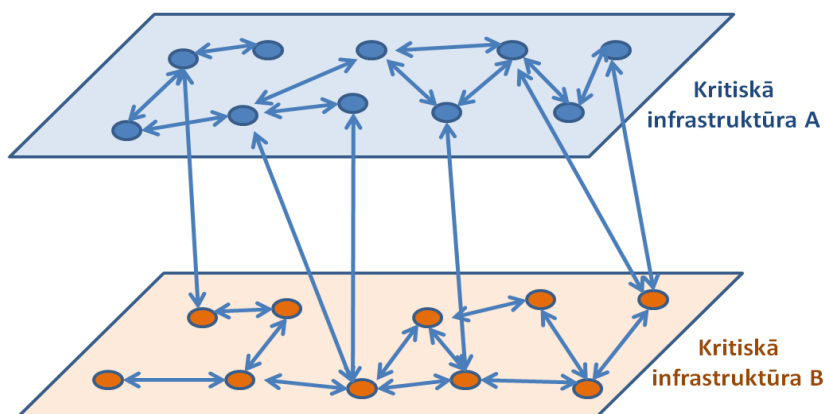
Šī pieeja ir uzskatīta par diezgan universālu, jo tā pēta, kā notikums grafā, kas attēlo konkrētu tīklu, ietekmē parametrus un īpašības saistītā tīklā.

Uz topoloģiju balstītajā pieejā (turpmāk tekstā - „topoloģiskā pieeja”) savstarpējās atkarības pakāpi parasti mēra, izmantojot grafam raksturīgās īpašības, piemēram: sakabes stiprumu, minimālo ceļa garumu starp mezgliem, vektora virzienu u.t.t., tādējādi novērtējot atkarības starp infrastruktūrām.

Pie šādas pieejas fiziskās saiknes galvenokārt tiek uzskatītas, pieņemot, ka savstarpējas atkarības galvenais avots ir ģeogrāfiskais tuvums. Ģeogrāfiskā tuvuma jēdziens (kas uzsver saikni starp diviem mezgliem teritoriālā tuvumā) kopumā ietver fiziskās un ģeotelpiskās atkarības, kā tas ir definēts darbā [63].

Tomēr pastāv būtiska atšķirība starp iepriekš minētajām kategorijām, jo parasti jēdzienu „fiziskā atkarība” izmanto, veicot ex-ante analīzi, savukārt jēdzienu „ģeotelpiskā atkarība” pielieto, veicot „ex-post” analīzi (bieži vien tas ir saistīts ar dabas katastrofu izpēti).

Pamatdoma šādai pieejai ir parādīta 1.2. attēlā, kurā tiek attēlots, kā perturbācijas, notikušas vienā grafā, kas pārstāv pirmo tīklu, spēj ietekmēt cita grafa īpašības, kas pārstāv otro infrastruktūru.



Att. 1.2. Topoloģiskā pieeja izmanto uz grafu tīkliem orientēto modelēšanu

Lai piemērotu šādu pieeju, vispirms būtu jāizvērtē turpmāk minētais:

- Pirmās infrastruktūras topoloģisko (kā arī, iespējams, dinamisko) modeli: tīkla mezgli un saites (dinamiskajam modelim – to, kādu plūsmas modeli ir jāpieņem).
- Šādā veidā būtu jāizvērtē arī otrā infrastruktūra.

- Sakabes mehānismu, kas darbojas starp abu tīklu mezgliem, tas ir, kuri no mezgliem pirmajā infrastruktūrā ir saistīti ar otras infrastruktūras mezgliem un otrādi.

Topoloģiskā pieeja paredz savstarpējas ietekmes „strukturālo” un „funkcionālo” analīzi. Pirmā ir domāta, lai analizētu, kā divu tīklu topoloģiskās īpašības ietekmē viena otru. Pastāv uzskats, ka strukturālo analīzi piemērot ir vienkāršāk, jo tā izskata tikai topoloģiskās īpašības un analizē, kā savstarpējās atkarības klātbūtne degradē šos parametrus. Tomēr daži autori uzsver, ka, izmantojot tikai strukturālo īpašību analīzi, ne vienmēr tiek nodrošināta izsmeļoša un vispusīga informācija.

Lai pārvarētu šos ierobežojumus, dažādi autori pievērta uzmanību arī tīklu funkcionālām īpašībām. Ir pieņemts, ka ir jāpēta plūsmas, kas "plūst" tīklos, piemēram, kā topoloģiskais notikums tīklā (piemēram, mezglu vai saites izņemšana) ietekmē tīklos pastāvošās plūsmas. Par piemēru var kalpot darbs [39], kurā tiek analizēta sistēma, kas sastāv no vairākiem *homogēniem* tīkliem, kuri, savstarpēji mijiedarbojoties, apmainās ar noslodzi, savukārt [55] ir pētīti savstarpēji atkarīgie *heterogēnie* tīkli (kurus veido dažāda rakstura infrastruktūras). Darbā ir pierādīts, ka sakabes starp tīkliem padara sistēmu vairāk uzņēmīgu pret kļūmēm.

1.2. Holistiskā pieeja

Atšķirībā no topoloģiskās pieejas holistiskā pieeja neparedz infrastruktūru sadalīšanu uz savām sastāvdaļām, lai analizētu to mijiedarbību. Ar šo pieeju katru infrastruktūru analizē kā vienotu veselumu un mēģina uzsvērt, cik vienas infrastruktūras darbība kā vesels objekts var ietekmēt citas infrastruktūras stāvokli.

Šī pieeja ir vairāk abstrakta, vienkāršota un atšķirībā no iepriekšējās pieejas drīzāk der kvalitatīvam ne kvantitatīvam novērtējumam. Turklāt, lai gan topoloģiskā pieeja parasti attiecas uz divu infrastruktūru mijiedarbības izpēti, šī pieeja sākotnēji bija izstrādāta, lai apsvērtu vienlaicīgi vairāku infrastruktūru mijiedarbību. Holistiskā pieeja, domājams, vairāk spēj analizēt mijiedarbības attiecībā uz pakalpojumu apmaiņu starp infrastruktūrām, nevis uz topoloģiskām īpašībām, kas ir efektīvāk, ja ir analizēta fiziskā savstarpējā atkarība. Iespējams, tāpēc šī pieeja vairāk noderīga stratēģiskajai analīzei, nevis operatīvai plānošanai.

Viens no pirmajiem darbiem par šo tēmu pieder Haimam [32], kas attīstīja IIM (Iejas-Izejas Neoperējamības Modeli) kā Nobela prēmijas laureāta Ļeontjeva teorijas nākamo soli. Savā darbā viņš ieviesa "neoperējamības" jēdzienu, ar ko apzīmēja infrastruktūras elementu

nepēju veikt tai noteikto funkciju. IIM parāda, kā var novērtēt kopējo efektu, ko izraisa infrastruktūras operējamības degradācija, ņemot vērā savstarpējas atkarības klātbūtni.

Lai kvantitatīvi novērtētu visu infrastruktūru kopējo lomu, autori [70] ievieša *atkarības indeksu*, kuru definēja kā Ļeontjeva koeficientu summu:

$$\delta_i = \frac{1}{n-1} \sum_{k=0}^n a_{ij} \quad (1.7)$$

Šeit δ_i ietekmes kopsumma – tas ir Ļeontjeva koeficientu kolonnas summa. A ir ietekmes matrica, citiem vārdiem, Ļeontjeva koeficientu matrica. Elementi a_{ij} šajā matricā attēlo neoperējamības daļu, kuru j -infrastruktūru ievieš i -infrastruktūrā.

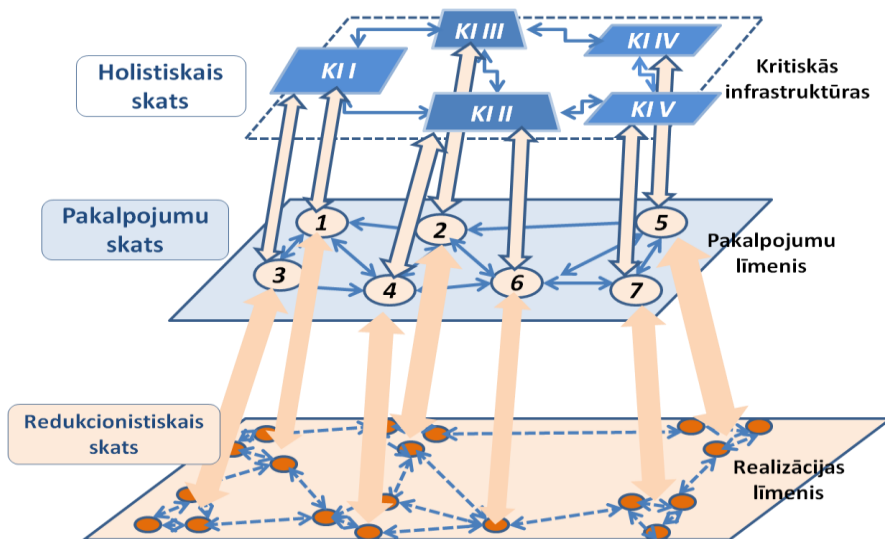
Atšķirīga pieeja tiek ierosināta [78], kas pieņem, ka par savstarpējās atkarības rādītāju tiek izmantota attiecība starp reižu skaitu, cik viena infrastruktūra rada kļūmes citā infrastruktūrā un to, cik reižu otrā infrastruktūra rada kļūmes pirmajā infrastruktūrā.

1.3. Jauktā holistiskā – redukcionistiskā pieeja

Lai pārvarētu iepriekšējo pieeju ierobežojumus, tika ieviesta „Jauktā holistiskā – redukcionistiskā pieeja (JHR) [23]. JHR pieeja ļauj attēlot infrastruktūru raksturlielumus un dinamiku, saglabājot modeļa sarežģītību pārvaldāmā līmenī.

Viens no veidiem, kā to realizēt lielā mērogā, ir uz intelektuāliem aģentiem balstīta modelēšana. Tādejādi ir modelētas augsta līmeņa attiecības un savstarpējās atkarības, ievērojot holistisku paradigmu, toties savstarpējā atkarība starp sastāvdaļām ir modelēta, izmantojot redukcionistiskas metodes. Šādi infrastruktūra ir modelēta vienlaikus kā monolīta vienība un kā savstarpēji saistītas sastāvdaļas kopums.

Turklāt, lai nodrošinātu mijiedarbību starp holistisku un redukcionistisku sistēmas prezentāciju, ir ieviests starpposms – Pakalpojumu līmenis (slānis). Pakalpojumu slāņa elementi atspoguļo materiālas vai nemateriālas (loģiskas, organizatoriskas u.c.) vienības, kas nodrošina kopējo resursu vai pakalpojumu. Šādas starpposma vienības tiek sauktas par *pakalpojumu sniedzējiem* (PS), jo tās pilda attiecīgas funkcijas vai sniedz pakalpojumus. 1.3. attēls demonstrē JHR pieeju, kas izmanto trīs infrastruktūru prezentācijas līmeņus.



1.3.att. Trīs modelēšanas līmeņi [22]

Domājot par informācijas apmaiņu starp kritisko infrastruktūru turētājiem un ņemot vērā starpnozaru raksturu, atkarības pakalpojumu līmenī ir noteicošas. Iesaistītās puses ir ieinteresētas izmantot pakalpojumus ar netraucētu pieejamību. Infrastruktūru turētāji nav ieinteresēti saņemt tehnisko informāciju par iespējamām kļūmēm, bet daudz vairāk ieinteresēti zināt par to ietekmi [4]. Situācija kļūst sarežģītāka, kad redukcionistiskais komponents, kas pieder vienai infrastruktūrai, var nodrošināt arī citas (piemēram, datoru tīklā rūteris nosūta informāciju, kas ir nepieciešama vairākiem saistītiem pakalpojumiem). Turklāt pakalpojums var būt transversāls un ne vienmēr ierobežots tikai uz vienu infrastruktūru, jo pakalpojumu sniedzējs var sniegt pakalpojumus vairākām infrastruktūrām.

1.4. Analītiskā pieeja

Līdz šim **analītiskā pieeja** kritisko infrastruktūru mijiedarbību aprakstīšanai tiek izmantota visai reti. Viens no pirmajiem praktiskajiem pielietojumiem ir saistīts ar „Methodologies for Interdependency Assessment” (MIA) projektu, kuru realizēja 2010. gadā [30]. Šajā projektā analītiskā pieeja tika izmantota savstarpējo atkarību novērtēšanai pakalpojumu līmenī. Ierosinātā metode ir balstīta uz dinamisko sistēmu teorijas principiem, lai nodrošinātu kritisko infrastruktūru savstarpējo atkarību kvantitatīvo analīzi. **Analītiskā pieeja** pielieto labi definētu matemātisku teoriju, kas dod iespēju modelēt dažādas problēmas.

Ņemot vērā, ka savstarpējās atkarības problēma lielā mērā ir atkarīga no starpsavienojumu tipiem un informācijas apmaiņu starp kritiskajām infrastruktūrām, analītiska pieeja izmanto dinamisko sistēmu teorijas galveno konceptu, proti, pārveduma funkcijas un korespondējošās frekvences reakcijas, kā pieeja, lai novērtētu savstarpējo mijiedarbību starp

kritiskajām infrastruktūrām. Šāda pieeja tika izmantota projektā MIA, kur tika definētas IKT un elektroapgādes tīklu sastāvdaļu pārveduma funkcijas. Analītiskās pieejas pielietošana ir plaši aprakstīta projektā MIA, kur analītiskais modelis bija izveidots kādam mākslīgi radītam, tomēr tuvam realitātei, gadījumam [12].

1.5. Imitācijas pieeja

Līdz šīm ir izstrādātas dažādas simulācijas pieejas, lai analizētu individuālo infrastruktūru praktiskos aspektus, piemēram, jaudas plūsmas un stabilitātes programmas elektroapgādes tīklos, hidrauliskas analīzes cauruļvadu sistēmās, satiksmes vadības modeļus transporta tīklos.

Pēdējos gados sāk parādīties simulācijas sistēmas, kas ļauj demonstrēt vairāku infrastruktūru mijiedarbību [24]. Noderīgs pārskats par simulācijas rīkiem ir veikts DIESIS projektā [26].

Viena no daudzsološākajām pieejām, lai analizētu savstarpējās atkarības kompleksajos tīklos, ir uz programmu aģentiem balstīta modelēšana [11]. Šādu modeļu pamatideja balstās uz tā, ka sarežģītas sistēmas uzvedība veidojas kā rezultāts no mijiedarbības starp autonomajiem un elementāriem indivīdiem, kas darbojas uz vienkāršu noteikumu pamata. Viens no pirmajiem darbiem Latvijā, kurš tika veltīts programmu aģentu mijiedarbības modeļu izpētei ar elektroenerģijas patērētāju prioritāšu un pasūtījumu datu bāzēm, ar energosistēmām un elektroenerģijas ražotāju izejvielu piegādātāju datu bāzēm, bija [42].

Ņemot vērā problēmas sarežģītību un sakarā ar matemātiskiem un metodiskiem ierobežojumiem, tiek uzskatīts, ka tikai simulācijas pieeja spēj sniegt detalizētus datus, kas ļauj īstenot operatīvus uzdevumus. Tomēr simulācijas sistēmas uzstādīšana un palaišana ir sarežģīts uzdevums komplikētības un datu iegūšanas dēļ.

Lai iedarbinātu simulācijas scenāriju, pētnieki parasti rekomendē trīs galvenos soļus:

- Izveidot iesaistītās infrastruktūras iekšējo modeli katram tās atsevišķam komponentam.
- Izveidot iekšējās mijiedarbības modeļus, kuri imitē, kā atsevišķa sastāvdaļa ar mijiedarbību katrā infrastruktūrā.
- Izveidot kopējo mijiedarbības modeli, kurā atsevišķas sastāvdaļas, kas pieder dažādām infrastruktūrām, mijiedarbojas savā starpā.

Tomēr jāievēro, ka pat tad, ja šāda pieeja teorētiski spēj reproducēt scenāriju ar augstu precizitāti, tā cieš no nepieciešamības savākt lielu daudzumu datu, turklāt liela daļa no tiem ir uzskatīti par komerciāli jūtīgiem. Tāpēc daudzos gadījumos modeļa izveidošanas un palaišanas process var kļūt par izšķērdīgu un ekonomiski nepamatotu.

1.6. Metriku loma

“Business Dictionary” jēdzienu “metrika” definē kā mērījumu standartu, ar kuru palīdzību var novērtēt plāna, procesa vai produkta efektivitāti, veikspēju, progresu vai kvalitāti [15]. Savukārt “Investopedia” jēdzienu “metrika” raksturo kā kvantitatīvas novērtēšanas parametru, vai mēru, ko izmanto mērīšanai, salīdzinājumam vai veikspējas, vai ražošanas monitoringam [36].

Šā pētījuma izpratnē savstarpējās atkarības metrikas ir mērījumu standarti, ar kuriem tiek novērtēta mijiedarbības pakāpe starp kritiskajām infrastruktūrām, tāpēc, attīstot un pielietojot metrikas, jāņem vērā šādi nosacījumi:

- Metrika pārstāv kvantitatīvu informāciju (piemēram, procenti, skaitli);
- Datus atbalstošiem rādītājiem jābūt reāli iegūstamiem;
- Mērīšanā jāizmanto tikai atkārtojamie procesi;
- Metrika ir noderīga, lai izsekotu sniegumu un vadītu resursus.

Šā pētījuma mērķis ir kvantitatīvi novērtēt elektroapgādes, telekomunikācijas un ūdens piegādes infrastruktūru mijiedarbības pakāpi, tāpēc ir jāpielieto metrikas (vai metriku kopu), kas mēra atkarības pakāpi starp šīm sistēmām vai tās komponentiem.

1.7. Secinājumi par pirmo nodaļu

Zinātniskas literatūras analīze ļāva noteikt visatbilstošākās metodes izvēli, lai pētītu triju izvēlēto kritisko infrastruktūru definētas atkarības. Tiek pētīta fiziskā, kibernetiskā, ģeotelpiskā un temporālā atkarība, kad par prioritāti tiek izvirzīta datu pieejamība un granularitāte. Pētījumā piedāvātā metode pielieto holistisku, topoloģisku, holisistisku – redukcionistisku, analītisku un imitācijas pieeju. Nosauktās KI atkarības turpmākajās pētījuma nodaļās tiek analizētas, izmantojot četrus modeļus: topoloģisko, analītisko, pakalpojumu dekompozīcijas un imitācijas modeli, turklāt katram modelim tiek piedāvātas atbilstošas metrikas KI mijiedarbības kvalitatīvajam un kvantitatīvajam novērtējumam.

2. KRITISKO INFRASTRUKTŪRU MIJIEDARBĪBAS MODEĻU ANALĪZE

Šīs nodaļas uzdevums ir izpētīt modeļus, lai noteiktu kritisko infrastruktūru savstarpējas mijiedarbības, ņemot vērā iepriekš definētas atkarības (fiziskā, topoloģiskā, ģeotelpiskā un temporālā) un apskatītās metodes un pieejas (skat. 3.att). Ar šo mērķi tiek veikts kritisko infrastruktūru modelēšanai un imitācijai veltīto pētījumu pārskats. Nodaļā tiek izvērtētas arī pētījumos un projektos pielietotās metrikas un to saistība ar izvēlēto modeli un atkarības veidu.

2.1. Uz topoloģiskās pieejas balstītais modelis

Uzskatīts, ka kompleksu tīklu topoloģiskā analīze un modelēšana, ir spējīga prezentēt kritisko infrastruktūru mijiedarbības un atkarības mehānismus visaugstākajā abstrakcijas līmenī [12]. Elektroapgādes un telekomunikācijas tīkla mijiedarbības modelēšanas piemērs ir izpētīts un īsi tiek izklāstīts darbos [65, 13]. Virtuālie Privātie Tīkli (VPN), kurus elektroapgādes operatori izmanto, lai savienotu vadības centrus ar elektroapakšstacijām, ietver rezerves savienojumus, kas palielina tīkla robustumu pret iespējamām telekomunikācijas mezglu atteikumiem. Ir konstatēts, ka viena telekomunikācijas mezgla bojāšana neizraisa ne viena elektroapgādes mezgla atslēgšanu no vadības tīkla, tātad ir secināts, ka šāds VPN ir "*N-1* robusts" (vai stabils).

Termins, "*N-1* robusts" nozīmē tīkla spēju izpildīt savas funkcijas, kad viens - no tā *N* komponentiem iziet no ierindas. Telekomunikācijas tīkls zaudē funkcionalitāti, ja notiek vienlaicīgs divu tīkla elementu (tīkla mezglu) atteikums. Tiek ieviesta varbūtība P_2 , kas kalkūlē katra elektroapgādes mezgla funkcionalitātes zaudēšanu, divu telekomunikācijas mezglu vienlaicīga atteikuma rezultātā. P_2 ir definēta kā:

$$P_2(i) = N_i / n(n-1) \quad (2.1)$$

kur N_i ir gadījumu skaits, kad elektroapgādes mezgls nav sasniedzams no vadības centra, ņemot vērā visas iespējamās kombinācijas, kad no ierindas iziet vienlaicīgi divi telekomunikācijas mezgli. Tas nozīmē, ka ir nepieciešams analizēt $n(n-1)$ gadījumus, kur n ir mezglu skaits telekomunikācijas tīklā. Nosauktus parametrus ir iespējams vispārināt, ieviešot:

$$P_k(i) = N_i / (n, k) \quad (2.2)$$

kur (n, k) pārstāv binominālo koeficientu, apzīmējot iespējamo pāru mezglu kļūmju skaitu, kur n ir elementu (mezglu skaits). Padziļinātu sistēmas analīzi veic, nosakot konkrētus mezglu pārus parametrus:

$$P_k^\infty = 1 \text{ or } 0,$$

kad telekomunikāciju mezglu pāris tiek izslēgts („1” ja mezgls nav aizsniedzams, bet „0, ja tā nav). Tas nozīmē, jo lielāka varbūtība P_2 , jo zemāka savstarpējā atkarība starp abiem tīkliem vai to sastāvdaļām.

Jāuzsver, ka iepriekš noteikto $P_2(i)$ rādītāju izmanto, lai rēķinātu i mezgla atkarību visā elektroapgādes sistēmā. Savukārt tā $P_k^a(i)$ indekss aprēķina atkarību α -grupas mezgliem. Lai novērtētu globālo elektroapgādes sistēmas atkarību no telekomunikācijas tīkla, ir jāizmanto iepriekšējais rādītājs kā vidējais rādītājs, kas tiek aprēķināts visiem elektriskajiem mezgliem, un kurš ir definēts kā **tīkla topoloģiskais robustums** = $\langle 1 - P_2 \rangle$.

2.2. Uz analītiskās pieejas balstītais modelis

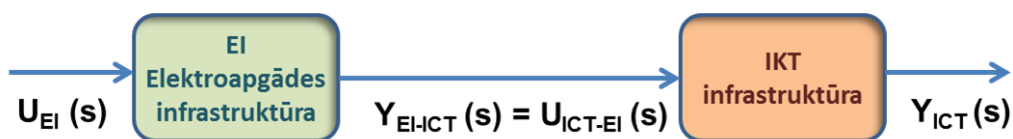
Zinātniskajā literatūrā var atrast uz analītiskās pieejas balstīto modeļu aprakstus, piemēram [12] pētījums definē galvenos principus modelim, kas tika pielietots elektroapgādes (EI) un informācijas un telekomunikācijas (IKT) infrastruktūru savstarpējās mijiedarbības izpētei:

- Identificēt lineāro vai nelineāro modeli EI un IKT apakšsistēmām;
- Noteikt galvenās pārneses funkcijas EI un IKT apakšsistēmām;
- Identificēt parametrus pārneses funkcijām;
- Noteikt svarīgākos ievadus EI, ņemot vērā atkarību no IKT;
- Noteikt svarīgākos ievadus IKT ņemot vērā atkarību no EI.

Shematiski savstarpējās atkarības starp EI un IKT infrastruktūru ir attēlotas 2.1. attēlā.

Ir pieņemts, ka:

- $U_{EI}(s)$ - EI ievada Laplasa transformācijas vektors;
- $Y_{EI-ICT}(s)$ - EI izvada Laplasa transformācijas vektors uz IKT infrastruktūru;
- $U_{ICT}(s)$ - IKT ievada Laplasa transformācijas vektors



2.1.att. Elektroapgādes infrastruktūras ietekme uz IKT infrastruktūru

2.1. attēls nosaka attiecības:

$$\frac{Y_{EI-ICT}(s)}{U_{EI}(s)} = \text{Transformācijas funkcijas matrica no EI uz IKT infrastruktūru} \quad (2.3)$$

$$\frac{Y_{IKT}(s)}{U_{IKT-EI}(s)} = \text{IKT infrastruktūras Transformācijas funkcijas matrica} \quad (2.4)$$

Šajā piemērā Laplasa transformācijas funkcija:

- a) apraksta veidu, kā EI ietekmē IKT;
- b) apraksta veidu, kā EI izvadi ietekmē IKT infrastruktūras izejas.

2.2.1. Analītiskā modeļa piemērs

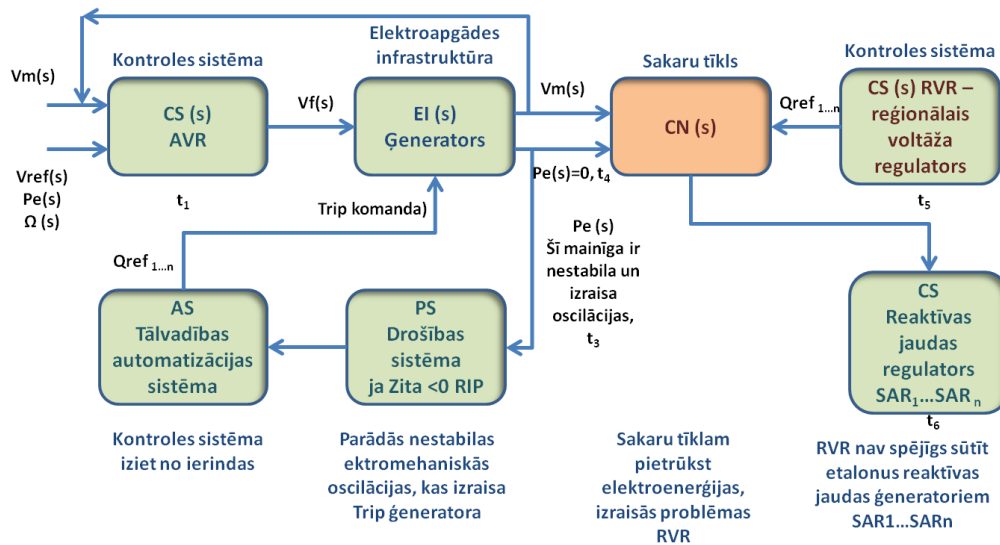
Darba turpinājumā tiek izskatīts piemērs, izmantojot dinamisko sistēmu teorijas pieeju ar mērķi demonstrēt savstarpējo atkarību starp elektroapgādes infrastruktūru un telekomunikācijas infrastruktūru [12]. Minētās infrastruktūras ir prezentētās ar piecām apakšsistēmām, kas mijiedarbojas savā starpā (skat. 2.2. attēlu):

- Elektroapgādes infrastruktūra (EI);
- Kontroles sistēmas (CS);
- Tālvadības automatizācijas sistēma (AS);
- Drošības sistēmas (PS);
- Sakaru tīkls (CN).

Avārijas situācija, kurā iesaistās abu infrastruktūru apakšsistēmas, var veidoties šādos posmos:

- 1) Ja AVR (Automātiskais sprieguma regulators) elektroapgādes sistēmas stabilizatorā (ESS) kāda iemesla dēļ notiks kļūme, tad ESS elektromehāniskās svārstības var savukārt izraisīt kļūmes kontroles sistēmā CS, kas savukārt var novest pie:
 - Oscilācijām un svārstībām EI;
 - EI bīstamām parametru novirzēm;
- 2) Ģeneratora elektromehāniska nestabilitāte var izraisīt drošības sistēmas (PS) iejaukšanos un savukārt:
 - Ģeneratora atslēgšanu.
 - Ģeneratora atslēgšana izraisa enerģijas trūkumu EI.
 - EI darbojas ar pasliktinātiem kvalitātes parametriem.
- 3) Enerģijas trūkums elektrotīklā var izraisīt enerģijas trūkumu sakaru tīkla vadības centrā (CNC). CNC bez adekvātas enerģijas piegādes var zaudēt savu funkcionalitāti. Tā rezultātā sakaru tīkla vadības centrs var zaudēt spēju pārvaldīt sakaru tīklu (CN) pilnā apjomā.
- 4) CNC funkcionalitātes pilns vai daļējais zaudējums var novest pie tā, ka Reģionālie sprieguma regulatori (RVR) pārtrauc sūtīt signālus reaktīvas jaudas regulatoriem, kas atrodas elektrostacijās savā kontrolētajā reģionā (SART1... SART N). Rezultātā vadības sistēma CS vairs nefunkcionē pilnajā apjomā.

Aprakstītu scenāriju ir iespējams realizēt, izmantojot transformācijas funkcijas, kas apraksta mijiedarbības starp dažādu infrastruktūru apakšsistēmām.



2.2.att. Mijiedarbības starp CN un EI, piedaloties PS, AS un CS (autora pārveidota shēma no [12])

Attēlā 2.2 – attēlotā apakšsistēmas mijiedarbība, kas demonstrē aprakstītu avārijas situāciju, kur:

$V_m(s)$ - Laplasa sprieguma transformācijas funkcija no maiņstrāvas ģenerators;

$V_f(s)$ - Laplasa ierosmes sprieguma ģenerators transformācijas funkcija;

$V_{ref}(s)$ - Laplasa etalona sprieguma transformācijas funkcija uz ģeneratoru;

$Q_{ref\ 1-N}$ - reaktīvās jaudas etalona vērtības ar atbilstošas elektrostacijas numuru;

$P_e(s)$ - Ģenerators elektroenerģijas jaudas Laplasa transformācijas funkcija;

$Z_{itai} - „i”$ ģenerators elektromehāniskā slāpēšana;

$\Omega(s)$ - Leņķiska (fāzes) ātruma ģenerators Laplasa transformācijas funkcija;

SART – Reaktīvas jaudas regulators.

Jāuzsver kontroles sistēmas un sakaru tīkla loma, jo sakaru tīkls (CN) sniedz pakalpojumus reģionāliem sprieguma regulatoriem (RVR) kā arī reaktīvās jaudas regulatoriem (SART₁, SART₂, utt.). Turklāt šīs funkcijas ir sadalītas dažādās fiziskās atrašanās vietās plašā teritorijā atkarībā no kontroles sistēmas hierarhiskas struktūras.

No augšminētiem piemēriem var noformulēt šādas metrikas, kas ļauj mērīt kritisko infrastruktūru mijiedarbību:

- Moduļa transformācijas funkcija $|G(j\omega)|$ nodrošina metriku, ar kuru var mērīt saikni starp infrastruktūrām, kuru darbība tiek modelēta, jo modulis ļauj novērtēt, cik lielā mērā ienākošais signāls ir pastiprināts vai novājināts sistēmā, kas tiek veidota ar transformācijas funkciju palīdzību frekvenču diapazonā no 0 līdz bezgalībai. Ja moduļa

$G(j\omega)$ vērtība ir nozīmīga pētītā frekvenču intervālā, tas liecina, ka pastāv savstarpēja atkarība.

- Fāzes transformācijas funkcija $\angle G(j\omega)$ analizē fāzes atšķirības starp ienākošo un izejas signālu dažādos frekvenču intervālos. Tā ir noderīga, lai veiktu secinājumus par to, ka sistēmas sastāvdaļas un apakšsistēmas reaģē uz ieejas signāla izmaiņām. Ja funkcijas $G(j\omega)$ fāze (tas ir $\angle G(j\omega)$) ir ļoti augsta noteiktā frekvenču intervālā, tas norāda uz lielām potenciālām izmaiņām izejas signālā attiecībā uz ienākošo signālu, kas būtu jāanalizē, lai novērtētu savstarpējo atkarību starp modelētām infrastruktūrām.

2.3. Pakalpojumu dekompozīcijas modelis

Šajā sadaļā tiek piedāvāta pieeja, kas ļautu uzraudzīt kritisko infrastruktūru, ņemot vērā pakalpojumu stāvokli, kurus sniedz infrastruktūra, kā arī šo pakalpojumu mijiedarbību. To var panākt, ja abstrahēties no mērījumiem, kas iegūti no konkrētas KI, un izmantotu kopīgus parametrus, ar kuriem var apmainīties starp iesaistītām infrastruktūrām.

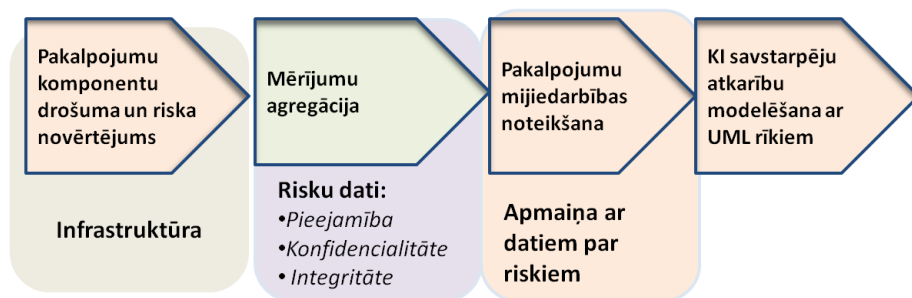
Šajā sadaļā arī tiek demonstrēta Universālās modelēšanas valodas izmantošana (Unified Modeling Language (UML)) ar mērķi izpētīt KI atkarības. Tika demonstrēts piemērs ar triju kritisko infrastruktūru mijiedarbības modelēšanu ar UML rīkiem vienā Latvijas pilsētas teritorijā.

2.3.1. Metodoloģija

Pieredze rāda [17], ka ir iespējams samazināt pakalpojumu sarežģītību caur noteiktu abstraktu parametru kopu, izmantojot uz riska novērtēšanu balstītās metrikas. Tas ļauj salīdzināt kritiskās infrastruktūras, kas kalpo ļoti atšķirīgiem mērķim (enerģētika, telekomunikācijas, ūdensapgādes, transports u.c.) un kuri sastāv no heterogēnām infrastruktūras sastāvdaļām. Tas ļauj kontrolēt svarīgus infrastruktūras parametrus, piemēram, pieejamību, konfidencialitāti un integritāti. Abstrahēšana uz kopīgiem parametriem varēs rosināt pakalpojumu sniedzējus dalīties ar risku datiem ar citiem saistītiem pakalpojumu sniedzējiem.

Šī pētījuma autors papildina metodiku, kas ir aprakstīta [2], [69] un [22], ar ceturto moduli – KI savstarpējo atkarību modelēšanu ar UML rīkiem. Piedāvāta metodika tiek veikta četros etapos (moduļos) (skat. 2.3.attēlu):

- Pakalpojumu komponentu drošuma un riska novērtēšana;
- Mērījumu agregācija;
- Pakalpojumi mijiedarbības noteikšana;
- Kritisko infrastruktūru savstarpēju atkarību modelēšana, izmantojot UML rīkus.



2.3.att. Kritisko infrastruktūru savstarpēju atkarību modelēšana četros etapos

Pakalpojumu komponentu drošuma un riska novērtēšana:

Pirmais solis balstās uz attiecīgās infrastruktūras riska analīzi ar mērķi noteikt pakalpojumus, kurus var uzskatīt par kritiskiem. Šo pirmo soļu laikā jāveic šādas darbības: *kritisko pakalpojumu identifikācija, savstarpējo atkarību identificēšana, galveno mērījumu noteikšana, metriku izveidošana un savstarpējās atkarības koeficientu noteikšana.*

Kritisko pakalpojumu identifikācijas aktivitātes mērķis ir katras infrastruktūras ietvaros noteikt pakalpojumus, ko var uzskatīt par kritiskiem. Pēc tam, kad pakalpojumi ir identificēti, jāidentificē visi resursi, kas veicina pakalpojuma mērķu sasniegšanu.

Lai *identificētu savstarpējas atkarības*, tiek izmantots identificēto kritisko pakalpojumu un to sastāvdaļu (resursu) saraksts. Šīs darbības mērķis ir apzināt visas attiecības (atkarības vai savstarpējas atkarības) starp pakalpojumiem. Šī darbības joma attiecas uz iekšējām atkarībām starp konkrētās infrastruktūras elementiem kā arī uz ārējām atkarībām (starp heterogēnu infrastruktūru pakalpojumiem).

Galveno mērījumu noteikšanas aktivitātes mērķis ir definēt katram pakalpojumam galvenos mērījumus, ņemot vērā pakalpojuma sastāvdaļas (resursus). Šādi mērījumi var būt, piemēram, sensori dati, datoru tīkla drošības sistēmas brīdinājuma signāli u.t.t. Ņemot vērā infrastruktūru komponentu heterogēno dabu, drošuma un riska līmenis tiek piesaistīts katram mērījumam. Lai noteiktu drošības un riska līmeņus, tiek piemērota īpaša skala, kas sastāv no pieciem līmeņiem [35].

Metriku izveidošana. Lai sagatavotu vienotas vērtības katram pakalpojumam, mērījumi, kas ir saistīti ar konkrēto pakalpojumu, tiek apvienoti metrikas formā. Šādas metrikas var sakombinēt kritēriju formā, tādējādi katru pakalpojumu būtu iespējams raksturot tikai ar trim kritērijiem:

- *Konfidencialitāte:* nav neatļautas informācijas izpaušanas attiecībā par datiem, kuru izmanto kritiskā infrastruktūra;
- *Integritāte:* nav neatļautu izmaiņu sistēmā saistībā ar kritisko pakalpojumu sniegšanu;

- *Pieejamība*: gatavība sniegt pakalpojumu ar atbilstošu servisa līmeni.

Katrs mērījums tiek izmantots, lai iegūtu vismaz vienu metriku, tāpēc tiek ieviests ietekmes koeficients (svars) W_{μ_i} , kuru piešķir katram mērījumam attiecībā uz konfidencialitāti, integritāti un pieejamību (C, I, A). Ietekmes koeficienti ļauj ņemt vērā mērījumus atkarībā no tās ietekmes un tiek izmantoti, lai aprēķinātu metriku risku un drošuma līmeni. Piemēram, metrikas drošuma līmeni nosaka, izmantojot šādu formulu (rezultātu noapaļo līdz veselam skaitlim):

$$AL_m = [\sum_{i=1}^n (AL_{\mu_i} * W_{\mu_i})] / [\sum_{i=1}^n (W_{\mu_i})], \quad (2.5)$$

kur m ir metrika, μ ir mērījums, AL_{μ_i} – ir mērījuma μ_i drošuma līmenis, n mērījumu skaits, kurus izmanto, lai sastādītu metriku, un W_{μ_i} ietekmes koeficients (svars) mērījuma μ_i .

Mērījumu agregācija

Šis solis ir veikts ar mērķi kritisko pakalpojumu periodiskos mērījumus pārveidot par riska un drošuma līmeņiem.

Normalizācija: normalizācijas procesā pārveido heterogēnus datus par normalizētiem datiem, kurus var salīdzināt un apstrādāt, izmantojot piecu līmeņu skalu. Līmeņu noteikšana prasa padziļinātas zināšanas konkrētas infrastruktūras pakalpojumu jomā un tādējādi tiek realizēta ar ekspertu vai ekspertu grupas piesaistīšanu. Mērījumi dati tiek normalizēti: etalona vērtība Ev tiek noteikta katram mērījumam. Šī vērtība tiek izmantota, lai aprēķinātu mērījuma novirzi pret etalona vērtību, izmantojot šādu formulu:

$$\Delta = |(\mu - Ev) / Ev * 100|, \quad (2.6)$$

kur μ ir mērījuma vērtība; Ev – etalona vērtība. Paralēli tiek definētas robežvērtības, lai klasificētu vērtības: 1 - nav sasniegts, 2 - vājš, 3 - pieņemams, 4 – pareizs un 5 - sasniegts.

Metriku riska līmeņu agregācija: Nākamā solī normalizētos mērījumus apvieno metrikās. Agregācijas formula balstās uz ietekmes koeficientiem (svariem) un ļauj novērtēt riska līmeni, rēķinot kā veselu skaitli starp mazāko "1", un augstāko riska pakāpi "5". Rezultāts tiek noapaļots līdz tuvākajam veselam skaitlim:

$$RL(m_x) = (RL_M + 1) - [\sum_{i=1}^n (NV(\mu_i) * W_{\mu_i})] / [\sum_{i=1}^n (W_{\mu_i})], \quad (2.7)$$

kur m_x ir metrika, RL_M – maksimālais riska līmenis, n mērījumu skaits, kurus izmanto, lai sastādītu metriku, $NV(\mu)$ – normalizēta vērtība μ , μ - mērījums un W_{μ_i} ietekmes koeficients (svars) mērījuma μ_i .

Kritēriju agregācija: Pēc riska līmeņa noteikšanas metrikas apkopo kritērijos. Metriku agregācijai tiek izmantots īpašs ietekmes svars (W_{mi}), kuru nosaka sniegtā pakalpojuma jomas

speciālisti, balstoties uz metrikas svarīgumu aprēķināmā kritērijā. Katram pakalpojumam kritērija riska līmenis tiek aprēķināts:

$$RL(C) = [\sum_{i=1}^n (RL(m_i) * W_{m_i})] / [\sum_{i=1}^n (W_{m_i})], \quad (2.8)$$

kur C - kritērijs, m - metrika, $RL(m_i)$ metrikas m_i riska līmenis; W_{m_i} – metrikas m_i svara koeficients un n metriku skaits kritērijā. Rezultāts tiek noapaļots līdz tuvākajam veselajam skaitlim.

Pakalpojumu savstarpējās atkarības noteikšana

Izmantojot svērto savstarpējas atkarības funkcionālo modeli, katram kritiskās infrastruktūras dienestam ir iespējams aprēķināt un iesniegt saistītas infrastruktūras pakalpojumu sniedzējam normalizētus drošuma un riska līmeņa aprēķinātus kritērijus. Pakalpojumu sniedzējs, kas saņem drošuma un riska līmeņa aprēķinātus kritērijus, var tos izmantot, lai aprēķinātu sava pakalpojuma riskus, ņemot vērā atkarības starp infrastruktūrām. Vairāku infrastruktūru un tās pakalpojumu mijiedarbības situācijā analīze kļūs ievērojami sarežģītāka.

2.3.2. Savstarpēju mijiedarbību modelēšana, izmantojot UML

Pieaugošo modelēšanas lomu programmatūras attīstībā veicina metodoloģija, kuru galvenokārt pārstāv „Object Management Group” (OMG) risinājumi. Šie risinājumi, kurus apzīmē kā Model Driven Architecture (MDA) [53], tiek izmantoti IKT sistēmu abstrahēšanai, modelēšanai, izstrādei un atkārtotai izmantošanai. Galvenais sistēmu modelēšanas komponents, kas balstās uz MDA principiem, ir „Unified Modeling Language™ (UML)” (Universāla modelēšanas valoda), un tas ir plaši pieņemts standarts modelēšanai un dažāda veida sistēmu projektēšanai. Tas ļauj veidot vairāku veidu diagrammas, tās elementus un pierakstus [54]. Neskatoties uz to, ka MDA modeļus var izveidot ar jebkāda veida modelēšanas valodu, UML pieder dominējošā loma.

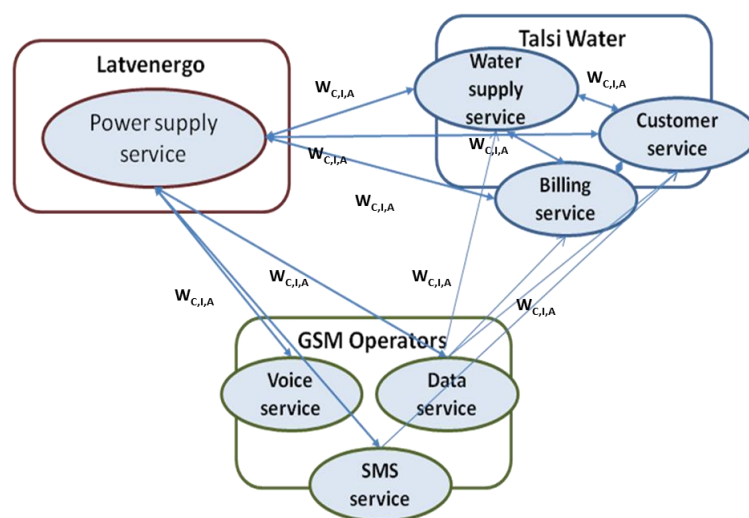
Galvenais MDA mērķis ir nodrošināt automatizētas transformācijas iespēju no platformas neatkarīga modeļa uz platformas specifisku izejas kodu. MDA modeļi ir pārstāvēti divās atšķirīgajās formās. Pirmo formu pārstāv modeļi, kas ir neatkarīgi no darba platformas. Šie modeļi tiek saukti *Platformas neatkarīgie modeļi* (PIM, „Platform Independent Models”). PIM ir abstraktie modeļi, kas nav izstrādāti kādai konkrētai attīstības videi. Lai realizētu PIM vidē izstrādātu modeli, jāizmanto *Platformas specifiskie modeļi* (PSM - „Platform Specific Models”). Lai PIM pārveidotu par PSM, var izmantot, piemēram, Jade [8], Repast [50] vai kādu citu imitācijas rīku.

2.3.3. Elektroapgādes, telekomunikācijas un ūdens apgādes infrastruktūras mijiedarbības modelēšanas piemērs Talsu teritorijā

Lai pārbaudītu aprakstītas metodoloģijas pielietojamību, šajā sadaļā ir realizēts triju infrastruktūru mijiedarbības scenārijs. Lai izveidotu konceptuālo sistēmas modeli, tiek izmantotas UML lietošanas gadījumu diagrammas, objektu mijiedarbības izpratnei tiek izmantotas UML secības diagrammas un modeļa detalizētākai izpētei ir izstrādātas UML klašu diagrammas.

Augšminētais scenārijs iekļauj pilsētas ūdens sadales tīklu (Talsi Ūdens), kas demonstrē savu pakalpojumu atkarību no elektroenerģijas piegādātāja pakalpojumiem (Latvenergo) un telekomunikāciju pakalpojumu sniedzēja (GSM operators). Šī scenārija uzdevums ir nodemonstrēt kā piemēru uz riska balstītu metodiku. Sarežģītāku un pilnīgi reālu scenāriju ir problemātiski izveidot sakarā ar datu trūkumu un šī pētījuma ierobežojumu dēļ. Plašāka informācija ir atrodama šī pētījuma autora publikācijās [83, 84, 85].

Talsu Ūdens kritiskās infrastruktūras riska analīzes posmā tiek definēti kritiskie pakalpojumi un to savstarpējā atkarība (skat. 2.4. attēlu). Savukārt, 2.5.att. parāda, no kādiem komponentiem, kas ir nepieciešami, lai sniegtu pakalpojumu, sastāv katrs Talsu Ūdens pakalpojums.

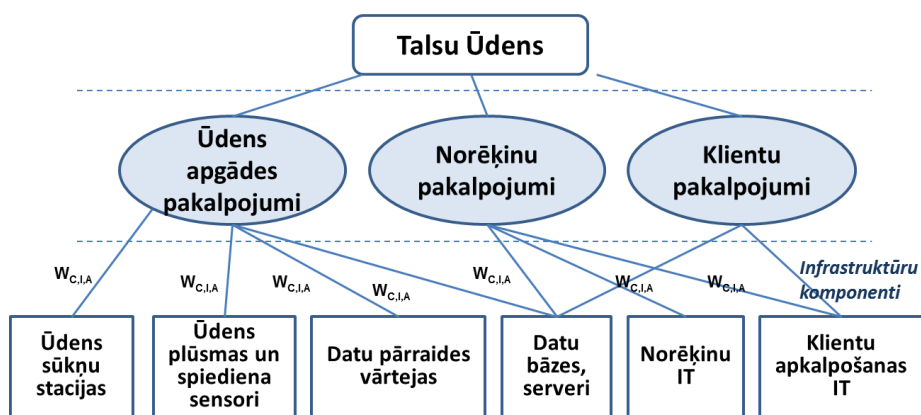


2.4.att. Mijiedarbības starp pakalpojumiem un pakalpojumu sniedzējiem (Zabašta u.c. [83])

2.4 attēlā var redzēt, Talsi Ūdens KI sniedz ūdensapgādes, norēķinu un klientu apkalpošanas pakalpojumus. Ūdensapgādes pakalpojumiem tiek izmantotas infrastruktūras sastāvdaļas, piemēram, ūdens apgādes pakalpojums ir balstīts uz ūdens sūkņēšanas iekārtām, uz SCADA, kas nodrošina ūdensvada tīkla kontroli un pārvaldību, ūdens plūsmas mērītājiem, sensoriem - raidītājiem, datu pārraides vārtējām un datu centra iekārtām (serveriem, datu bāzēm,

programmatūru u.c.) [85]. Savukārt datu pārraides vārtejas balstās uz GSM - GPRS pakalpojumu sniedzējiem. Daļa no infrastruktūras komponentiem tiek dalīta starp pakalpojumiem, piemēram, datu bāzes un serverus izmanto, lai sniegtu ūdens piegādes, norēķinus un klientu apkalpošanas pakalpojumus.

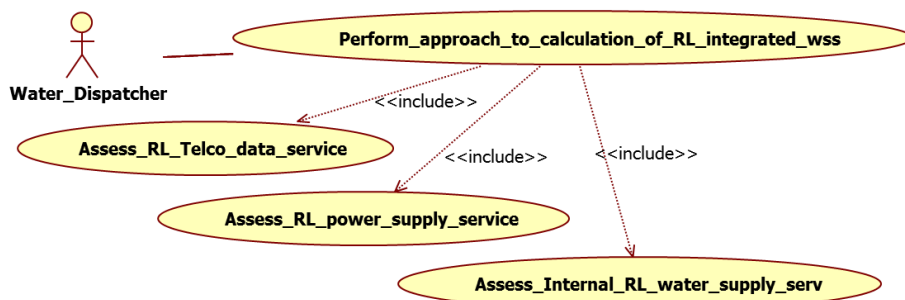
Tiek konstatēts, ka GSM – GPRS operatora galvenā infrastruktūra pārskatītajā teritorijā sastāv no bāzes stacijas, kas nodrošina datu pārraides un SMS pakalpojumus ūdens piegādātājam. Tiek pieņemts, ka datu pārraides (GPRS) un SMS pakalpojumus nav iespējams sniegt bez elektroapgādes pakalpojumiem, ņemot vērā, ka GSM bāzes stacijas rezerves barošanas avoti un vārteju akumulatori nodrošina rezerves barošanu uz laiku pēc noteiktās normas uz divām stundām.



2.5.att. Talsi Ūdens pakalpojumu dekompozīcija [83]

Lai izveidotu triju infrastruktūru mijiedarbības UML modeli, tiek izmantots StarUML, atvērtā koda UML rīks, kurš ir licencēts atbilstoši „General Public License (GPL)” noteikumiem.

Lietošanas gadījumi. 2.6.attēlā var redzēt UML *lietošanas gadījumu diagrammas*, kuras ļauj noteikt apvienota ūdens piegādes pakalpojuma riska līmeņi, kurš saintegrē kopā iekšējo risku, kā arī ietekmi no telekomunikācijas operatora datu pakalpojumiem un no elektroapgādes Latvenergo pakalpojumiem.

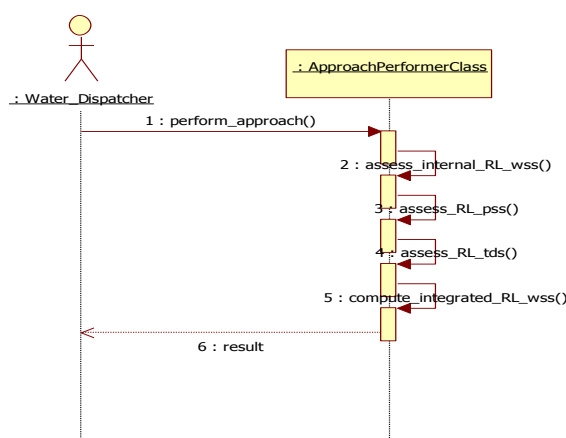


2.6.att. lietošanas gadījumu diagrammas riska līmeņa noteikšanai [84]

Aģenta simbols 2.6. attēlā pārstāv personu vai dienestu, kas aktivizē lietošanas gadījumu, kas mūsu piemērā ir ūdens apgādes dienesta dispečers, kuram jāizvērtē ūdens apgādes pakalpojuma integrētais riska līmenis.

Secību diagrammas. Detalizēta infrastruktūru mijiedarbība tiek modelēta, izmantojot secības diagrammas. Viena no secības diagrammām (skat. 2.7. attēlu) integrē riska pakāpi ūdens apgādes pakalpojumam.

„Approach_Performer_Class” (skat. 2.7. attēlu), kurš ir atbildīgs par integrēta riska līmeņa noteikšanu, saņem pieteikumu no ūdens dienesta dispečera. Nākamajā solī tiek aprēķināts ūdens apgādes pakalpojuma iekšējais riska līmenis. 3. un 4. solī izvērtē ārējo pakalpojumu (elektroapgādes un datu pārraides pakalpojumi) ietekmi uz ūdens apgādes pakalpojumu. Ar 5. soli tiek aprēķināts ūdensapgādes pakalpojuma integrētais riska līmenis, turklāt 6. solī aprēķinātais rezultāts tiek piegādāts ūdens dienesta dispečeram.

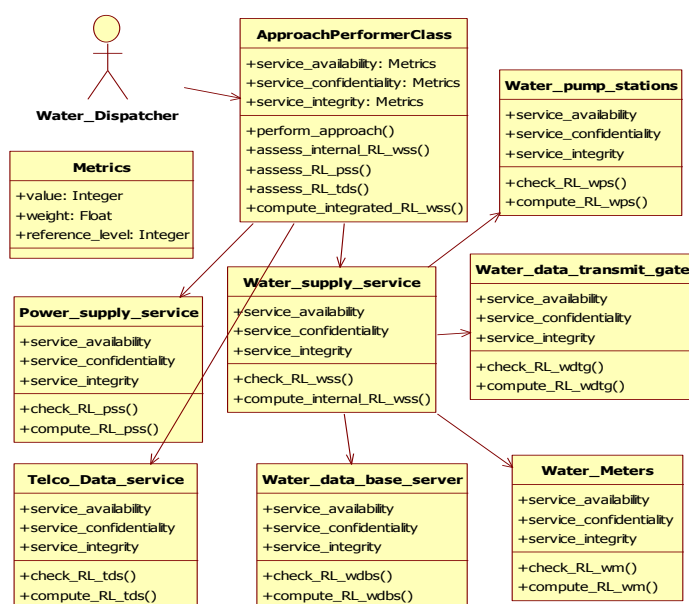


2.7. att. Ūdensapgādes pakalpojuma integrētā riska līmeņa novērtēšana [84]

Secību diagrammas līdzīgā veidā apraksta dalībniekus un mijiedarbību citos lietošanas gadījumos, bet sakarā ar šā darba apjoma ierobežojumiem tie tālāk netiek aprakstīti.

Klašu diagramma. 2.8. attēlā var redzēt deviņas klases, kur četras klases pārstāv ūdensapgādes pakalpojumu un tās sastāvdaļas, divas klases pārstāv elektroapgādes un datu pārraides pakalpojumus, un vienā klasē ierosina un kontrolē pakalpojuma riska līmeņa novērtēšanas procesu. Katras klases īpašības un darbības parametri netiek norādīti shēmās, lai saglabātu attēlu salasāmību. Viena konkrēta klase - "Metrics"- tiek izveidota, lai aprakstītu klašu atribūtu parametrus un klašu darbības parametrus. Klasēm ir piešķirti atribūti "vērtība", "svars" un "atsauces līmenis", kas ir saistīti ar pakalpojumu parametriem (pieejamība, konfidencialitāte un integritāte). Īpaša klases izveidošana ir nepieciešama tāpēc, ka vienotie standartizētie parametri tiek piemēroti atšķirīgajām kritiskajām infrastruktūrām.

Lai gan 2.8. attēlā piedāvāta ontoloģija tika izveidota, lai izpētītu kritisko infrastruktūru mijiedarbību vienā konkrētā pilsētā, to ir iespējams pielāgot un papildināt ar citām klasēm, ņemot vērā konkrētas pilsētas specifiku.



2.8. att. Infrastruktūru mijiedarbības klašu diagramma

Secinājumi

Šajā sadaļā tiek izmantotas metrikas, kuras ļauj novērtēt savstarpēji sasaistīto kritisko infrastruktūru pakalpojumu konfidencialitāti, integritāti un pieejamību.

Šīs nodaļas autora ieguldījums kritisko infrastruktūru mijiedarbības pētījumā ir tas, ka reālā scenārijā, kas iekļauj triju infrastruktūru mijiedarbību nelielā Latvijas pilsētas teritorijā, ar UML rīkiem tiek izveidots PIM modelis un tiek aprobētas uz riska novērtēšanas balstītās metrikas. Augšminētais scenārijs iekļauj pilsētas ūdens sadales tīklu (Talsi Ūdens), kas demonstrē savu pakalpojumu atkarību no elektroenerģijas piegādātāja pakalpojumiem (Latvenergo) un telekomunikāciju pakalpojumu sniedzēja (GSM operatoru).

2.4. Uz imitācijas pieejas balstītie modeli

Uz imitācijas pieejas balstītie modeli ir vērsti galvenokārt uz katras atsevišķas sastāvdaļas dinamikas analīzi. Pielietojot šādu modeli, var apsvērt komponentu funkcionalitātes pastāvīgu līmeņa degradāciju, resursu trūkumu, ārējo un iekšējo kļūmju dinamiku un citas parādības. Parasti šādiem modeļiem ir kvantitatīvais raksturs un tie kalpo operatīviem mērķiem. Simulācijas metodoloģija tiek izmantota, lai novērtētu ietekmes, kurus izraisa kļūmes, izmantojot scenāriju, kurā iesaistās vairākas nevienmērīgas, savstarpēji saistītas infrastruktūras [56, 10].

Viena no daudzsoļākajām pieejām mijiedarbības analīzei kompleksos tīklos ir programmu aģentu paradigma [11]. Šo modeļu pamatā ir ideja, ka kompleksa uzvedība ir mijiedarbību rezultāts starp autonomajiem un elementāriem indivīdiem, kas darbojas uz vienkāršu noteikumu pamata. Tāpat savstarpēji saistīto infrastruktūru uzvedību var analizēt, izmantojot „bottom-up” pieeju, kad visu sistēmu sāk modelēt no vienkāršo (lokālo) elementu darbības, un nākamajā solī, novērtējot kopējas sistēmas evolūciju, analizē, kā tās komponenti mijiedarbojas ar savā starpā [11].

Vairākos ES realizētos projektos tiek izmantoti dažādi imitācijas rīki, starp tiem visbiežāk tiek pieminēti:

- Programmu aģentu imitatori;
- Reāllaika imitatori;
- Domēna imitatori;
- Uz notikumiem balstītie imitatori;
- Uz ontoloģiju balstītie imitatori;
- Funkcionālie emulatori;
- Kombinatorisku metožu imitatori;
- Ieejas-izejas neoperējamības modeļi vai Ļeontjeva modeļi;
- Entītijas-mijiedarbību imitatori;
- Ekspertu sistēmas;
- „Monte Carlo” imitatori.

Papildus nosauktiem eksistē vēl imitācijas rīku dažādas kombinācijas.

Šajā pētījumā kā piemērs tiek aprakstīti šādi imitācijas modeļi:

- Uz pakalpojumiem bāzētie modeļi (SimCIP)
- Programmu aģentu modeļi un federatīvie modeļi (DIESIS)
- Piedāvājuma un pieprasījuma tipa modeļi (I2Sim)

2.4.1. Uz pakalpojumiem bāzētie modeļi (SimCIP)

Projekts IRRISS [76] tika uzsākts 2006. gadā ar mērķi noteikt savstarpējas atkarības starp infrastruktūrām, izmantojot programmu aģentu imitatorus, un attīstīt starpprogrammatūru (Middleware Improved Technology - MIT), un veicināt uz IT balstītu komunikāciju starp dažādu infrastruktūras operatoriem.

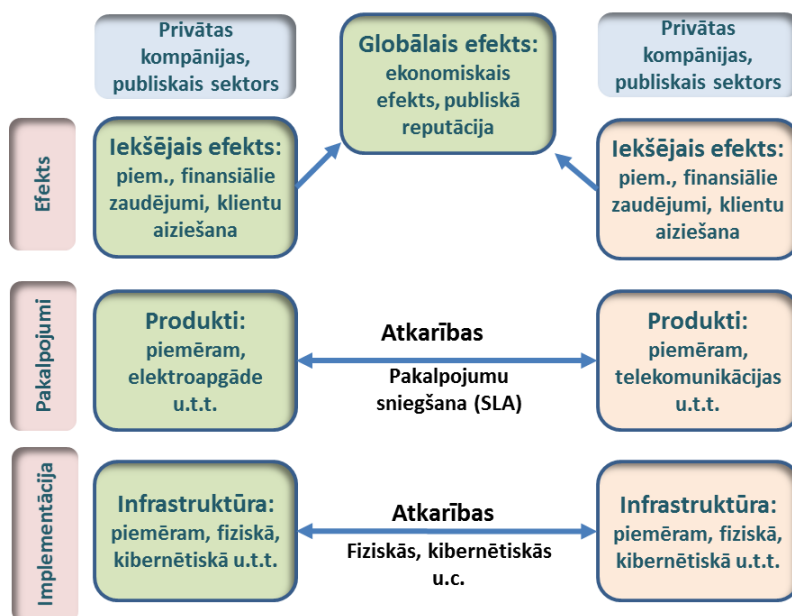
Atbilstoši scenārijam veiktā imitācija balstās uz reālu scenāriju, nosauktu par "Rome Mini Telco Blackout". Scenārijs imitēja notikumus Romā, kad 2004 2. janvārī tika appludināti Telecom Italia telekomunikācijas mezgli.

Imitators SimCIP izmanto „Services and Effect – ISE” modeli (sk. 2.9. attēlu). ISE modelis sastāv no trim pilnīgi atdalītiem līmeņiem:

1. Implementācijas līmenis: apkopo domēna specifiskus datus, loģiku un sastāvdaļu darbības modeli;
2. Pakalpojumu līmenis: datu apmaiņa starp dažādiem modeļa komponentiem (iekšējais vai ārējais domēns);
3. Darbības līmenis: datu apstrādes analīze.

Kā programmu aģentu imitators SimCIP var simulēt vairākas heterogēnas infrastruktūras integrētā vidē. SimCIP uzdevums ir noteikt mijiedarbības starp komponentiem, nosakot sākotnējās vērtības, vākt un novērtēt imitācijas rezultātus, ko veic ārējie imitatori.

Aģenti iekapsulē tīkla komponentu stāvokli, un daži no tiem tiek pārveidoti par mainīgiem, kas ir pietiekami abstrakti, lai ISE modelī veiktu ar tiem apmaiņu noteiktajā pakalpojumu slānī. Projektā izmantotais SimCIP imitēja elektrotīkla un telekomunikāciju tīkla mijiedarbības, bet PPS-Sincal un NS-2 attiecīgi tika izmantoti kā divu infrastruktūru ārējie imitatori.

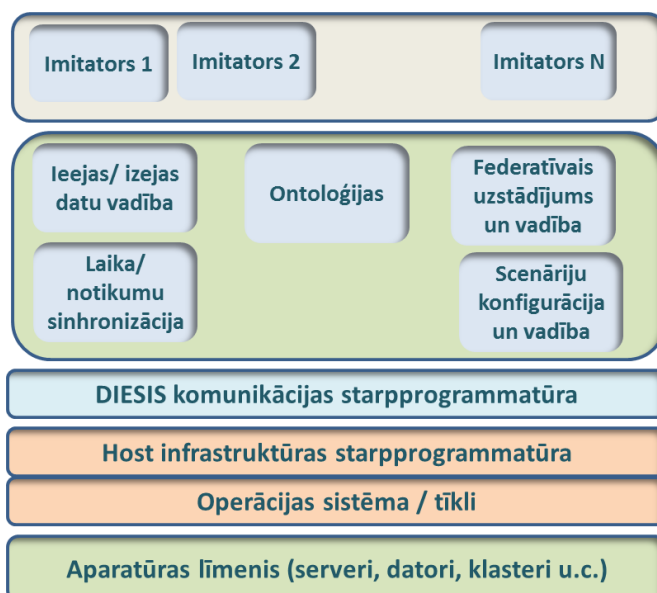


2.9.att. „Service-Effect ISE” kritisko infrastruktūru imitatora blokshēma [77]

2.4.2. Programmu aģentu modeli un federatīvie modeli (DIESIS)

Projekts DIESIS, kuru finansēja Eiropas Komisija, tika uzsākts 2008. gadā [64]. Projekta uzdevums ir veikt pētījumus ar mērķi izstrādāt federatīvās imitācijas rīku, lai veiktu kritisko infrastruktūru mijiedarbības modelēšanu un imitāciju. Bija plānots, ka jauns rīks kļūs par daļu no Eiropas e-infrastruktūras [76], kas ļautu pētniekiem piekļūt unikāliem un dalītiem resursiem, tostarp datiem, instrumentiem, skaitļošanas un komunikāciju resursiem. Šāda Eiropas e-infrastruktūra atbalsta dažādu partneru sadarbību, veicot kritiskās infrastruktūras pētījumus, vienlaikus saglabājot konfidencialitāti un tiesības un intelektuālu īpašumu, kas piemīt dažādiem modeļiem un imitācijas paketēm.

Kā parādīts 2.10 attēlā, starpprogrammatūra ir izstrādāta, lai nodrošinātu sadarbību starp dažādām federatīviem imitatoriem pēc augsta līmeņa arhitektūras principa (High-Level Architecture - HLA).



2.10.att. DIESIS arhitektūra [64]

Starpprogrammatūra atbalsta arī scenāriju konfigurāciju un pārvaldību un simulācijas veikšanu, izmantojot darbplūsmas. Turklāt DIESIS [64] modelī ir iekļauta ontoloģija, kas ļauj pielietot zināšanas par heterogēnām infrastruktūrām un veikt aprakstus par infrastruktūrām un starpsavienojumiem starp infrastruktūras tīkliem.

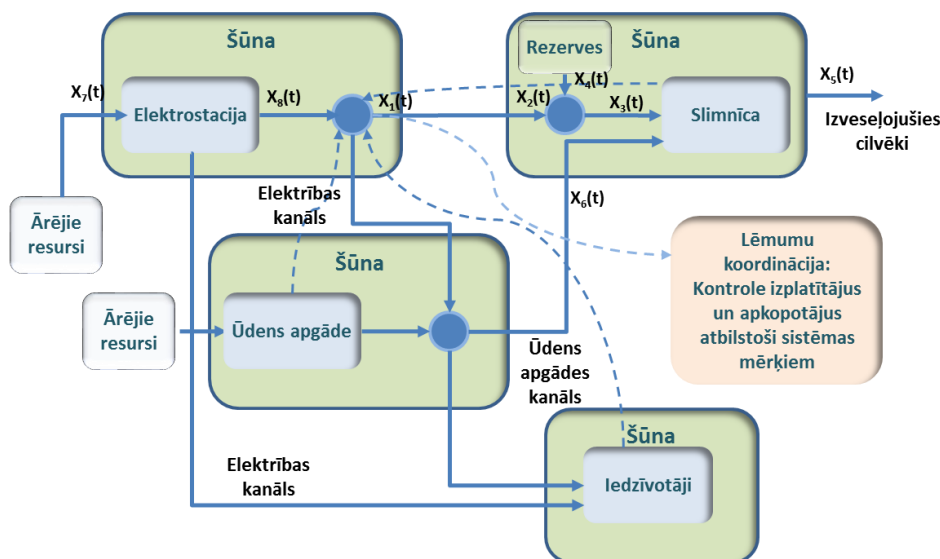
DIESIS-ontoloģija tika izmantota, lai raksturotu trīs dažādas infrastruktūras: dzelzceļš, elektroapgāde un telekomunikācijas tīkls. Lai pierādītu ontoloģijas pielietojamību, tika izmantots Romas plūdu scenārijs no iepriekš minēta IRRISS projekta.

2.4.3. Piedāvājuma un pieprasījuma tipa modeļi (I2SIM)

Par piemēru šāda tipa modeļiem var kalpot I2Sim imitācijas vide, kuru izstrādāja Britu Kolumbijas Universitāte JIRP projekta ietvaros [48]. Sistēmas darbība balstās uz resursu plūsmas modelēšanu, kuru veic starp infrastruktūru sastāvdaļām, neatklājot savas iekšējas detaļas. Katrs komponents izmanto iekšējo modeli, lai novērtētu savu statusu, bet I2Sim apvieno šos modeļus vienotā „sistēmas sistēmu” risinājumā.

Simulatora galvenais uzdevums ir atspoguļot laika skalā notikumus tā, lai būtu iespējams prognozēt globālas sistēmas attīstību atkarībā no konkrētiem pieņemtiem lēmumiem. I2Sim papildus uzdevums ir veikt analīzi un atklāt neaizsargātās vietas sistēmā, kā arī nepilnības sistēmas darbināšanas procedūrās. Līdzīgi kā Petri tīkliem, I2Sim iekļauj vienības (skat. arī 2.11):

- Šūnas (Ražošanas vienības): uzņēmus un ārējos resursus, piemēram, enerģiju, darbaspēku, izejvielas u.c.
- Kanāli (Transporta vienības): vienības, kas nodrošina transportēšanu, piemēram, vadi, caurules, ceļi.
- Marķieri (Apmaiņas vienības): apzīmē apjomu, kas tiek padots uz ievadēm vai apzīmē saražotas produkcijas apjomu izvados, piemēram, medicīnas personāls, ūdens vienības, telefona zvani u.c.)
- Vadība (Izplatītājs & Agregātors): veido saskarnes starp fizisko un lēmumu pieņemšanas slāni.



2.11.att. I2Sim ontoloģija: šūnas, kanāli, marķieri un vadība [48]

Apkopojot izskatītus piemērus, var secināt, ka nosauktie imitācijas modeļi tika izmantoti, lai pētītu fiziskās atkarības (mijiedarbības starp elektroapgādes un telekomunikācijas tīkliem), kibernetiskās atkarības (mijiedarbības starp telekomunikācijas un elektroapgādes tīkliem),

temporālās (tiek mērīta sistēmu neoperējamības izplatīšana) un tika ņemtas vērā ģeotelpiskas saiknes starp sistēmām.

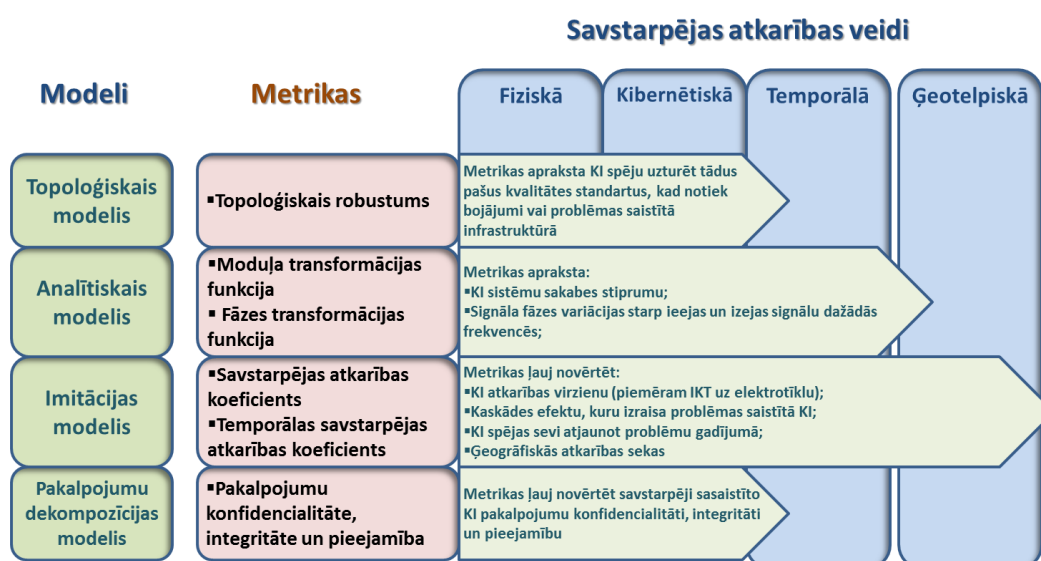
2.5. Secinājumi par otro nodaļu

Balstoties uz *datu pieejamības un granularitātes pieeju*, pētījuma autors izanalizēja modelēšanas metožu izmantošanu saistībā ar infrastruktūru savstarpējas atkarības veidiem un izdarīja secinājumus par modeļu izmantošanu (skat. 2.12. attēlu).

Topoloģiskāis modelis tiek veiksmīgi pielietots, lai pētītu fiziskās un kibernetiskās savstarpējās atkarības, tomēr tas ir maz piemērots ģeotelpiskās atkarības pētījumam un netika piemērots temporālai atkarībai. Skatoties no mērogojamības viedokļa, *topoloģiskāis modelis* ir piemērots dažāda izmēra tīkliem, ņemot vērā modeļa izstrādāšanas un analīzes izmaksas.

Analītiskais modelis tiek viennozīmīgi izmantots, lai modelētu fiziskās, kibernetiskās un temporālās savstarpējās atkarības. Tikmēr ģeotelpiskā savstarpējā atkarība netika vispusīgi modelēta. Balstoties uz modeļa izstrādāšanas izmaksām, *analītiskais modelis* ir visai tuvs *imitācijas modelim*, bet, lai gan *analītiskā modeļa* rezultātu analīze prasa mazāk skaitļošanas resursu, atgriezenisko saišu un transformāciju funkciju definēšana prasa vairāk cilvēkresursu.

Šajā nodaļā ir parādīts, ka *Pakalpojumu dekompozīcijas modelis* tiek veiksmīgi pielietots, lai pētītu savstarpējās atkarības starp pilsētas ūdens sadales tīklu, kas demonstrē savu pakalpojumu atkarību no elektroenerģijas piegādātāja pakalpojumiem, un telekomunikāciju pakalpojumu sniedzēja, izmantojot uz riska balstītu metodiku. Lai gan fiziskās un kibernetiskās atkarības ir veiksmīgi modelētas, tomēr šāds modelis ir maz piemērots ģeotelpiskās atkarības un temporālās atkarības pētījumam.



2.12.att. Izskatīto modeļu pielietojums KI savstarpējas atkarības pētījumiem

Imitācijas modelis dod iespēju modelēt visus savstarpējās atkarības veidus (skat. 2.12.att.). Neskatoties uz salīdzinoši augstām cilvēkresursu izmaksām modeļa izstrādāšanas fāzē, kuras ievērojami pieaug kopā ar pētīto tīklu apjomu un sarežģītību, tas vislabāk der, lai pētītu savstarpējās atkarības starp pilsētas ūdens sadales, elektroapgādes un telekomunikāciju tīklu. *Imitācijas modelis* ir vispiemērotākais, lai modelētu un imitētu fiziskās, kibernetiskās un temporālās konsekvences, kuras ūdensvada tīklā izraisa kļūmes, un bojājumus, kas notiek elektroapgādes un telekomunikācijas tīklā, tādēļ imitācijas modelis tiek izmantots triju KI mijiedarbību analīzei konkrētajā piemērā 4.nodaļā.

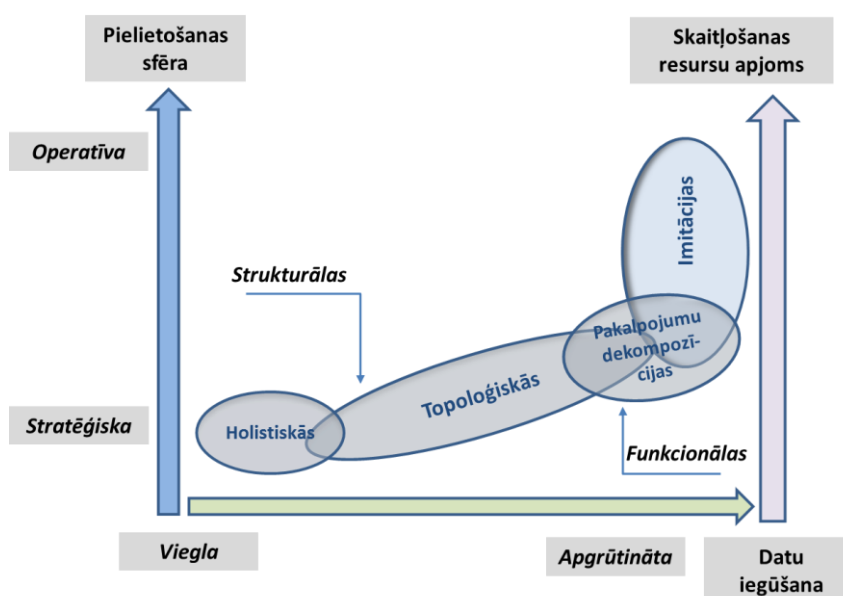
3. METRIKAS KRITISKO INFRASTRUKTŪRU ANALĪZEI

Šajā nodaļā autors pēta kritisko infrastruktūru mijiedarbības kvantitatīvus raksturojumus un veic metriku analīzi un klasifikāciju. Šim nolūkam autors izmanto 2. nodaļā veiktu modeļu analīzi un tajos izmantotas metrikas. Papildus šīs nodaļas uzdevums ir pamatot metrikas, kuras tiek pielietotas 4.nodaļā demonstrētā piemērā par elektroapgādes, telekomunikācijas un ūdens apgādes tīkla mijiedarbību.

3.1. Metriku izvēles pieejas

Metrikas, kas kvantitatīvi raksturo infrastruktūru mijiedarbības, var klasificēt šādi: metrikas, kas mēra infrastruktūru mijiedarbību makro īpašības un to ietekmi uz sistēmas kopējo funkcionalitāti, un metrikas, kas ļauj aprēķināt infrastruktūru vai tās sastāvdaļu stiprumu vai vājumu [31]. Pirmā metriku grupa spējīga atbalstīt lēmumu pieņemšanu organizatoriskā un stratēģiskā līmenī, bet otrā grupa atbalsta lēmumu pieņemšanu inženierzinātniskā vai praktiskā līmenī.

Daži pētnieki klasificē metrikas trijās dimensijās, saistot tās ar informācijas saturu, spēju atbalstīt lēmumu pieņemšanu un kalkulācijas izmaksas apjomu [16]. Tiek identificētas šādas kategorijas: metrikas, kas raksturo mijiedarbības makro vai „stāvokļa” (core) īpašības, piemēram, kļūmes izplatīšanas virzienu [78] vai ilgumu [79]. „Kodola” metrikas vērtē gan kļūmju cēloņus un sekas konkrētā infrastruktūrā vai tās sastāvdaļās, gan arī stratēģiju un mehānismus, kas ir paredzēti, lai uzlabotu kritiskas infrastruktūras aizsardzību un elastīgumu. Savukārt sektoru specifiskās metrikas raksturo konkrētas infrastruktūras stāvokli kopskatā vai sastāvdaļu līmenī.

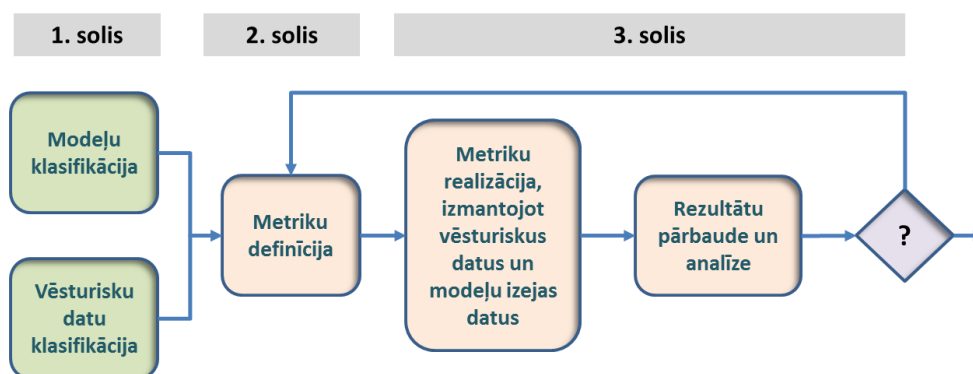


3.1.att. Mijiedarbības metriku klasificēšana ([22] ar autora papildinājumiem)

Kopumā infrastruktūru mijiedarbības novērtēšanai pielietotās metrikas var klasificēt saistībā ar pielietošanas sfērām, modeļa realizācijai nepieciešamu resursu apjomu un izejas datu iegūšanai vajadzīgu laiku un darbu apjomu [22] (skat. 3.1. att.).

Kā parādīts 3.1. attēlā, holistiskas metrikas ir samērā viegli izstrādāt un pielietot, bet jāatceras, ka tās ir fundamentāli un stratēģiski orientētas. No otras puses, imitācijas modeļos izmantotās metrikas spēj sniegt operatīvo informāciju, taču tās prasa vairāk skaitļošanas resursu un pietiekoši detalizēti izstrādātus modeļus. Tas ir problemātiski, jo, pirmkārt, kritiskās infrastruktūras operatori nevēlas sniegt savus datus, baidoties, ka tie var aizplūst pie konkurentiem, un, otrkārt, tāpēc, ka jāvāc milzīgs datu apjoms. Grafika vidū ir izvietotās topoloģiskā un pakalpojumu dekompozīcijas modeļa metrikas, kas attiecībā uz dažiem aspektiem satur abu iepriekšējo klašu priekšrocības un trūkumus. Piedāvātā metode metriku noteikšanai un ieviešanai ir parādīta 3.2.attēlā. Tā paredz šādus soļus [14]:

- a) **Modeļu un vēsturisku datu klasifikācija.** Modeļu un datu apzināšana ir divi paralēlie vai alternatīvie procesi. Modeļi ir izveidoti, lai atveidotu un abstrahētu savstarpējās atkarības starp infrastruktūrām un iegūtu metrikas (parasti no stohastiskās simulācijas procesa). Datus parasti iegūst no ierakstiem par uzņēmumu kļūmēm un avārijām un tos izmanto, lai izveidotu datu bāzi par „cietušajiem” infrastruktūras komponentiem un kļūmju secību. Metrikas var aprēķināt no vēsturiskiem datiem un no modeļa izejas rezultātiem.
- b) **Metriku definīcija.** Otrajā solī izstrādā metrikas, kuras ļauj kvantitatīvi raksturot savstarpējo atkarību un kuras ir piemērotas elektroapgādes, IKT un ūdens apgādes tīklu mijiedarbības raksturošanai.
- c) **Metriku ieviešanas process.** Šajā etapā tiek veiktas procedūras, algoritmi un pielietoti instrumenti, lai aprēķinātu izvēlētās metrikas. Iegūtie rezultāti tiek novērtēti, veidojot atgriezenisku saiti ar 2. soli.



3.2. att. Metriku noteikšanas un ieviešanas algoritms [14]

Analizēto projektu pieredze rāda [22, 26, 13, 76], ka nav iespējams izveidot visaptverošas metrikas, kas būtu pielietojamas kopējā vērtību līmenī visiem savstarpējās atkarības veidiem. Tā kā viens no šā pētījuma mērķiem ir elektroapgādes, IKT un ūdens apgādes tīklu mijiedarbes kvantitatīva raksturošana, tāpēc ir svarīgi noteikt metrikas, kas kvantitatīvi mēra atkarības starp šīm sistēmām un komponentiem.

3.2. Atkarības novērtēšanas metrikas

Lai novērtētu mijiedarbības starp infrastruktūru mezgliem, autors piemēroja darbā [14] izstrādātās un pētījuma autora aprobētās metrikas [89], proti: *Fiziskās atkarības koeficients (FAK)*, *Kibernētiskās atkarības koeficients (KAK)* un *Ģeotelpiskās atkarības koeficients (ĢAK)*.

Iepriekš minēto koeficientu mērķis ir novērtēt:

- Atkarības virzienu un arī savstarpējās atkarības klātbūtni gadījumā, ja ir konstatētas atkarības pretējā virzienā;
- Sakabes spēku saistībā ar darbības virzienu.

Atkarības koeficientus aprēķina šādi:

Ūdens infrastruktūras Fiziskās atkarības koeficients

$$FAK_{NW} = \frac{N(NW | NP)}{N(NP)},$$

(3.1)

kur $N(NP)$ ir elektroapgādes tīkla mezglu darbības traucējumu proporcija un $N(NW/NP)$ ir ūdensapgādes tīkla mezglu darbības traucējumu proporcija energosistēmas zudumu dēļ.

Telekomunikācijas infrastruktūras Fiziskās atkarības koeficients:

$$FAK_{NT} = \frac{N(NT | NP)}{N(NP)}, \quad (3.2)$$

kur $N(NT/NP)$ telekomunikācijas tīkla mezglu darbības traucējumu proporcija energosistēmas zudumu dēļ.

$N(NP)$ ir jāizvērtē kā skaitu, kad elektroapgādes infrastruktūra vai tās sastāvdaļas degradēja pakalpojumu kvalitāti ārēju notikumu dēļ T laika intervālā.

Turklāt tiek ieviests elektroapgādes infrastruktūras degradācijas jēdziens, kas ir saistīts ar telekomunikācijas infrastruktūras ietekmi.

Kibernētiskās atkarības koeficients:

$$KAK_{NP} = \frac{N(NP | NT)}{N(NT)}, \quad (3.3)$$

kur $N(NP)$ ir elektroapgādes tīkla mezglu darbības traucējumu proporcija un $N(NP/NT)$ ir elektroapgādes tīkla mezglu darbības traucējumu proporcija sakaru pārtraukumu dēļ.

Ģeotelpiskās atkarības koeficients:

$$GAK_{NWTP} = \frac{N(NW|NP)}{N(NP)} + \frac{N(NT|NP)}{N(NP)} + \frac{N(NP|NT)}{N(NT)}, \quad (3.4)$$

kur $N(NW/NP)$, $N(NT/NP)$ un $N(NP/NT)$ ūdens, telekomunikāciju un elektroapgādes infrastruktūru traucējumu proporcija ģeotelpisku faktoru dēļ.

Apskatot koeficientus (3.1)-(3.4), var pieņemt, kā tā vērtība var būt mazāka, lielāka vai ekvivalenta "1". Ja $N(NW/NP)/N(NP) \geq 1$, tas nozīmē, ka ūdensapgādes tīkla mezgliem ir spēcīga atkarība no elektroapgādes tīkla mezgliem. Atbilstoši, ja $N(NW/NP)/N(NP) < 1$, tas nozīmē, ka ūdensapgādes tīkla mezgliem ir vāja atkarība no elektroapgādes tīkla mezgliem, turklāt jo tuvāk koeficienta vērtība nullei, jo vājāka ir atkarība.

Laika mērogā izteiktās savstarpējās atkarības

Metrikas tiek pielietotas, lai kvantitatīvi izmērītu vienas infrastruktūras ietekmi uz otru, novērtējot pārtraukuma vai zaudējumu posma ilgumu un atbilstoši atjaunošanas posma ilgumu ietekmējamajā infrastruktūrā. Zimmerman un Restrepo [79] izstrādāja vienkāršu metriku, lai to izmantotu saistībā ar elektroenerģijas zudumiem un to ietekmi uz citām nozarēm, proti, **lavīnveida efektu relatīvais ilgums**, kas mēra pārtraukuma posma ilgumu $T(e)$ ietekmējošā infrastruktūrā un pārtraukuma vai zaudējumu posma ilgumu $T(i)$ skartā infrastruktūrā i .

Relatīvais ilgums tiek aprēķināts kā $T(i)/T(e)$ attiecība, un tas tiek izmantots, lai mērītu savstarpējās atkarības laika vienībā un lai interpretētu lavīnveidīga efekta virzienu. Jēdziens *Relatīvais ilgums* var būt izmantots scenārijā, kurā notiek elektroapgādes, telekomunikācijas un ūdens apgādes tīkla mijiedarbība, lai mērītu *Fiziskās atkarības relatīvo ilgumu (FRI)* un *Kibernētiskās atkarības relatīvo ilgumu (KRI)*.

Lai izrēķinātu *relatīvu ilgumu*, tiek izmantots [79] *dīkstāves ilguma* jēdziens $T(\cdot)$, kas apzīmē laika intervālu, kurā visas sistēmas vai tās komponentu pakalpojumu kvalitātes (QoS) līmenis atšķiras no vēlamā vai saskaņotā kvalitātes līmeņa.

Ūdens apgādes tīkla mezglu **Fiziskās atkarības relatīvais ilgums:**

$$FRI_{NW} = \frac{T(NW)}{T(NP)} \quad (3.5)$$

Telekomunikācijas tīkla mezglu **Fiziskās atkarības relatīvais ilgums:**

$$FRI_{NT} = \frac{T(NT)}{T(NP)}, \quad (3.6)$$

kur $T(NP)$ elektroapgādes tīkla dīkstāves ilgums; $T(NW)$ un $T(NT)$ ūdens un telekomunikācijas mezglu dīkstāves vai pakalpojumu degradācijas ilgums, kas ir elektroapgādes tīkla dīkstāves vai pakalpojumu līmeņa degradācijas rezultāts.

Kibernētiskās atkarības relatīvais ilgums:

$$KRI_{NP} = \frac{T(NP)}{T(NT)}, \quad (3.7)$$

kur $T(NT)$ telekomunikācijas mezglu dīkstāves vai pakalpojumu degradācijas ilgums un $T(NP)$ elektroapgādes tīkla mezglu dīkstāves vai pakalpojumu degradācijas ilgums, kas ir telekomunikācijas tīkla dīkstāves vai pakalpojumu līmeņa degradācijas rezultāts

Ja attiecības (3.5), (3.6) vai (3.7) ir mazākas par 1, tas nozīmē, ka atkarīgai infrastruktūrai ir atjaunošanas un reģenerācijas īpašības, vai aizsardzības pret defektiem mehānisms ir pietiekoši spēcīgs, lai mazinātu atkarības efektu. Tieši pretēji, ja attiecības (3.5), (3.6) vai (3.7) ir lielākas vai vienādas ar 1, tad atkarīgas infrastruktūras ir cieši saistītās ar kļūmju avotu.

Papildus definētām metrikām 2.sadaļā tika definētas arī metrikas:

- **Tīkla topoloģiskais robustums** = $\langle 1 - P2 \rangle$. Analizējot uz topoloģiskās pieejas balstītus modeļus, tika izmantots pieņēmums "N-1 robusts", kas nozīmē tīkla spēju izpildīt savas funkcijas, kad viens - no tā N komponentiem iziet no ierindas. Tiek ieviesta arī varbūtība P_2 , kas kalkūlē katra elektroapgādes mezgla pārvaldības zaudēšanu, divu telekomunikācijas mezglu vienlaicīga atteikuma rezultātā: $P2(i) = N_i / n(n-1)$.
- Pētot uz **analītiskās pieejas** balstītus modeļus, tiek definētas metrikas:
 - **Moduļa transformācijas funkcija** $|G(j\omega)|$, kas nodrošina metriku, ar kuru var mērīt saikni starp infrastruktūrām, kuru darbību modelē.
 - **Fāzes transformācijas funkcija** $\angle G(j\omega)$, kas analīze fāzes atšķirības starp ievades un izejas signālu dažādos frekvenču intervālos.
- Pētot uz **pakalpojumu dekompozīcijas** principiem balstītus modeļus, tiek definētas metrikas:
 - **Konfidencialitāte**: nav neatļautas informācijas izpaušanas attiecībā par datiem, kuru izmanto kritiskā infrastruktūra;
 - **Integritāte**: nav neatļautas izmaiņu sistēmas saistībā ar kritisko pakalpojumu sniegšanu;
 - **Pieejamība**: gatavība sniegt kritisko pakalpojumu ar atbilstošu servisa līmeni.

3.3. Secinājumi par metriku izvēli

Šajā pētījumā izmantotā metodoloģija dod iespēju izstrādāt metrikas, ar kurām var kvalitatīvi un kvantitatīvi novērtēt kritisko infrastruktūru mijiedarbības (savstarpējas atkarības). Iegūtie rezultāti tiek apkopoti 3.1. tabulā:

3.1. tabula

Metrikas kritisko infrastruktūru mijiedarbības novērtēšanai

Nr.	Metrikas	Savstarpējas atkarības veids			
		Fiziskās	Kibernētiskās	Ģeotelpiskās	Temporālas
1	Fiziskās atkarības koeficients	Jā	Jā	Jā	Nē
2	Kibernētiskās atkarības koeficients	Jā	Jā	Jā	Nē
3	Ģeotelpiskās atkarības koeficients	Jā	Jā	Jā	Nē
4	Fiziskās atkarības relatīvais ilgums un Kibernētiskās atkarības relatīvais ilgums:	Nē	Nē	Nē	Jā
5	Tīkla topoloģiskais robustums	Jā	Jā	Nē	Nē
6	Moduļa transformācijas funkcija un Fāzes transformācijas funkcija	Jā	Jā	Nē	Jā
7	Pakalpojuma konfidencialitāte, integritāte un pieejamība	Jā	Jā	Nē	Nē

3.1 tabulā izmantotās metrikas kopumā nosedz visus kritisko infrastruktūru mijiedarbības veidus, tomēr tiek secināts, ka nav iespējams izveidot visaptverošas metrikas, kas būtu pielietojamas kopējo vērtību līmenī visiem savstarpējās atkarības veidiem.

Atbilstošu metriku identificēšana ir ļoti svarīga, lai nodrošinātu reāla vai "fiziska" modeļa izveidošanu un imitāciju, jo metriku analīze tiek izmantota, lai pieņemtu lēmumus par darbībām, kurus būtu jāveic, lai samazinātu savstarpējās ietekmes riskus. Domājot par savstarpējās atkarības metriku praktisko izmantošanu, ir jāņem vērā:

- Rezultātu novērtējums un apstiprināšana, kad metrikas izmēģina reālā piemērā;
- Modeļa parametru kritisko robežu noteikšana, jo var pieļaut, ka modelēšanas parametri ir pamatoti tikai noteiktās robežās. Par modelēšanas parametriem tiek uzskatītas modelī izmantotās datu vērtības, piemēram, elektroapgādes tīkla bojājumu ilgums, modeļa imitācijas laiks, rezerves barošanas avota darbības ilgums.

Ņemot vērā, ka iepriekšējā nodaļā tiek pamatota imitācijas modeļa izmantošana triju kritisko infrastruktūru mijiedarbības analīzei, tiek izvēlētas imitācijas modelim vispiemērotākās metrikas: *Ūdens infrastruktūras fiziskās atkarības koeficients (FAK)* un *Ūdens infrastruktūras fiziskās atkarības relatīvais ilgums (FRI)*. FAK tiek mērīts kā procentuāli izteikta attiecība, savukārt FRI tiek mērīts kā laika posms, kurš tiek izteikts stundās, minūtēs u.t.t.

Izvēlētas metrikas turpmāk tiek aprobētas, izmantojot reālus datus, kas iegūti no bojājumu uzskaites statistikas, datus, kas iegūti modeļa imitācijas procesā, un datus, kas ir iegūti pētījumos par ūdens apgādes nozares problēmjaudājumiem.

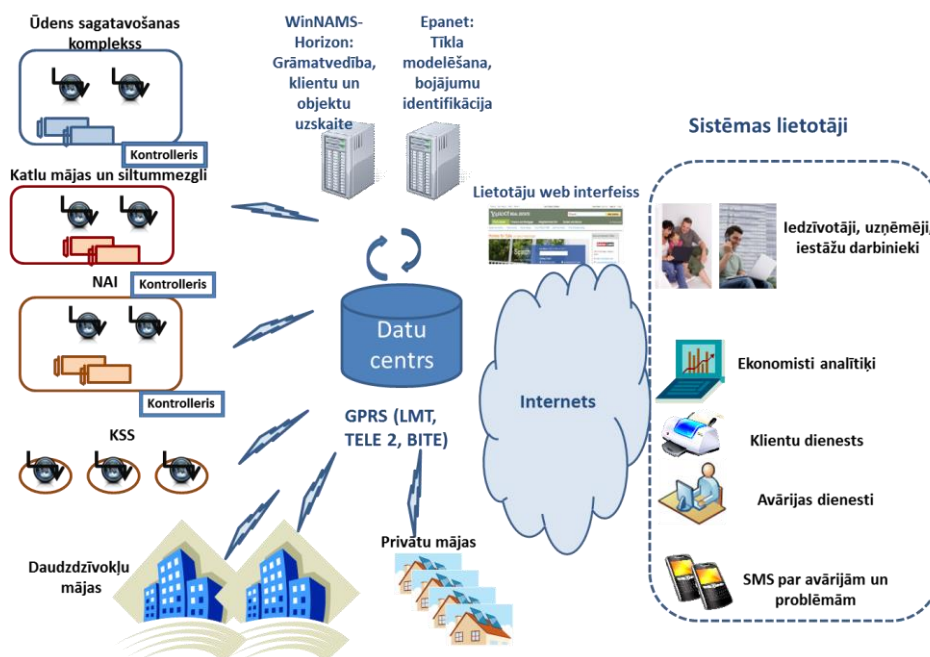
4. ELEKTROAPGĀDES, TELEKOMUNIKĀCIJU UN ŪDENSAPGĀDES TĪKLU MEZGLU MIJIEDARBĪBAS MODEĻA IZVEIDE UN SIMULĀCIJA

4.1. Scenārija pamatojums un apraksts

Pēdējo gadu laikā vairākas automatizētas mērījumu nolasīšanas sistēmas AMR (Automatic Meter Reading) un viedu mērījumu infrastruktūras AMI (Advanced Metering Infrastructure) ir uzstādītas ūdens apgādes tīklos (ŪAT) un siltuma sadales tīklos (SST) Latvijas pašvaldībās ar mērķi samazināt ūdens noplūdes un siltuma zudumus, lai uzlabotu norēķinus un klientu apkalpošanu, kā arī uzlabotu siltumapgādes pakalpojumu efektivitāti.

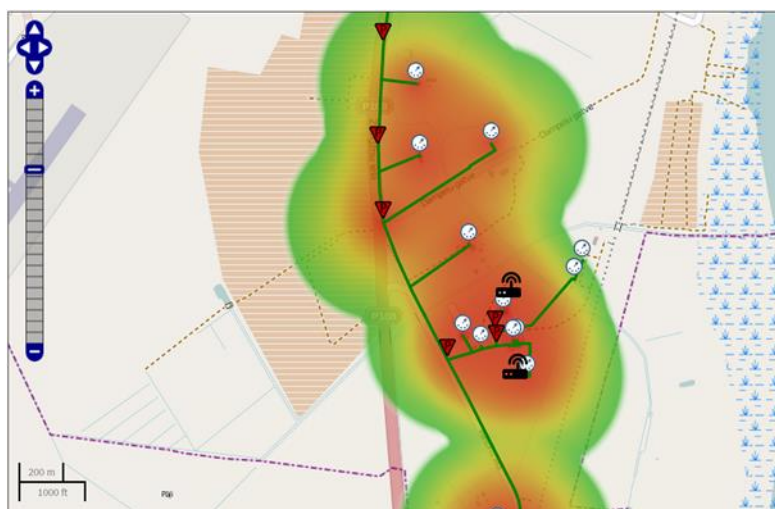
Kā piemēru var pieminēt Kuldīgas novada komunālās saimniecības datorizētā modeļa izveidi, kuru izstrādāja projekta „Komunālās saimniecības sistēmas modeļu izveide Kurzemes reģionā” ietvaros [86]. Piedāvātais modelis paredzēja periodisku automātisku mērījumu datu savākšanu no ūdenssaimniecības objektiem (ūdens sagatavošanas kompleksi, notekūdeņu attīrīšanas iekārtām u.c.), ka arī no siltumsaimniecības objektiem - katlu mājām, siltummezgliem un apakšstacijām - (skat. 4.1. att.). Mērījumu dati tiek izmantoti avāriju dienestu un klientu dienestu vajadzībām, ka arī uzņēmumu darbības plānošanai. Līdzīga Kuldīgas modelim automatizēta mērījumu nolasīšanas sistēma tika ieviesta 2010-12. gadā trijos Latvijas novados: Krāslavā, Preiļos un Līvānos. Gan ūdens sadales tīklā, gan pie klientiem tika uzstādītas 4250 datu nolasīšanas ierīces, kuras mijiedrobojas vienotā bezvadu tīklā ar datu centru, izmantojot 195 vārtejas – koncentratorus, kas darbojas GSM/GPRS tīklā [9].

Prasības sistēmas noturībai pret kļūmēm, kas notiek elektroapgādes vai GSM tīkla bojājumu gadījumos, atšķiras atkarībā no datu izmantošanas mērķiem. Piemēram, datus, kurus izmanto norēķinos ar klientiem, kā rāda pieredze, pietiek apkopot reizi dienā. Savukārt, ja ūdensvada tīkla stāvokļa analīzi veic ar mērķi identificēt tīkla bojājumus, noplūdes vai patvaļīgus pieslēgumus, datus ir jāanalizē ik pēc dažām minūtēm. Piemēram, uz riska analīzes bāzēta ūdensvada noplūdes identifikācijas sistēma, kas tika ieviesta Harrogate pilsētā North Yorkshire apvienotā Karalistē [73], analizē datus ik piecās minūtēs, savukārt „Talsu novada datorizētas ūdenssaimniecības vadības kontroles sistēmas” projekta uzdevums noteica ūdens spiediena datus apkopot ik pēc 10 minūtēm [85].



4.1. att. Kuldīgas novada komunāla saimniecības datorizēta modeļa blokshēma (Zabašta [86])

“Smart Metering” projekta ietvaros [57] 2012-13. gadā Ventspilī sadarbībā ar SIA Ūdeka, ierobežotā ŪAT segmentā, tika izveidots bezvada sensoru tīkls, ar kura palīdzību tiek vākti mērījumu dati no 14 ūdens plūsmu un 9 ūdens spiediena mērītājiem. Tika veikti pētījumi, lai izmēģinātu noplūžu identifikācijas metodes un tiek izstrādātas metrikas, lai novērtētu ŪAT stāvokli, balstoties uz sensoru bezvada tīkla mērījumiem, un lai salīdzinātu ar izveidoto teorētisko tīkla modeli. 4.2. attēls atspoguļo ŪAT sensoru bezvadu uzraudzības sistēmas ekrāna attēlu. Šajā teritorijā atrodas viena transformatoru apakšstacija un viena GSM bāzes stacija.



4.2. att. ŪST sensoru bezvadu uzraudzības sistēmas ekrāna attēls

Pēdējos gados realizēto projektu izpēte [86, 85, 73, 57, 88] rāda, ka telekomunikāciju operatoru infrastruktūra, galvenokārt GSM-GPRS un Wi-Fi tīkli, kļuva par neatņemamo AMR un AMI sastāvdaļu, tāpēc mērķis ir izmērīt un novērtēt, ka dīkstāves un bojājumi, kas notiek elektroapgādes un telekomunikācijas tīkla mezglos, izplatās un izpaužas ūdens sadales tīkla mezglos. Datu nolasīšanas, apstrādes un pārraides ierīces, kas ir uzstādītas ŪAT mezglos, reprezentē šajā pētījumā ŪAT infrastruktūru, kas mijiedarbojas ar elektroapgādes un telekomunikācijas tīkla mezgliem.

Piedāvātais modelēšanas scenārijs imitē ŪAT mezglu mijiedarbību ar elektroapgādes un telekomunikācijas tīkla mezgliem. Lai gan šis scenārijs balstās galvenokārt uz pētījumiem, veiktiem Ventspils ŪAT izmēģinājumā segmentā, eksperimenta rezultāti var būt vispārināti un atkārtoti, ņemot vērā citu ŪAT infrastruktūras īpašības.

Šis pētījums ir pirmais šajā jomā mēģinājums Latvijā un arī Baltijā izstrādāt un izmēģināt modeli, kas imitē triju kritisko infrastruktūru savstarpējo ietekmi un kvantitatīvi mēra savstarpējās atkarības.

Tiek izvirzīts pieņēmums:

- a) Piedāvātais modelis ļauj izpētīt ūdens apgādes tīkla mezglu vidēja dīkstāves laika (ŪMDL) atkarību no rezerves barošanas avota darbības laika (RBDL) un rezerves barošanas avota nomainīšanas laika (RBNL) savstarpējo korelāciju noteikto parametru robežās un apstākļos, kad notiek elektroapgādes un telekomunikācijas tīkla dīkstāves.
- b) Ir iespējams izvērtēt savstarpējas mijiedarbības ar polinomu, un minimizētu ūdensvada tīkla mezglu vidējo dīkstāves laiku noteikto parametru robežās.

$$R_{i,j,k} = f(t, m_j^1, m_j^2, \dots, m_j^p, m_k^1, m_k^2, \dots, m_k^p; m_i^1, m_i^2, \dots, m_i^r) \rightarrow \min, \text{ kur } m_j^l \in M_j; m_k^n \in M_k; m_i^r \in M_i$$

$R_{i,j}$ - funkcija $f(.)$ laika t . Specifisku metriku kopa: M_j (elektroapgādes tīkls), M_k (telekomunikācijas tīkls) un M_i , (ūdens apgādes tīkls), kurus izmanto, lai mērītu infrastruktūru j, k un i rezultativitātes līmeni.

4.2. Modeļa parametru izvēle un pamatojums

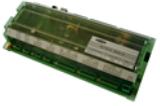





4.2.1. Ūdensapgādes tīkla mezglu parametru noteikšana

Lai izvēlētos ūdensvada tīkla mezglu parametrus, pētījuma autors veica Baltijas un EU tirgu piedāvāto tehnisko risinājumu apskati. Apskats ļauj izdarīt secinājumus, ka viens no galvenajiem AMR/ AMI elementiem, protams, vārtejas – koncentratori ar retu izņēmumu neizmanto rezerves barošanu (skat. 4.1. tabulu). Apzinoties šo problēmu, daži Latvijas un Lietuvas pētnieki veic pētījumus, ar mērķi izveidot risinājumus vārteju rezerves barošanai,

izmantojot tipveidīgas baterijas vai akumulatorus, līdzīgus tiem, kurus jau pielieto sensoru – transiveru elektroapgādei. Viens no šādiem piemēriem ir „Smart Metering” projekts [88].

4.1. tabula

Vārteju – koncentratoru raksturojumi saistībā ar elektroapgādi

Attēls	Nosaukums, ražotājs	Funkcionalitāte	Elektroapgāde	Baterijas aptuvenais darbības laiks
	DKEG-10 „Valsena” sadarbībā ar „Sigma Telas”, Lietuva	Saņem signālus no ūdens, siltuma, spiediena un elektrības mērītājiem. Datu apmaiņai ar centrālo sistēmu izmanto GSM/GPRS un/ vai Ethernet.	Ārēja barošana 220 – 380v; Jauda 10W	0,5 - 1 stunda
	Mazzy Aqua TB3 – TB6 SIA Micro Dators, SIA Mazzy, Latvija	Saņem signālus no Mazzy TCR ūdens sensoriem un, izmantojot GSM/ GPRS, pārsūta uz serveri.	Ārēja barošana 220v; Maksimāla jauda 1.3W	3 – 5 stundas
	Gateway Scout-WEB (ar moduli 500 mW). „Sensus”, ASV / Kanāda	Saņem signālus no ūdens mērītājiem. Datu apmaiņai ar centrālo sistēmu izmanto GSM/GPRS un/ vai Ethernet.	Ārēja barošana 220v; Maksimāla jauda 0.5 – 1W	4 – 6 stundas
	Mazzy Heat TB2 SIA Micro Dators, SIA Mazzy, Latvija	Saņem signālus no Mazzy TCR siltuma sensoriem un, izmantojot GSM/ GPRS, pārsūta uz serveri.	Ārēja barošana 220v; Maksimāla jauda 1.3W	3 – 5 stundas
	DJGZ23-STAR1101 PLC Datu Koncentrators. „Star Instrument”, Ķīna	Saņem signālus no enerģijas mērītājiem. Datu apmaiņai ar centrālo sistēmu izmanto GSM/GPRS un/ vai elektroapgādes līnijām.	Ārēja barošana 220 – 380v; Jauda 10W	0,5 - 1 stunda
	WaterMind Commercial & Industrial AMI GSM Supervision. „Itron”, Kanāda	Balstās uz Itron WaterMind sistēmas arhitektūru, apstrādā ūdens plūsmas un spiediena mērījumus. Datu apmaiņai ar centrālo sistēmu izmanto GSM/GPRS.	Ārēja barošana 220v un/ vai litija baterijas. Dati par jaudu netika publicēti.	Ražotājs apgalvo, ka raidot datus tikai reiz diena, tad baterija nodrošinās barošanu 5 gadus.

Tātad, plānojot ūdens apgādes mezglu parametrus triju infrastruktūru mijiedarbības modelim, jāpatur prātā, cik ilgi vārtejas – koncentratori būtu spējīgi darboties, izmantojot tipveidīgus rezerves barošanas avotus. 4.1. tabulā var redzēt, ka vidējais aprēķinātais vārteju - koncentratoru funkcionēšanas laiks ārējas elektroapgādes zaudēšanas apstākļos svarstās 0.5–6 stundas robežās. Ar lielu varbūtību var pieņemt, ka rezerves barošanas izmaksas šajā laika diapazonā nav tieši saistītas ar aparātūras funkcionēšanas laiku. Tomēr rezerves barošanas risinājumi, kas nodrošinātu ilgāku laiku, piemēram, vairākus mēnešus vai gadus, prasītu citus risinājumus un daudz lielākas izmaksas.

Rezerves barošanas avota darbības laiks (RBDL): Tātad, balstoties uz iepriekšējo analīzi, tika izvēlēts ūdens apgādes tīkla mezglu darbības laiks no rezerves barošanas avotiem 0.1–6 stundas robežās.

Otrs ūdens apgādes tīkla mezglu parametrs, proti, *rezerves barošanas avota nomainīšanas laiks (RBNL)*, tiek pieņemts robežās starp 4–48 stundām. Šāds pieņēmums tiek izdarīts, balstoties uz aptaujāto ekspertu apkopotajiem viedokļiem [9, 91].

4.2.2. Elektroapgādes tīkla mezglu parametru izvēles pamatojums

Elektroapgādes tīkla mezglu parametri tika izvēlēti, izanalizējot SAFI, SAIDI un CAIDI dati par Talsu un Ventspils sadales tīkla iecirkņiem par 2011. gadu (skat. 2. Pielikumu). Papildus tika izmantoti SAFI, SAIDI un CAIDI dati par Latviju kopumā, kas bija pieejami AS „Sadales Tīkls” 2011. gada darbības pārskatā [66] (skat. 4.2. tabulu).

4.2. tabula

Dīkstāvju dati elektroapgādes sadalēs tīklos 2011. gadā

		Vidējie rādītāji				Ekstremālie rādītāji			
Iecirk-nis		SAIFI	SAIDI (min.)	CAIDI (min.)	Vidējais laiks starp dīkstāvēm (st.)	SAIFI maks.	SAIDI (min.) maks.	CAIDI (min.) maks.	VLSB (st.) min.
Talsi	Plānotie	0.0261	6.267						
	Neplānotie	0.1738	17.711						
	Kopā:	0.1999	23.978	119.936	43817	0.6480	68.1600	363	13519
Ventspils	Plānotie	0.0185	4.2694						
	Neplānotie	0.1138	11.437						
	Kopā:	0.1323	15.707	118.758	66235	0.4320	40.6800	421	20278
Latvija	Kopā:	5.6	945	168.75	1564				

Izmantojot datus no 4.2. tabulas, tiek aprēķināti modeļa parametri: Vidējais un maksimālais dīkstāves laiks (MTTR- „Mean time to repair”) un Vidējais un maksimālais laiks starp bojājumiem st. (MTTF – „Mean time to failure”) (skat. 4.3. tabulu).

4.3. tabula

Modeļa parametri: dīkstāves laiks un laiks starp bojājumiem

Rādītājs (stundas)	Talsi	Ventspils	Latvija
Vidējais dīkstāves laiks (MTTR average)	2.00	1.98	2.81
Maksimālais dīkstāves laiks (MTTR max.)	6.05	7.02	Nav pieejams
Vidējais laiks starp bojājumiem st. (MTTF average)	43817	66235	1564
Minimālais laiks starp bojājumiem st. (MTTF min.)	13519	20278	Nav pieejams

Tiek konstatēts, ka Ventspils un Talsu iecirkņu dīkstāves rādītāji ir labāki ne kā Latvijas vidējie rādītāji. Lai nodrošinātu labāku modelēšanas un imitācijas rezultātu, un labāku vizualizāciju, tiek izvēlēti Latvijas vidējie rādītāji. Papildus, lai simulācijas grafiki nebūtu pārāk gari, laiks starp dīkstāvēm tiek samazināts 5 reizes, kas neatstāj ietekmi uz imitācijas rezultātiem, jo šis laiks ievērojami pārsniedz citus simulācijas parametrus. Rezultātā modelī tiek izmantoti šādi parametri:

- *Vidējais laiks starp bojājumiem:* $1564 : 5 = 313$ st. (200 – 500 st. robežās)
- *Simulācijas laiks* ir ierobežots 4000 stundās, kas nodrošina 9-12 ciklus.
- *Vidējais dīkstāves laiks:* 2.81 stundas ($\pm 2\sigma = 0.28 - 5.34$ st.)

4.2.3. Telekomunikācijas (GSM) tīkla mezglu parametru izvēles pamatojums

Vidējais laiks starp bojājumiem (MTTF): pētījuma autoram pastāvēja dilemma, proti, vai izmantot TELE 2 bāzes staciju dīkstāvju statistiku, kas bija pieejama par 2011–2012. gadu, vai izmantot elektroapgādes tīkla modeļa imitācijas rezultātus, jo katram no variantiem ir priekšrocības un trūkumi. Ņemot vērā, ka bāzes staciju dīkstāvju statistika ir grūti korelējama ar elektroapgādes mezglu dīkstāvēm un lai, mainot modeļa parametrus, būtu iespējams reģistrēt un analizēt korelācijas, tika izvēlēts otrs variants - modeļa imitācijas rezultāti.

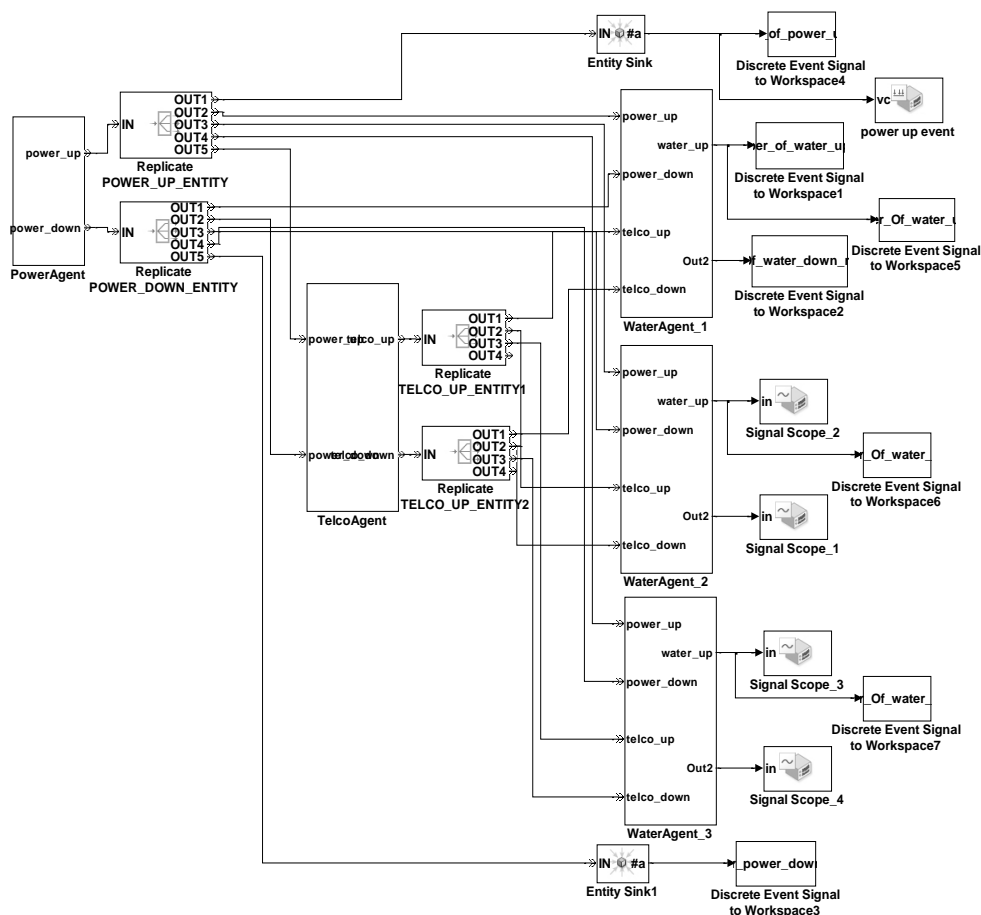
Rezerves barošanas avota darbības laiks - saskaņā ar TELE 2 normatīviem bāzes stacijas rezerves barošanas avota darbības laiks tiek projektēts 2 stundas. Izdarīts pieņēmums, ka minimālais un maksimālais darbības laiks, ko izmantotu modelī, : 0.1–5 stundas.

Vidējais dīkstāves laiks – TELE 2 papildus rezerves barošanas avotiem izmanto pārvietojamus elektroģeneratorus. Izdarīts pesimistisks pieņēmums, ka rezerves barošanas avotu nomaiņa ilgstošu elektroapgādes pārtraukumu gadījumos var svārstīties 3 - 32 stundu robežās.

4.3. Modeļa apraksts

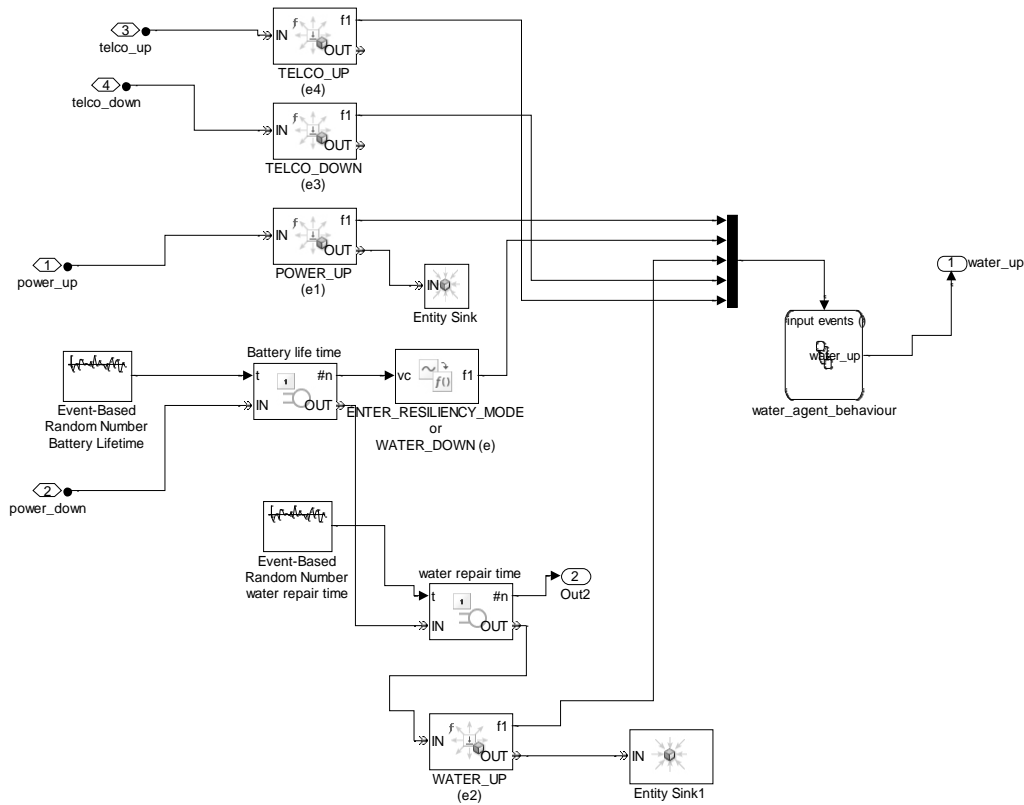
Šajā pētījumā ir izmantots MatLab[®] Simulink[®] modelēšanas un imitācijas rīks kā populārs inženieru un zinātnieku modelēšanas rīks.

4.3. attēls atspoguļo sistēmas modeli, kas ietver vienu elektroapgādes tīkla mezglu, vienu telekomunikācijas tīkla mezglu un trīs ŪAT mezglus. Piedāvātais modelis ir piemērojams jebkurai no augšā aprakstītiem AMR vai AMI piemēriem. Modeļa ievades parametri ir aprakstīti 4.2 nodaļā.



4.3. att. Sistēmas modelis, kas ietver elektroapgādes, telekomunikācijas un ūdens apgādes tīkla mezglus

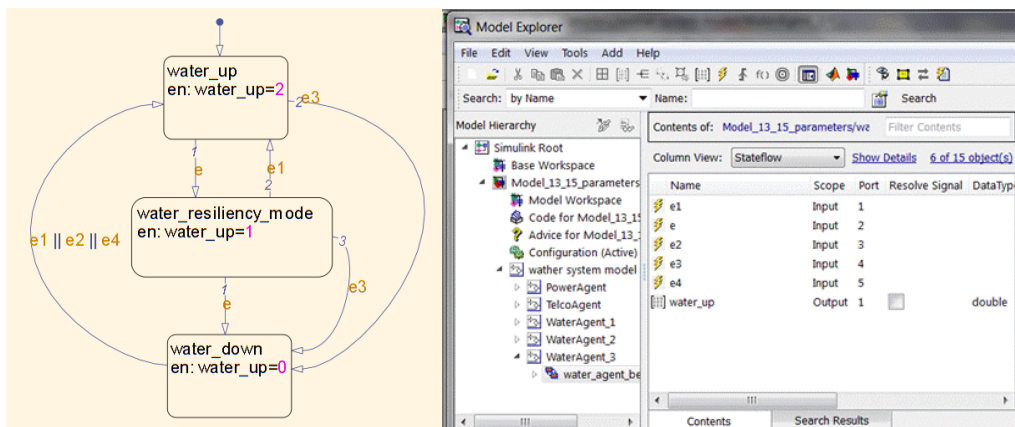
Turklāt 4.4. attēls parāda simulācijas modeļa daļu, kas attēlo ūdens mezglu darbību.



4.4. att. Simulācijas modeļa daļa, kas attēlo ūdens mezglu darbību

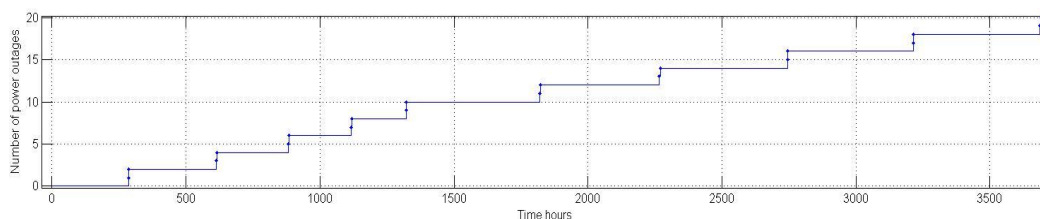
Ūdens mezgla modeļa ievadi (skat. 4.4. attēlu) tiek nodrošināti ar izejām no elektroapgādes tīkla modeļa: *Vidējais dīkstāves laiks* (“power_down”) un *Vidējais laiks starp bojājumiem* (“power_up”). Ievadi no telekomunikācijas tīkla modeļa nāk kā mezglu dīkstāves (“telco_down”) un kā mezglu darbības atjaunošanas signāli (“telco_up”). Pirmais gadījumu skaitļu ģenerators, izmantojot 4.2. nodaļā noteiktus parametrus, ģenerē RBDL, bet otrais gadījumu skaitļu ģenerators ģenerē RBNL parametrus.

„State flow chart” (SFC) uz 4.5a. attēlā pārslēdzas starp ūdens mezgla stāvokļiem: “water up”, “water node in resilience mode” (saņem barošanu no rezerves avota) un “water down”, kad ūdens mezgls nedarbojas normālā režīmā elektroapgādes vai telekomunikācijas infrastruktūras kļūmes dēļ. Attēls 4.5b. demonstrē mijiedarbību starp ievadiem, funkcijām un portiem ūdens mezgla SFC. Piemēram, ieejas signāls “e” uz portu 2, pārslēdz SFC “Resilience mode” stāvoklī, proti, uz “water_up=1”. No šāda stāvokļa SFC pārslēdz uz “water_up=2” (uz normālas darbības stāvokli), kad signāls “e1” pienāk uz portu 1, vai SFC pārslēdzas stāvoklī “water_down”, ja signāls “e3” atnāk uz portu 4.

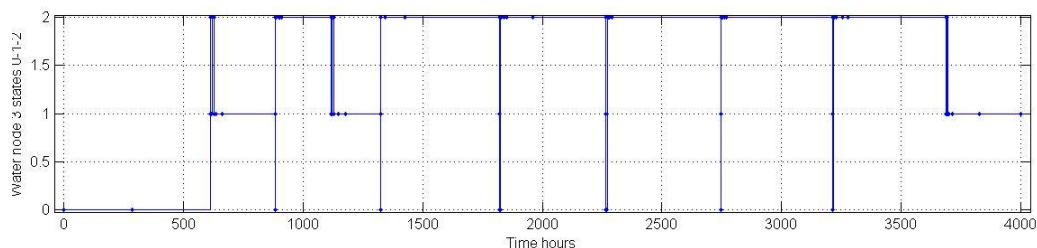


4.5. att. a) Ūdens tīkla „State Flow Chart”; b) Model Explorer, kurš demonstrē mijiedarbību starp ievadiem, funkcijām un portiem ūdens mezgla SFC

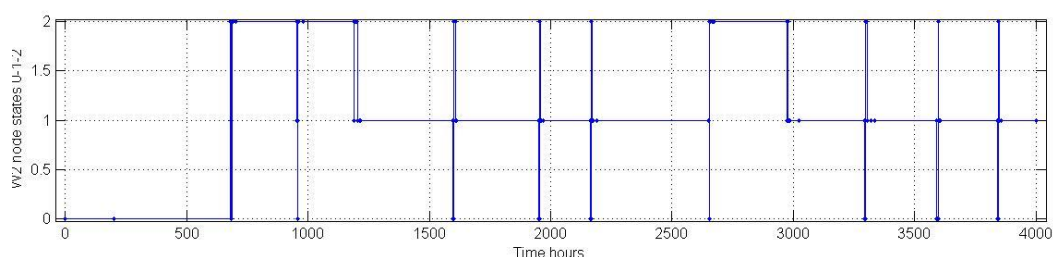
Attēls 4.6. parāda elektroapgādes mezglu dīkstāvju skaitu, savukārt attēli 4.7. un 4.8. parāda ūdens apgādes tīkla mezglu stāvokli, kur “2” nozīmē normālo darbības režīmu, “1” – mezgls nodrošina savas funkcijas, izmantojot rezerves barošanas avotu, un “0” – mezgls nefunkcionē sakarā ar elektroapgādes trūkumu, vai sakarā ar to, ka nedarbojas atbilstošais telekomunikācijas tīkla mezgls.



4.6. att. Elektroapgādes tīkla mezgla dīkstāves imitācijas laikā



4.7. att. Ūdens apgādes tīkla mezgla (W1) dīkstāves imitācijas laikā: 0-1-2



4.8. att. Ūdens apgādes tīkla mezgla (W2) dīkstāves imitācijas laikā: 0-1-2

Modeļa imitācijas rezultāti ir apkopoti 4.4. tabulā. Detalizētie imitācijas rezultāti atrodas 3. Pielikumā.

Imitācijas rezultāti norāda uz ciešo saikni starp kļūmēm elektroapgādes tīklā un dīkstāvēm ūdens sadales tīklā, jo ūdens infrastruktūras *Fiziskās atkarības koeficients*

$$FAK_{NW} = \frac{N(NW | NP)}{N(NP)} = 116/150 = 0.77$$

ŪST mezglu vidējais dīkstāves laiks 2.36 st. un elektroapgādes tīkla mezglu vidējais dīkstāves laiks 2.69 st., tāpēc laika mērogā fiziskās atkarības koeficients, citiem vārdiem *Fiziskās atkarības relatīvais ilgums*: $FRI_{NW} = \frac{T(NW)}{T(NP)} = 0.88$.

$$FRI_{NW} = \frac{T(NW)}{T(NP)} = 0.88.$$

Ja izmantot ūdensvada mezglu vidējo dīkstāves laiku, ņemot vērā elektroapgādes tīkla mezglu dīkstāvju skaitu, proti, 1.80 stundas, tad $FRI_{NW} = \frac{T(NW)}{T(NP)} = 0.67$.

4.4. tabula

Modeļa imitācijas rezultātu kopsavilkums

Imitācijas rezultāti								
Imitācijas kārtas	1	2	3	4	5	6	7	8
ŪAT mezglu rezerves barošanas avota darbības laiks (st.)	0.1	3	6	1.5	4.5	5.5	2.75	1
ŪAT mezglu rezerves barošanas avota nomainīšanas laiks (st.)	48	24	4	36	12	46	43	38
ŪAT mezglu vidējais dīkstāves laiks (st.)	2.27	2.34	1.49	1.81	2.12	2.65	2.14	1.75
Elektroapgādes tīkla mezglu vidējais dīkstāves laiks (st.)	2.34	2.34	2.34	2.55	2.55	2.55	2.49	2.49
Laika mērogā fiziskās atkarības koeficients	0.97	1.00	0.64	0.71	0.83	1.04	0.86	0.70
ŪAT mezglu vidējais dīkstāves laiks, ņemot vērā elektroapgādes tīkla mezglu dīkstāvju skaitu (st.)	2.27	1.56	0.99	1.92	1.65	1.77	1.71	1.81
Laika mērogā fiziskās atkarības koeficients, ņemot vērā elektroapgādes tīkla mezglu dīkstāvju skaitu	0.97	0.67	0.42	0.75	0.65	0.69	0.69	0.73

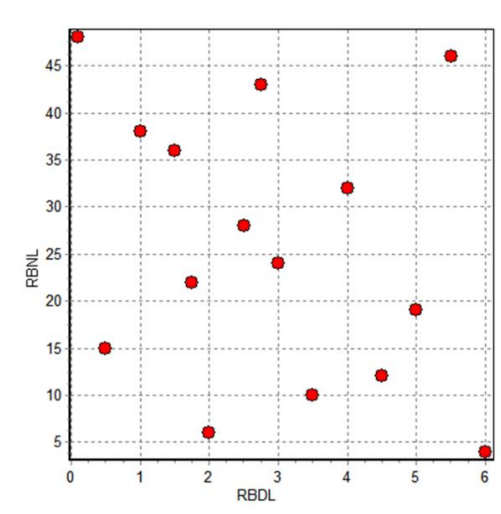
Imitācijas rezultāti									
Imitācijas kārtas	9	10	11	12	13	14	15	Vidējais kopumā	
ŪAT mezglu rezerves barošanas avota darbības laiks (st.)	4	2.5	1.75	5	0.5	3.5			
ŪAT mezglu rezerves barošanas avota nomaiņas laiks (st.)	32	28	22	19	15	10	6		
ŪAT mezglu vidējais dīkstāves laiks (st.)	2.88	3.16	1.74	3.62	2.42	2.60	2.46	2.36	
Elektroapgādes tīkla mezglu vidējais dīkstāves laiks (st.)	2.49	3.16	3.30	3.30	2.80	2.80	2.80	2.69	
Laika mērogā fiziskās atkarības koeficients	1.16	1.00	0.53	1.10	0.86	0.93	0.88	0.88	
ŪAT mezglu vidējais dīkstāves laiks, ņemot vērā elektroapgādes tīkla mezglu dīkstāvju skaitu (st.)	1.73	2.01	1.74	1.98	2.42	1.82	1.57	1.80	
Laika mērogā fiziskās atkarības koeficients, ņemot vērā elektroapgādes tīkla mezglu dīkstāvju skaitu	0.69	0.64	0.53	0.60	0.86	0.65	0.56	0.67	

Eksperimenta rezultāti demonstrē ne tikai eskalācijas efekta trūkumu, bet arī ŪST mezglu ievērojamu dīkstāvju laika samazināšanu, jo laika mērogā fiziskās atkarības koeficients, ņemot vērā elektroapgādes tīkla mezglu dīkstāvju skaitu, ir 0.67.

4.4 Eksperimenta rezultātu polinomiāla aproksimācija

Imitācijas dati tiek apkopoti ar EdaOpt eksperimentu rezultātu apstrādes rīku, kuru izstrādāja RTU pētnieki. Kopējais mēģinājumu skaits otras kārtas kompozītu plānu matricai ar d-faktoru skaitu izvēlēts pēc formulas: $n = 2^d + 2d + n_0$ pie $d < 5$ un $n = 2^{d-1} + 2d + n_0$ pie $d \Rightarrow 5$.

Eksperimentā tiek veikti 15 mēģinājumi, tas pārsniedz nepieciešamu minimālo mēģinājumu skaitu, kas ir 9. Mēģinājumu koordinātes pārklāj vienmērīgi eksperimenta lauku (skat. 4.9. att.).



4.9. att. Eksperimenta plāna 2 D projekcija

Tiek analizēta ūdens apgādes tīkla mezglu vidēja dīkstāves laika (ŪMDL) rādītāja atkarība no rezerves barošanas avota darbības laika (RBDL) un rezerves barošanas avota nomainīšanas laika (RBNL) rādītāju savstarpējas korelācijas noteikto parametru robežās. Analīzei tiek izmantots pielāgotais ŪMDL, kurš ir pārrēķināts, ņemot vērā elektroapgādes tīkla mezglu dīkstāvju skaitu.

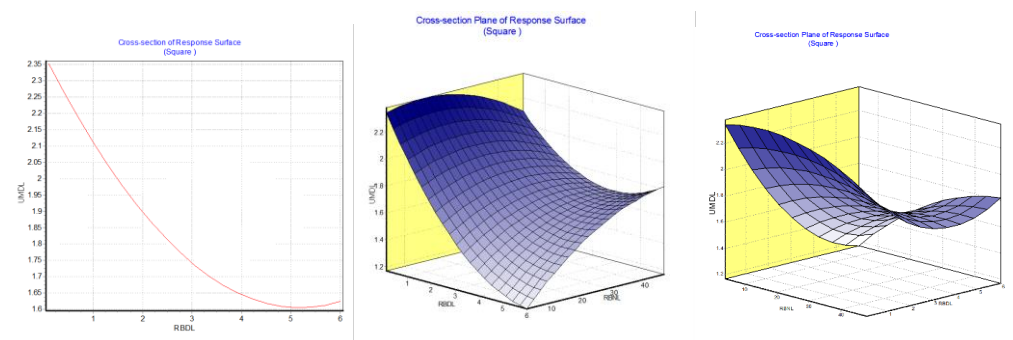
Tika veikta rezultātu aproksimācijas: lineāra, kvadrātiskā un kubiskā. Pēc kārtas tiek atmesti mēģinājumi, atzīmētus ar „Bad point number”, kuros ir maksimālais „Rel error”. Labākus rezultātus nodrošināja kvadrātiskā aproksimācija, bet sliktākus kubiskā aproksimācija, jo Sigma Cross, Sigma cross%, Sigma, Sigma% ir labāki kvadrātiskai aproksimācijai (skat. 4.5. tabula).

4.5. tabula

Ekspierimentu datu kvadrātiskā aproksimācija

	Bez punktu izslēgšanas	Ar viena punkta izslēgšanu (12)	Ar divu punktu izslēgšanu (12, 14)
Sigma Cross	0.438762	0.437805	0.431625
Sigma Cross%	139.118474%	138.695410%	133.680008%
Sigma	0.195635	0.195765	0.175157
Sigma %	62.030159	62.017881	54.248318
Sigma 0	0.252564	0.252732	0.231711
Sigma 0%	80.080591	80.064740	71.763779
MeanExpValue	1.794640	1.795607	1.782679
Max error	0.315387	0.315660	0.322879
Bad point number	1.422500	1.422500	1.422500
Max rel error	0.315212	0.314782	0.294118
BadRelPoint No	12	12	14

4.10. attēla var redzēt divu un trīs dimensiju attēlus, kas demonstrē korelācijas starp ūdens apgādes tīkla mezglu RBDL, RBNL un ūdensvada mezglu vidējo dīkstāves laiku ŪMDL.



4.10. att. Kvadrātiskā aproksimācija ar viena punkta izslēgšanu

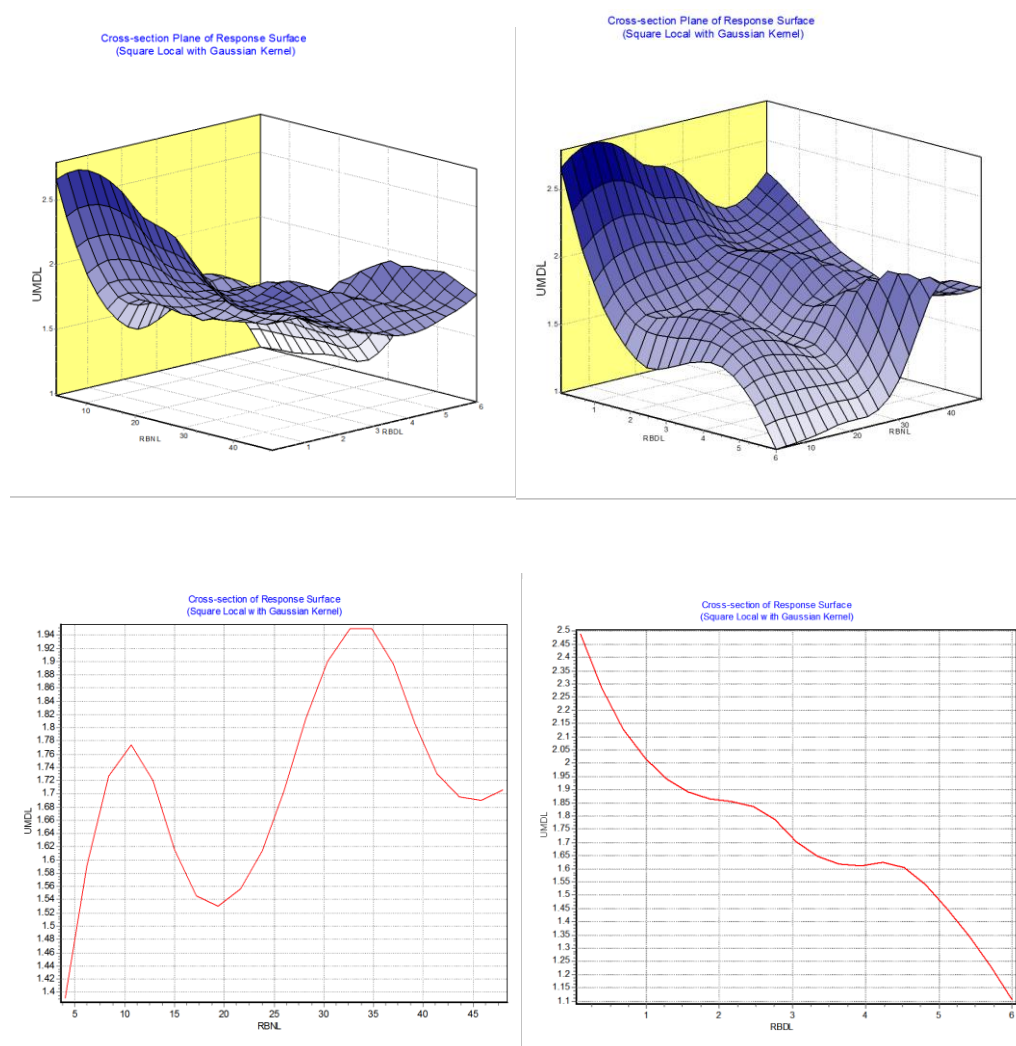
Ar EdaOpt palīdzību tiek izrēķināti polinoma koeficienti kvadrātiskai aproksimācijai ar viena mēģinājuma izslēgšanu. Rezultāta ir šāds polinoms:

$$R = 2.3532 - 0.3894 * X_1 + 0.00812 * X_2 + 0.0289 * X_1 * X_1 + 0.0035 * X_1 * X_2$$

Savukārt kvadrātiskai aproksimācija ar divu mēģinājumu izslēgšanu deva šādu polinomu
 $R = 2.2919 - 0.4901 * X_1 + 0.0201 * X_2 + 0.0448 * X_1 * X_1 + 0.0037 * X_1 * X_2$

Tomēr turpmākai eksperimenta rezultātu analīzei tiek izmantots polinoms ar viena mēģinājuma izslēgšanu, jo, ieliekot tajā izmēģinājumu datus, kalkulācijas rezultāti ir tuvāk eksperimenta rezultātiem.

Turpmāk tiek veikta lokāla aproksimācija ar mērķi konstatēt iespējamo lokālos minimumus. Aplūkojot 4.11. att., var redzēt vismaz divus lokālus minimumus.



4.11. att. Lokāla kvadrātiskā aproksimācija ar viena punkta izslēgšanu

4.5 Secinājumi par ceturto nodaļu

Ūdensvada mezglu vidējais dīkstāves laiks, kurš ir aprēķināts, ņemot vērā elektroapgādes tīkla mezglu dīkstāvju skaitu, demonstrē atkarību no rezerves barošanas avota darbības laika un rezerves barošanas avota nomainīšanas laika savstarpējas korelācijas noteikto parametru robežās, proti:

- Polinoma koeficienti norāda, ka X_1 parametri (RBDL) lielāka mērā ietekmē ŪMDL ne kā X_2 (RBNL) parametri, tomēr X_2 parametru ietekmi nedrīkst izslēgt, ņemot vērā, ka parametru vērtības pārklājas eksperimenta laika skalā;
- Lai gan aproksimācijas grafiki rāda, ka izpētītu parametru robežās polinomiāla funkcija tiecas uz minimumu tad, kad RBDL tiecas uz maksimumu, tomēr analīze atklāj arī funkcijas lokālus minimumus, kas ir saistīti ar telekomunikācijas tīkla mezglu noturību pret ārējas elektroapgādes pārtraukumiem.
- Eksperimenta rezultātu analīze rāda, ka tipveidīgo rezerves elektrobarošanas avotu izmantošana ūdensvada tīkla mezglos, proti, vārtējās – koncentratoros, ir efektīvs risinājums, ņemot vērā samērīgas izmaksas, tomēr tas nav pietiekošs, lai nodrošinātu nepārtrauktu un drošu datu savākšanu no objektiem, jo fiziskās atkarības koeficients ir 0.77, bet laika mērogā fiziskās atkarības koeficients ir 0.67.
- Kā risinājumi, kas nodrošinātu nepārtrauktu un drošu datu savākšanu no ūdensvada tīkla objektiem, var būt:
 - ✓ Rezerves barošanas avota darbības laika palielināšana;
 - ✓ Papildus tīkla mezglu izmantošana („Redundant Advanced Metering Infrastructure”), šādā veidā palielinot sensoru tīkla robustumu (skat. šī darba 2.1. nodaļu, kur ir aprakstīts tīkla topoloģiskais robustums).

Rezerves barošanas avotu darbības laika un to nomaiņas laika optimizācija var būt nākotnes pētījuma temats. Projektējot sensoru tīklus, kas uzrauga un pārraida datus no ūdensvada tīkliem, jāņem vērā arī tāds faktors kā ekspluatācijas izmaksas ar mērķi atrast bilanci starp nepieciešamajiem resursiem, lai atjaunotu rezerves barošanas avotus, un izmaksām, kas ir nepieciešamas, lai nodrošinātu nepārtrauktu rezerves barošanu tīkla mezgliem.

5. KRITISKAS INFRASTRUKTŪRAS DATORVADĪBAS METODES, PIELIETOJOT BEZVADU SENSORU TĪKLUS

Pēdējos gados Latvijā, Lietuvā un Igaunijā tiek realizēti vairāki projekti, kuros tiek izmēģināti dažādi automatizētas datu nolasīšanas sistēmas risinājumi, piemēram, Ventspilī, Talsos, Tukumā, Jelgavā, Aizkrauklē, Rīgā, Utenā, Haapsalā u.t.t., kas demonstrēja labus rezultātus. Tomēr pašvaldību uzņēmumi un kompānijas, kas realizē projektus, sastopas ar nopietnām problēmām: risinājumu neadekvātas izmaksas, aparatūras nestabila darbība, palielinātas ekspluatācijas izmaksas. Jaunu tehnisko risinājumu ieviešanu kavē arī speciālistu trūkums komunālās saimniecības uzņēmumos, laboratorijas iekārtu un attiecīgu kompetenču trūkums pētniekiem.

Šajā nodaļā pētījuma autors analizē problēmas, ar kurām sastopas tehniskie speciālisti un pētnieki, kas ievieš praksē kritisko infrastruktūru datorvadības pārvaldības metodes, pielietojot bezvadu sensoru tīklus, un apraksta tehniskus risinājumus, kuri tiek izstrādāti apskatītos projektos.

Autors piedalījās projektos “Talsu novada datorizētas ūdenssaimniecības vadības kontroles sistēmas paplašināšana” [59], testējot izstrādātu sistēmu 2009-2010. gadā. Projektā “Kuldīgas novada komunālo pakalpojumu pārvaldes sistēmas priekšizpēte un modeļa izstrāde, izmantojot informācijas un komunikāciju tehnoloģiju (IKT) risinājumus” [86] autors bija projekta vadītājs, pētījuma un izstrādātā modeļa līdzautors 2009-2010. gadā. Autors sagatavoja projekta pieteikumu, bija projekta koordinators un pētījumu līdzautors projektā “Innovative e-services for water supply management (E-Water)” 2010-2012. gadā [57]. Šā pētījuma autors bija viens no projekta idejas iniciatoriem, projekta pieteikuma sagatavotājs un projekta zinātniskais vadītājs projektā “Smart Metering” 2012-2013. gadā [88].

Pēdējos gados „Service Oriented Architecture” SOA (uz pakalpojumiem orientēta tehnoloģija) tika izmantota ar labiem panākumiem lielās, izplatītās programmatūras sistēmās, ar „business-to-business” mijiedarbību, jo iekārtu integrācijas joma kļūst arvien svarīga. SOA „idejas” pārņemšana uz ierīces līmeni izskatās kā daudzsološa pieeja, lai piesaistītu visuresošās viedo ierīces un radītu jaunas sinerģijas starp programmatūras sistēmām un iegultajām ierīcēm [75]. SOA, piemēram, ir spējīga nodrošināt sadarbības funkcijas starp siltumenerģijas apgādes sistēmām un sistēmām, kas nodrošina komfortu ēkās – ventilācija, siltumsūkni u.t.t. Šāda pieeja nodrošina vienlaicīgi gan izmaksu ietaupījumu, gan iekšējo komfortu.

Tomēr SOA pielietošana ierīcēs ar ierobežotiem resursiem, tādiem kā bezvadu tīklu sensoru mezgli, vēl joprojām ir pētījumu problēma, pateicoties neatrisinātiem jautājumiem [1, 67]:

- Protokolu nesaderība, kurus izmanto dažādi mēraparatūras ražotāji, jo tie ir pārsvarā „appropriate” protokoli;
- Zems datu pārraides ātrums no bezvadu sensoru mezgliem līdz koncentratoriem;
- Bezvadu sensoru mezglu ierobežotas datu apstrādes spējas;
- Sensoru mezglu maza atmiņa, kas ierobežo XML shēmu izmantošanu, jo tās prasa daudz lielāku atmiņu;
- Ierobežota akumulatora jauda.

Iepriekš minētie ierobežojumus var atrisināt, izmantojot divas pieejas. Pirmā pieeja saziņai ar sensoru tīkliem paredz izmantot starpprogrammatūru vārteju ierīcēs. Otrā pieeja paredz nodrošināt savietojamu, izmantojot „Simple Object Access Protocol” (SOAP) vai „Constrained Application Protocol” (CoAP), pielietojot Web servissus uz bezvadu sensoru mezgliem, neizmantojot vārtejas [6, 25, 37].

Pētniecības centieni vairākums tiek vērsts uz starpprogrammatūras izmantošanu, kas darbojas uz jaudīgākām ierīcēm vai vārtejām [43]. Šādas starpprogrammatūras uzdevums ir sensoru tīkla funkcionalitātes realizācija, izmantojot standarta SOA tehnoloģiju.

Tādā veidā saziņai sensoru tīkla ietvaros joprojām var izmantot specializētus, “slēgtus” protokolus, tomēr šāds pakalpojumu modelis tika vienkāršots, lai gan nav standartizēts. Lai izvairītos no resursu ietilpīgām operācijām, veiktām uz sensoru mezgliem, starpprogrammatūra, kas izvietota uz vārtejas ierīcēm, vispirms sazinās ar mezgliem „ad hoc” veidā, un pēc tam tulko to funkcionalitāti kā interneta pakalpojumus ārējām sistēmām. Šāda dizaina piemērs tiek aprakstīts Aviles-Lopez et al. darbā [1].

Šīs pieejas priekšrocība ir tāda, ka ļauj resursu ietilpīgus uzdevumus, saistītus ar standarta pakalpojumu izpildīšanu, veikt uz vārtejām, tomēr tai ir arī daži trūkumi, piemēram, komunikācijas joslas platuma ierobežojumi, datu apstrādes spējas, un ierobežotas spējas atbalstīt neviendabīgumu mezglu līmenī.

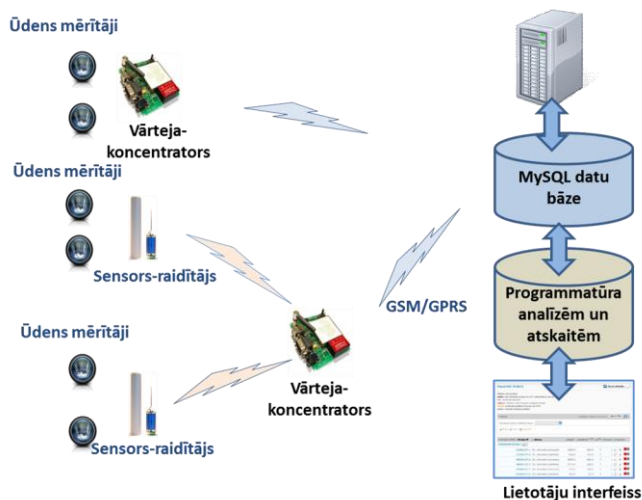
Turpmāk aprakstītajos risinājumos tiek izmantotas starpprogrammatūras, kas darbojas uz vārtejām.

5.1. Talsu novada datorizētas ūdenssaimniecības vadības kontroles sistēmas apraksts

Saskaņā ar projekta uzdevumu „Talsu novada datorizētas ūdenssaimniecības vadības kontroles sistēmas paplašināšana - piegāde un uzstādīšana” līdz 2011. gada beigām tika uzstādīti 347 ūdens patēriņa mērītāji, 19 ūdens spiediena mērītāji un mērīšanas datu lasīšanas un pārraidīšanas iekārtas. Serveri un programmatūra, kas veica tīkla uzraudzību, mērījumu datu analīzi un atskaišu sniegšanu, tika uzstādīta Talsu Ūdens (TW) telpās. Viens no projekta

uzdevumiem paredzēja izstrādāt risinājumu, lai vismaz daļēji automatizētu rēķinu par ūdens patēriņu sagatavošanu, tāpēc tika izmēģināts risinājums saskarnei starp esošo grāmatvedības sistēmu Horizon un mērījumu datu bāzi.

Talsu novada datorizētas ūdenssaimniecības vadības un kontroles sistēmas tehnisko risinājumu [59] var apskatīt 5.1. attēlā.



5.1. att. Tehniskā risinājuma blokshēma (Zabašta [85])

Kontroles sistēma izmanto šādus risinājumus:

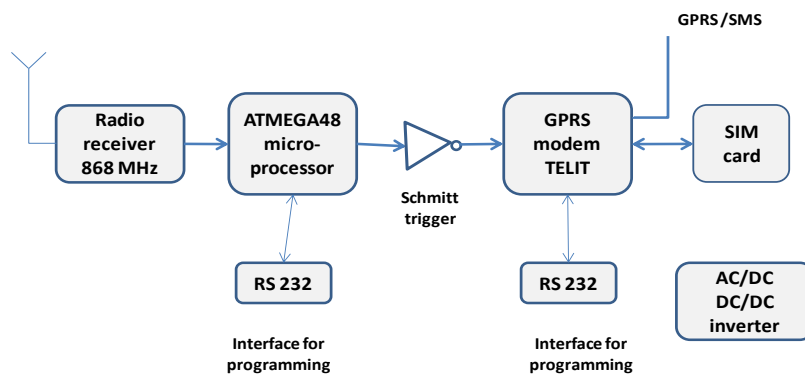
- Ūdens plūsmas un ūdens spiediena mērītāji ar impulsu izejām nodrošina datus uz sensoriem - raidītājiem. Tie ir aprīkoti ar piederumu ("herkons"), kas pārveido magnētiskus signālus par elektriskiem impulsiem;
- Datu pārraide no sensoriem uz vārtejām - koncentratoriem tiek veikta, izmantojot „Short Range Devices” (SRD) nelicencētu telemetrijas joslu 868 MHz;
- GSM tīkls (GPRS) tiek izmantots datu pārraidei starp vārtejām - koncentratoriem un serveri;
- MySQL datu bāze tiek izmantota mērīšanas datu uzglabāšanai un apstrādei;
- Sistēmas lietotāju piekļuve datu bāzei tiek īstenota, izmantojot Web interfeisu.

Šāds risinājums nodrošina šādas priekšrocības:

- Centrālo serveri var izvietot jebkurā Latvijas vai ārzemju datu centrā, kur ir pieejams interneta pieslēgums;
- Izvēlēties jebkuru pieejamo GSM tīkla operatoru vai vairākus operatorus vienlaicīgi;
- Izmantot esošos mobilo operatoru tīklus un neveikt investīcijas telekomunikācijas tīkla attīstībā;

- Izmantot konkurences priekšrocības starp tīkla operatoriem, izvēloties vislabākās cenas un pakalpojumus;
- Attīstīt vadības un kontroles sistēmu un pievienot jaunus klientus bez lieliem kapitāliem ieguldījumiem;

Vārteja – koncentrators, attēlotais 5.2. att. periodiski saņem mērījumu datus, kas tiek nosūtīti no ūdens plūsmas un ūdens spiediena mērītājiem un pārraida tos uz serveri.



5.2. att. Vārtejas – koncentrators blokshēma (Talsi)

Vārtejas - koncentratoru galvenie elementi:

- Mikrokontroleris (Atmel), kas kontrolē uztvērēju un visu koncentratoru. Tā ir arī uzglabāšanas vieta uzskaites datiem, kas iegūti no pakļautiem sensoriem.
- Uztvērējs, kas izmanto Short Range Devices (SRD) nelicencētu telemetrijas joslu, 868–870 MHz;
- TELIT GSM modems GM862 (vai vēlākas modifikācijas) datu pārraidei. Tajā ir visi vajadzīgie elementi, lai īstenotu GPRS modema funkcijas. Modemam ir iekšējais procesors un atmiņa, lai veiktu programmēšanu Python valodā.

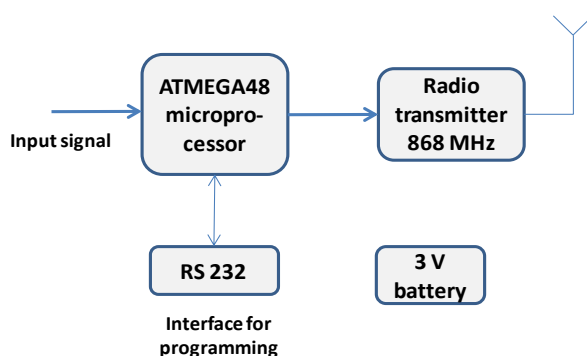
Projektā ir izmantotas divu tipu vārtejas - koncentratori:

- Pirmais tips - apkopo datus no sensoriem – raidītājiem, kurus uzstāda blakus plūsmas vai spiediena mērītājiem pie klientiem. Šādam koncentratoram ir ne tikai GSM modems, bet arī uztvērējs, lai saņemtu datus no pakļautiem sensoriem.
- Otrā tipa vārtejas - koncentratori tiek uzstādīti tieši objektos kopā ar mērītājiem. Koncentratoram ir divas ieejas: viena signālu saņemšanai no ūdens plūsmas un otra - no ūdens spiediena mērītājiem.

Sensora - raidītāja galvenā funkcija ir saņemt impulsus no skaitītāja, pārveidot tos ziņojumos un pārraidīt ar noteikto periodiskumu uz piesaistītu koncentratoru.

Sensora - raidītāja blokshēma (skat. 5.3. att.) sastāv no šādiem moduļiem:

- ATMEGA48/88 mikroprocesors, kas saņem impulsus no plūsmas un spiediena mērītājiem, pārveido ziņojumā (par „telegrammu”) un nodod tos raidītājam. Mikroprocesors ir savienots ar mērītāju ar vadu ķēdi. Tas uztver herkona releja stāvokļa izmaiņas (impulsus) un reģistrē tos savā atmiņā.
- Mikroprocesors izmanto "C" valodā rakstītu programmu. Pielāgotais lokālām vajadzībām Wireless M-Bus protokols tiek izmantots, lai izveidotu radio saiti.
- Raidītājs RFM22, kas pārraida telegrammas uz koncentratoru, izmanto 868 MHz frekvenci.
- Barošanas moduli nodrošina 3 V baterija, kuras darbības laiks ir aprēķināts apmēram uz 6–10 gadiem.



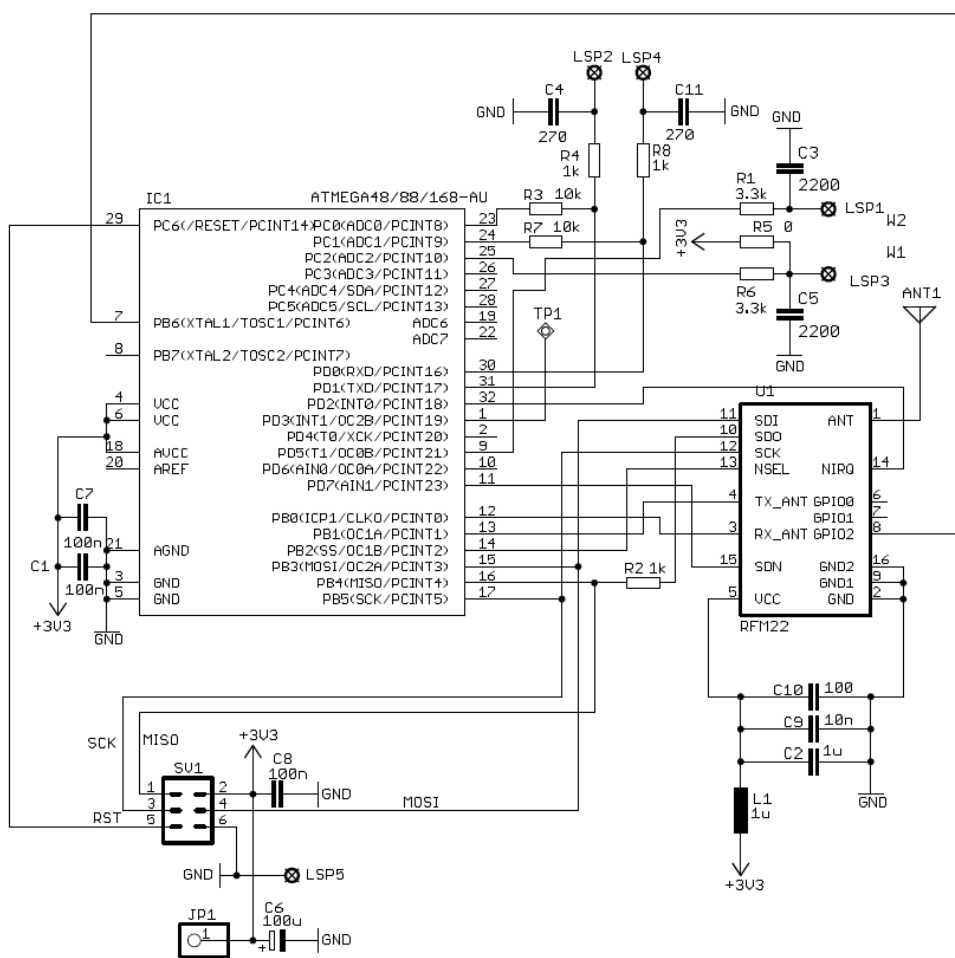
5.3. att. Sensora - raidītāja blokshēma [85]

Attēlā 5.4. var redzēt sensoru – raidītāju ICR ar 3 V bateriju, kas atrodas starp augšējo un apakšējo plati.



5.4. att. Sensora - raidītāja ārējais izskats

Savukārt 5.5. attēlā ir parādīta sensora – raidītāja ICR augšējās plātes (RR42) elektriskā shēma.



1. RFM22 vieta likt RFM42.
2. Zem RFM42 likt planu izolāciju.
3. Rezistoru R5 nemontēt.

Att. 5.5. Sensora – raidītāja ICR augšējās plates (RR42) elektriskā shēma

5.2. Rīgas Siltums pilot-projekta sistēmas apraksts

Starpprogrammatūra uz vārtejas ierīcēm tika demonstrēta praksē, kad Rīgas Siltums un Micro Dators veica kopīgu izmēģinājuma projektu, kura mērķis bija uzstādīt bezvadu siltuma skaitītāju nolasīšanas ierīces 28 siltumapgādes apakšstacijās. Mērījumu dati no siltuma skaitītājiem tika pārraidīti uz sistēmas serveri vairākas reizes stundā atbilstoši noteiktajam grafikam, kā arī pēc attiecīgā pieprasījuma saņemšanas. Izmēģinājuma projekta objekti tika atlasīti vissarežģītākajās vietās Rīgā: apkures apakšstacijās, kas tika izvietotas Vecrīgas pagrabos [5].

Tika mērīti un apstrādāti šādi parametri:

Q = Enerģijas apjoms (MWh)

V = Ūdens apjoms (m³)

T_1 = Tekoša temperatūra (ievados) (*C)

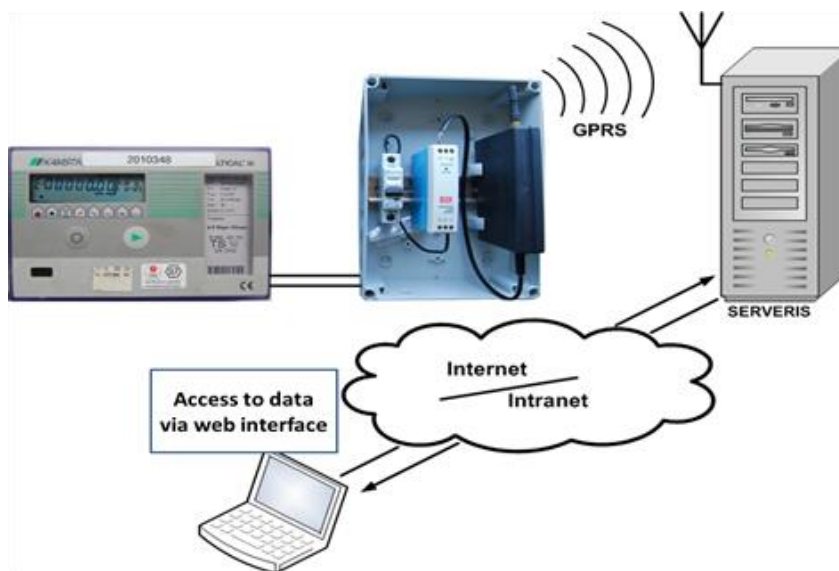
T_2 = Tekoša temperatūra (izejoša) (*C)

$T_1_T_2$ = temperatūras starpība (*C)

P = Tekoša jauda (MW)

F = Mērītais apjoms (m³/h)

Automatizētas siltuma mērītāju vadības un kontroles sistēmas blokshēma ir parādīta attēlā 5.6.



Att. 5.6. Vadības un kontroles sistēmas blokshēma

Visi 28 siltummezgli tika aprīkoti ar Kamstrup Multical mērītājiem, kas nodrošināja saziņu ar ārējām iekārtām, izmantojot Multical protokolu loģiskā līmenī, un RS232 M-Bus pieslēgumu fiziskā līmenī.

Projektā izmantoja otrā tipa vārtejas – koncentratorus, kurus uzstādīja kopā ar Multical mērītājiem. Vārtejas ierīces TB3 tika pieslēgtas pie 220V sprieguma, kā rezultātā ierīces ir spējīgas izmantot pilnu GSM modemu kapacitāti, lai nodrošinātu savienojumu ar serveri. Multical mērītājiem savukārt ir nodrošināta rezerves barošana no baterijas ar paredzamo baterijas darbības laiku līdz 8 gadiem. Tomēr testi, kas veikti izmēģinājuma projekta laikā, atklāja, ka bieža datu vākšana, piemēram, viens pieprasījums ik 60 sekundes, saīsina baterijas darbības laiku apmēram līdz 3 - 6 mēnešiem. Šis aspekts ir jāņem vērā, projektējot automātisko siltuma skaitītāju datu vākšanas sistēmu siltumapgādes tīkliem.

Izmēģinājuma projekta vajadzībām, tika izmantoti OS Gentoo Linux sistēmas serveris un 5,0 MySQL datu bāze. Mērījumu dati tika pārsūtīti uz serveri šādā veidā: mērījumu nolasīšanas ierīce TB3 periodiski nosūta datu vākšanas pieprasījumus uz Multical, ierakstot datus savā

atmiņā kā mazus failus ar laika zīmogu, kuri pēc tam tiek augšupielādēti uz serveri un tālāk sakārtoti datu bāze saskaņā ar laika zīmoga piezīmēm.

Lai nodrošinātu vārteju komunikāciju elektroenerģijas pārtraukumos, dažas TB3 ierīces tika apgādātas ar rezerves baterijām. Tātad gandrīz visi mērījumu dati sasniedz datu bāzi, neatkarīgi no GSM tīkla traucējumiem vai maiņstrāvas elektroenerģijas padeves pārtraukumiem uz vārtejas ierīcēm.

5.2.1. Risinātie problēmjaucējumi

AMR sniegums tiek raksturots vismaz ar diviem parametriem: pirmkārt, cik ilgi darbojas sistēma bez rezerves avotu nomaiņas, un otrs, sensoru tīkla caurlaidspēja, vai citiem vārdiem, cik liels mērījumu datu procents tiek reģistrēts sistēmas datu bāzē.

Lai nodrošinātu ūdens AMR sistēmas ultrazemu enerģijas patēriņu un ilgu darbības laiku, ir nepieciešams panākt visu sensoru un tīkla mezglu precīzu sinhronizāciju. Tīkla pilnīga pamošanās ir obligāts priekšnosacījums: ja daži tīkla mezgli paliek neaktīvi, tad papildus informācijas zudumiem "mirušu" mezglu dēļ, tiek pazaudēti dati no mērītājiem, tāpēc, ka pietrūkst derīgo ceļu līdz vārtejām - koncentratoriem.

Sensoru tīkla mezgli iziet no ierindas, ne tikai barošanas avotu dēļ, bet arī sakarā ar fiziskiem bojājumiem un vides traucējumiem. Atsevišķu mezglu dīkstāves nedrīkst ietekmēt sensoru tīkla kopējo funkcionalitāti. Sensoru tīkla spēju saglabāt savu funkcionalitāti, kad atsevišķie mezgli nefunkcionē, sauc par bojājumu toleranci [44]. Atsevišķo mezglu bojājumi var izraisīt ievērojamas tīkla topoloģijas izmaiņas, kas prasītu tīkla rekonfigurāciju un ziņojumu pakešu pāradresāciju. Turklāt pastāv risks, ka liels mezglu skaits vienlaikus nosūta un saņem ziņojumus. Tas var radīt nepieņemamu ziņojumu sadursmi un veicināt atkārtoto retranslāciju apjomu, tādējādi pārplūdinot un piesātinot tīklu, kā rezultātā būtiski samazinot saņemto ziņojumu likmi.

Inženieri un pētnieki, kas īstenoja Talsu projektu, ņēma vērā pašvaldības prasības par aparatūras izmaksām, kuras nedrīkstēja pārsniegt 30-35 EUR uz vienu sensoru - raidītāju. Bija arī ņemtas vērā iespējamās klientu manipulācijas ar individuāliem ūdens skaitītājiem, tāpēc tika izstrādāta papildus programma, kas reģistrēja bojājumus vados, kas savienoja ūdensmērītāju un sensoru - raidītāju.

5.2.2. Datu pārraide

Lai samazinātu kopējās sistēmas izmaksas, sensoriem ir tikai divi darba režīmi: ūdens mērītāji impulsu reģistrācija un ziņojumu (telegrammu) nosūtīšana vārtejām vairākas reizes stundā, tādēļ stingra sinhronizācija sensoru tīklā netika neizmantoja. Ziņojumu sadursmes

varbūtība ir novērtēta aptuveni 1:10 000. Ir novēroti tikai daži gadījumi, bet nav bijis iespējams tos precīzi novērtēt.

Talsu Ūdens un Rīgas situms projektos tiek izmantoti līdzīgie risinājumi: viens mērītāja ziņojums (telegramma) 24 baitu lielumā (skat. 5.1. tabulu). Vārteja – koncentrators saņemtos ziņojumus pārveido http formātā un sūta, izmantojot TCP/IP protokolu. Vienas sesijas datu apjoms sastāda ap 6 Kbt, līdz ar to vienas vārtejas mēneša trafiks var sasniegt kritisku robežu 10 Mbt, pēc kuras GSM operatori pielieto soda sankcijas.

Lai samazinātu datu apjomu, kas tiek sūtīts no vārtejām - koncentratoriem uz serveri un pretējā virzienā, datu failos tiek izmantoti teksta saīsinājumi un teksta abreviatūra, turklāt faili ir sadalīti īsākos ziņojumos, piemērojot Md5 summu, lai pārbaudītu failu integritāti. Tādēļ, ja daži no ziņojumiem ir sakropļoti, tikai daļa no faila jānosūta atkārtoti. Talsu Ūdens eksperti piekrita palielināt laiku starp ziņojumiem līdz 10 minūtēm no ūdens spieduma mērītājiem un līdz 30 minūtēm no ūdens plūsmas mērītājiem, kas ir uzskatīts par nepieciešamu priekšnosacījumu rezerves bateriju dzīves cikla pagarināšanai, jo tas nav pretrunā ar pakalpojumu kvalitāti, par ko vienojās projekta partneri.

5.1. Tabula

Ziņojumu formāti

Atmiņas rinda	kods	Formāts
0	0x68	start (telegrammas sākums)
1	18	length (datu apgabala garums)
2	18	length (datu apgabala garums)
3	0x68	start
4	8	datu virziens
5	0..255	Count primAddr (primārā adrese)
6	0x72	funkcija
7	0..255	SecAddr 0.baits (kopā sekundārā adrese/seriālais numurs)
8	0..255	SecAddr 1.baits (kopā sekundārā adrese/seriālais numurs)
9	0..255	SecAddr 2.baits (kopā sekundārā adrese/seriālais numurs)
10	0..255	SecAddr 3.baits (kopā sekundārā adrese/seriālais numurs)
11	0xAC	Ražotājs low byte (kopā ražotājs)
12	0x48	Ražotājs high byte (kopā ražotājs)
13	0..255	Iekārtas (Device) versija
14		medium (mbus kods pēc klasif)
15		impValue (multiplikators)
16	0..99	waterCountL (impulsu skaits nepastāvīgā atmiņā)
17	0..255	waterCountRAM

18	0..255	waterCountRAM
19	0..59	minu (vārtejas pulksteņa minūtes)
20	0..23	ho (vārtejas pulksteņa stundas)
21	0..255	statusCount (min. no baterijas ar (nometās uz 0 pāri 256. t.i. 256 minūte būs atkal 0))
22	0xXX	Checksum
23	0x16	stop

Nākamais faktors, kas ietekmē AMR sniegumu, ir GSM tīkla drošums, ko izmanto datu pārraidei starp vārtejām un centrālo serveri. Lai gan GSM LMT un TELE 2 tīkli Talsu rajonā pārklāj 100% teritorijas un nodrošina tīkla pieejamību gandrīz 99.9% (TELE 2 dati), tomēr ziņojumu kavēšana un mezglu nepieejamība Talsu ARM notiek regulāri. Tam par iemeslu ir GSM tīkla pārslodze un GPRS zemāka prioritāte, salīdzinot ar balss un SMS savienojumiem.

5.2.3. Rezerves barošana

Bezvada tīkla sensora punkts kā elektronikas ierīce bieži vien tiek aprīkots ar ierobežoto barošanas avotu (≤ 0.5 Ah, 1.2-3 V). Barošanas avotu nomaiņa bieži vien nav viegls uzdevums, vai izmaksā neadekvāti dārgi, tāpēc zems enerģijas patēriņš sensoru tīklos ir nopietna problēma.

Jaudas patēriņš var sastāvēt no trijiem cikliem: *mērījumu veikšana, komunikācija ar citiem punktiem vai koncentratoriem un datu apstrāde.*

Formula (5.1) apraksta raidīšanas uztveršanas patērēto [67].

$$P_c = N_T [P_T(T_{on} + T_{st}) + P_{out}(T_{on})] + N_R [P_R(R_{on} + R_{st})] \quad (5.1)$$

$P_{T/R}$ - jauda, ko patērē raidītājs / uztvērējs;

P_{out} - raidītāja izejas jauda;

T / R_{on} - raidītāja / uztvērēja darbības laiks;

T / R_{st} - raidītāja / uztvērēja darba uzsākšanas laiks;

$N_{T/R}$ - raidītāja / uztvērēja ieslēgšanas skaits noteikta laika periodā, kurš ir atkarīgs no uzdotām funkcijām un no izmantotas MAC (Medium Access Control) shēmas.

Samazinot raidīto pakešu garumu, samazinās signāla pārraides laiks, līdz ar to ierīču ieslēgšanas momentā patērēta jauda kļūst ievērojamāka salīdzinājumā ar kopējo patērēto jaudu. Šādā situācijā raidītāja – uztvērēja izslēgšana signāla pauzēs var kļūt neefektīva jaudas dēļ, kuru patērē ieslēgšanas laikā.

Raidīšanas laikā patērētai jaudai papildus jāņem vērā datu apstrādes procesā patērēta enerģija. Lai sensora punkts pildītu signālu uztveršanas funkcijas, mikroprocesoram jābūt gatavam reģistrēt signālus. Tradicionāliem mikroprocesoriem, kas pielieto CMOS tehnoloģiju, ir visai ierobežota energoefektivitāte, jo tie pastāvīgi patērē jaudu, kamēr ir ieslēgti. Šī jauda ir

proporcionāla ieslēgšanas biežumam, ierīces kapacitātei un sprieguma svārstībām. Daži autori iesaka samazināt procesora ieslēgšanas biežumu atkarībā no darba procesu vajadzībām. Piemēram, darba [67] autori piedāvā izmantot noslodzes prognozēšanas shēmu, kas balstās uz iepriekšējas noslodzes analīzes.

Enerģijas patēriņš **datu apstrādes procesā** var būt aprēķināts pēc šādas formulas:

$$P_p = CV_{dd}^2 f \quad (5.2)$$

V_{dd} - sprieguma svārstības („swing”);

C – ierīces kapacitāte;

f – ieslēgšanas biežums.

Bezvada sensoru ierīce (ICR), ko izstrādāja „Micro dators” Talsu projektā, ilustrē baterijas darbības laiku. Izmantojot formulu (5.1), var pieņemt, ka vidēja kopēja strāva, ko patērē ICR stundas, laikā ir:

$$I_{ks} = I_{ps} + I_{ts} = I_{ps} + NT_{Ton} \quad (5.3)$$

I_{ps} – procesora strāva;

I_{ts} – raidītāja strāva;

NT – raidītāja ieslēgšanas skaits noteikta laika periodā (mūsu gadījumā vienas stundas laikā)

Ņemot vērā, ka mikroprocesors ir ieslēgts pastāvīgi, raidītāja ieslēgšanas biežums tiek noregulēts 2-6 reizes stundā, raidīšanas laiks 20 - 50 msec, starp sesijām raidītājs ir izslēgts, bet uztvērēja ICR nav, tad ieliekot konkrētus strāvas lielumus, saņemam:

$$I_{ks} = 0,040 \text{ mA} + 6 \cdot 80 \text{ mA} \cdot 0,050 \text{ s} / 3600 \text{ s} = 0,046 \text{ mA}$$

Pieņemot, ka bezvada sensoru ierīcē tiek izmantota baterija ar kapacitāti 7500 mAh, tad $T_{bater.} =$

$$C_{bater} / I_{ks} = 7500 / 24 \text{ st} / 365 \text{ dienas} = 18,6 \text{ gadi}$$

Šādā teorētiskā aprēķinā netika ņemta vērā baterijas novecošana un vides faktoru ietekme uz bezvada sensoru ierīci, kas var ievērojami samazināt baterijas darbības laiku.

5.2.4. *Mērījumu datu integrācijas ar esošām IT sistēmām*

Viens no Talsu Ūdens projekta uzdevumiem bija atrast iespēju jaunas sistēmas mērījumus saintegrēt ar esošām Talsu Ūdens IT sistēmām: grāmatvedības, klientu norēķinu, nekustamo īpašumu apsaimniekošanas un u.c. Šim mērķim tika izmēģināta XML pieprasījumu sūtīšana, kas nodemonstrēja jaunās un vecās sistēmas integrācijas iespējas. Tomēr laika trūkuma dēļ šis risinājums netika attīstīts. Ilustrācijai var apskatīt daļu XML ziņojuma:

```

- <readouts floor_date="2011-10-01 00:00:00" ceil_date="2011-10-31
23:59:59">
- <readout>
<equipment_number>15720</equipment_number>
<value>2.1700</value>
<consumption>0.28</consumption>
<date>31.10.2011 13:30:00</date>
<address>Darza 9, 54. dz. (aukstais)</address>
<client_no />
<meter_type>1</meter_type>
<common_meter />
</readout>
- <readout>
<equipment_number>15708</equipment_number>
<value>5.1200</value>
<consumption>0.72</consumption>
<date>31.10.2011 13:30:00</date>
<address>Darza 9, 54. dz. (karstais)</address>
<client_no />
<meter_type>2</meter_type>
<common_meter />
</readout>

```

5.3. Bezvadu sensoru tīkla tehnoloģijas pētījumi un eksperimenti Ventspilī

Ventspils Augstskolas VIRAC, Kauņas Universitātes Telekomunikāciju un elektronikas fakultāte, Latvijas Interneta Asociācija un Ventspils Ūdeka 2012-13. gadā realizēja projektu „Smart Metering”, kuru finansēja ERAF Latvijas - Lietuvas pārrobežu programma. Projekta mērķis bija izpētīt jaunus IKT tehniskus risinājumus, kurus var pielietot siltuma piegādes un ūdensvada tīklos, aprīkot ar aparatūru universitāšu laboratorijas, kurās var gatavot nozares speciālistus, un izstrādāt Tehnoloģijas attīstības un pielāgošanas programmu vidējam laika termiņam.

5.3.1. Ūdensvada izmēģinājuma tīkla segmenta izvēle

Ūdensvada izmēģinājuma tīkla segmentam vajadzēja apmierināt priekšnosacījumus, kas ļautu veikt nepieciešamus eksperimentus dabā, analizēt rezultātus un ļautu izmantot izstrādātos risinājumus arī citos ūdens vai siltuma apgādes tīklos.

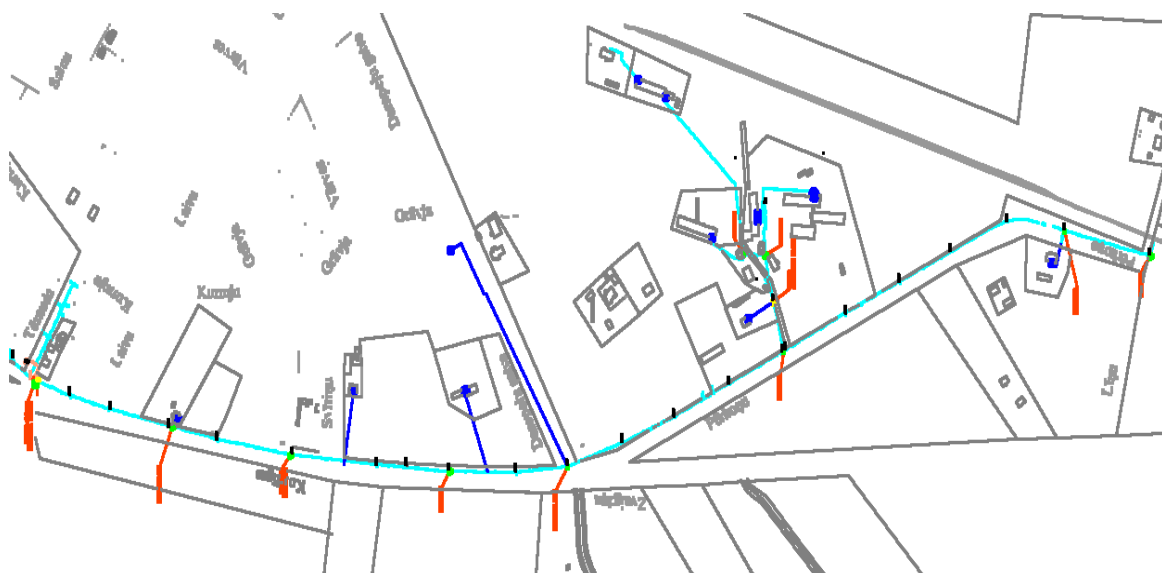
Viens no svarīgākajiem faktoriem, ir piemērota tīkla segmenta izvēle. Izvēlētai vietai jābūt tādai, kas ļautu izspēlēt visus eksperimentālos scenārijus, analizēt rezultātus un izdarīt pareizus secinājumus (skatīt 5.7. att.):

Izvēlētam ūdensvada izmēģinājuma tīkla segmentam ir šāds raksturojums:

- Izolēts tīkla segments ar ierobežotu abonētu skaitu, lai mazāk ietekmētu abonentus ūdens mērītāju uzstādīšanas laikā;
- Rajons ar nelielu automašīnu trafiku, lai būtu mazāk problēmu ar aparatūras un mastu uzstādīšanu;

- Augstas ēkas, uz kurām var uzstādīt raidīšanas - uztveršanas aparāturu;
- Pieejamas ūdensvada akas;
- Atzarojumi no galvenā tīkla, kuros varētu veikt datu analīzi un tīkla modelēšanu;
- Iespēja izveidot slēgtu tīkla segmentu.

Šāds tīkla segments ar nosaukumu „Selga”, bija izvēlēts Kuldīgas, Dampēļu un Pērkonu ielu rajonā.



5.7. att. Eksperimentālais ūdensvada tīkla segments “Selga”

Tas ir slēgts segments ar vairākiem atzarojumiem, un tas ļāva iekļauties budžeta apjomā, kas bija vajadzīgs sensoru un mēraparātūras uzstādīšanai. Tīkla ievads ir kontrolēts ar SCADA, kas nodrošina ieejas spiediena un plūsmas mērījumus. Turklāt izmēģinājuma tīkls ir pietiekoši garš, lai tajā veiktu šķidrums dinamikas imitāciju (viļņu izplatīšanās).

Tehniskās problēmas, kas jāatrisina saistībā ar mērīšanas datu pārraidi no ūdensvada akām:

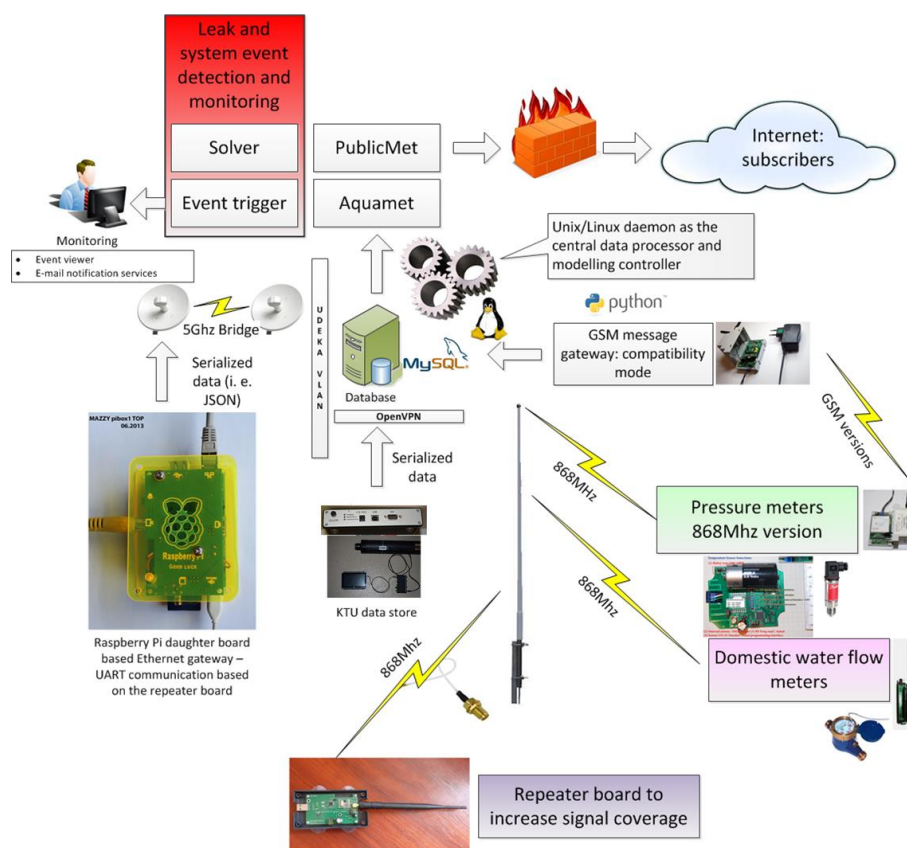
- Elektroenerģijas padeve spiediena mērītājiem;
- Esošās plūsmas un spiediena mērījumu sensorus – raidītāju adaptācija, lai izmantotu 868MHz RF, nevis GPRS;
- Raidīta signāla stiprums, ņemot vērā šķēršļus un interferenci;
- Signāla pārraide no ūdensvada akām;
- Datu pakešu retranslācija, izmantojot Ethernet;
- Fiziskā skaitītāju uzstādīšana objektos;
- Programmatūras pielāgošana datu apstrādei un vizualizācijai

Tika izlemts, par pamatu izmantot IT House un Micro Dators AquaMet kodu un to pārveidot atbilstoši jauniem risinājumiem.

„Smart Metering” sistēma, kuru plānoja izveidot projekta gaitā, sastāv no šādām sastāvdaļām (skat. 5.8.att.) :

- Ūdens patēriņa un spiediena mērītāji;
- Sensori - datu pārraides ierīces, ISM diapazons 868 MHz;
- Ethernet vārtejas, kas pārveido signālus no sensoriem uz TCP/IP;
- 5 GHz Bridge, lai nodrošinātu datu plūsmu uz esošo pašvaldības Wi-Fi tīklu;
- GSM datu pārraides vārtejas;
- Sistēmas notikumu un noplūžu monitoringa un noteikšanas sistēma;
- Centrālā datu bāze;
- Tehniskais risinājums datu uzglabāšanas Kauņas Tehniskās Universitātes mērījumiem, veiktiem uz siltumtrasēm;

Smart Metering sistēmas visaptverošs apraksts ir sniegts turpmākajās nodaļās.



5.8. att. “Smart Metering” sistēmas blokhēma (Zabašta u.c. [88])

5.3.2. *Sensori - transiveri*

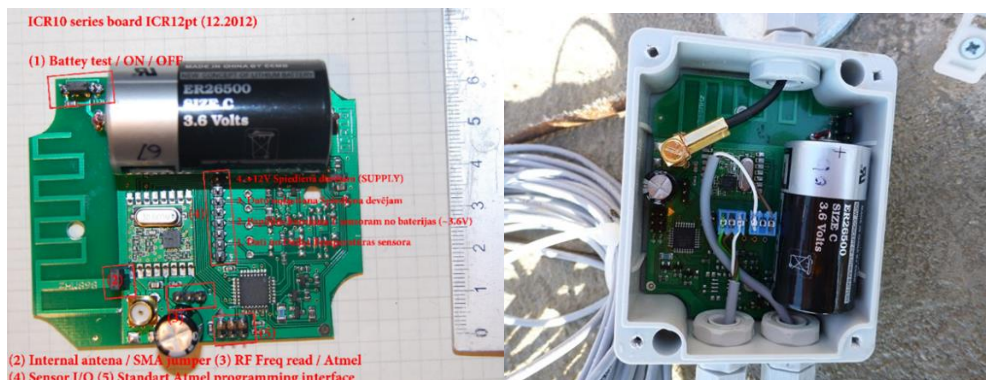
Vieglākai prototipēšanai un lētākai radio frekvences integrālās shēmas izmantošanai, tika izvēlēts HopeRF Electronics (<http://www.hoperf.com>) radio frekvenču (RF) moduli, jo tie satur atbilstošas modulācijas shēmas aparatūras līmenī: raidītāju un uztvērēju. Šādi mikročipi nodrošina vieglu integrāciju ar Atmel sēriju (ATMEGA48, ATmega88, ATMEGA168, ATmega328), tiem ir zemas izmaksas, laba enerģijas efektivitāte un apmierinoša signāla novājināšana. Atmels mikroshēmas var izvēlēties atkarībā no sensoru tīklu elementu prasībām pret skaitļošanas jaudu. RFM tiek izmantoti mājas automatizācijas un rūpnieciskās kontroles ierīcēs, sensoru tīklos, veselības monitora ierīcēs un citur [60].

RFM (22B/23B) moduļa galvenie parametri:

- Frekvences diapazons: 433/470/868/915 ISM diapazons;
- Jūtība: -121dBm;
- Izejas jaudas diapazons: +13 dBm (RFM23B), +20 dBm Max (RFM22B);
- Zems enerģijas patēriņš: 18.5 mA uztveršana, 30 mA @ +13 dBm raidīšana, 85 mA @ +20 dBm raidīšana;
- Pārtraides ātrums: 0.123 to 256 kaps;
- FSK, GFSK un OOK modulācija;
- Digitāla RSSI;
- Zems enerģijas patēriņš izslēgšanas režīmā;
- “Wake-up” taimeris;
- TX un RX 64 baitu FIFOs;

Mikrokontrolera komunikācija ar radio moduli tiek veikta, izmantojot SPI (Serial Peripheral Interface Bus), kas ir sinhronais sērijas datu pārtraides standarts ar nosaukumu “Motorola” un kas darbojas pilnā duplexā režīmā. Modulācijas shēma GFSK (Gausa Frequency-Shift Keying) tika izvēlēta, jo tā ir pielāgota izplatītākajām bezvadu sakaru tehnoloģijām, tādām kā Bluetooth, DECT utt. Papildus GFSK modulācijai “Manchester” kodēšanas shēma [46] tiek izmantota komunikācijās procesā.

Attēlā 5.9. ir parādīts sensora – raidītāja ārējais izskats ar iezīmētiem kontaktiem, kurus izmanto aparatūras testēšanai un programmēšanai.



5.9. att. Sensora – raidītāja ārējais izskats

5.3.3. Retranslācijas princips

Ierobežotais vārteju skaits, kas kalpo, lai izveidotu savienojumu ar “back-end” sistēmu, kas apstrādā datus un izveido pakalpojumus, veicināja atkārtotāju risinājumu izstrādi. Vārteju izgatavošana un uzstādīšana ar mērķi iekļauties esošā pašvaldības Wi-Fi tīklā ir sarežģīta un dārga, jo tā prasa papildu mastu un 5GHz tiltu (“bribges”) izmantošanu. 5.10. attēlā var redzēt 5GHz tīkla mastus, kurus uzstādīja projekta gaitā, lai nodrošinātu piekļuvi tīklam Ethernet vārtejā, kas savāc sensoru datus, izmantojot 868 MHz antenu (skat. 5.10. Att., kur vienā mastā var redzēt 868 MHz un 5GHz antenas).

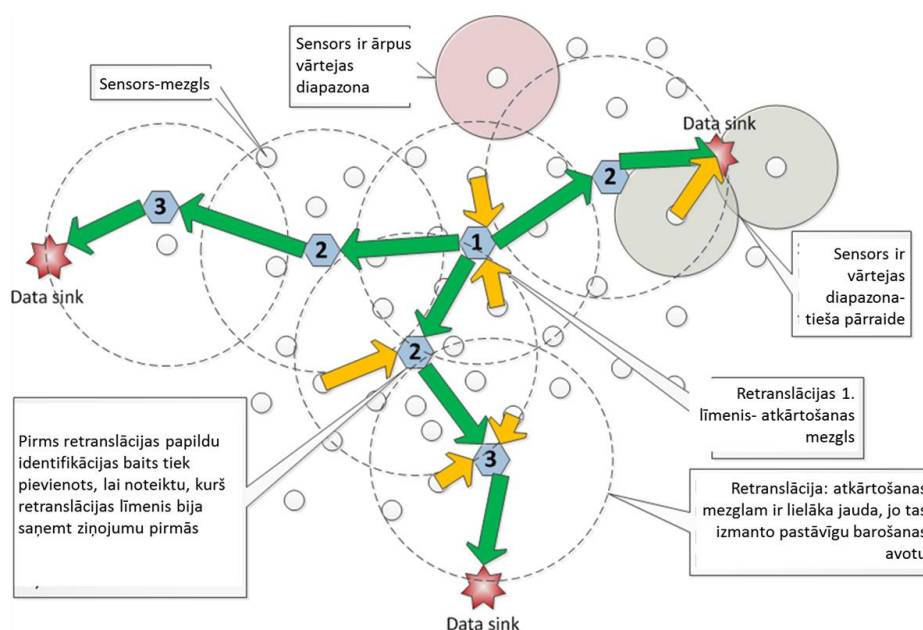


5.10. att. 5GHz “bridge”, kuru izmanto, lai radītu Smart bāzes tīklu.

Retranslatora uzdevums ir izveidot daudzslāņaino vienvirziena datu nosūtīšanas infrastruktūru. Viena no tipiskām bezvadu tīklu problēmām rodas saistībā ar sūtījumu kolīzijām un maršrutizācijas kontroli. Ņemot vērā, ka pārraide notiek tikai vienā virzienā, neveidojas slēptie mezgli un citas problēmas. Izstrādātais risinājums (skat. 5.11. att.) ietver:

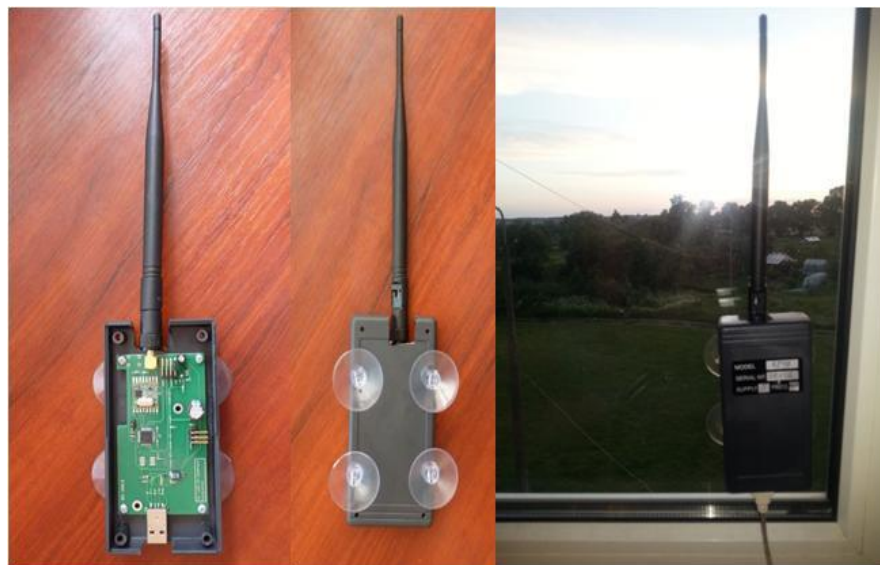
- Sensoru - mezglu ziņojumi tiek nosūtīti “akli” bez adreses informācijas saistībā ar turpmāko retranslāciju.

- Ja sensors - mezgls atrodas vārtejas uztveršanas diapazonā, dati tiek saņemti, dekodēti un pēc tam ziņojums tiek kodēts tālākai nosūtīšanai uz serveri.
 - Ja sensors - mezgls ir ārpus vārtejas uztveršanas diapazona, ziņojumu saņem retranslācijas mezgls.
- Retranslatoriem (atkārtotāju mezgliem) ir izmantotas labākas antenas (attiecībā uz jutīgumu un pārraides pārklāšanas zonu), retranslatori ir pieslēgti pastāvīgam enerģijas avotam, tāpēc tikai trīs vārtejas un trīs retranslatori nodrošina tīkla pārklājumu visiem sensoriem - mezgliem, uzstādītiem izmēģinājuma tīklā.
 - Kad retranslatoris saņem jaunu sensoru ziņu bloku, tas ievieto to rindā uz retranslāciju. Pirms retranslācijas papildu identifikācijas baits tiek pievienots, lai būtu iespējams noteikt, kādu retranslācijas līmeni retranslē ziņojumā.
 - Pēc pārraides līmeņa identifikācijas numura piešķiršanas, ziņojums tiek pārraidīts vai tuvākai vārtejai vai citam retranslācijas mezglam.
 - Ja uztvērējs ir vārteja, tā noņem identifikācijas baitu un dekodē ziņojumu;
 - Ja uztvērējs ir cits retranslācijas mezgls, tas nolasa līmeņa identifikācijas baitu un salīdzina ar savu līmeņa identifikatoru:
 - Ja līmeņa identifikators ir lielāks vai vienāds ar ziņojuma baitu, tad ziņojums tiek anulēts;
 - Ja līmeņa identifikators ir mazāks, tad ziņojuma baitu tiek pārrakstīts ar uztveroša retranslatora identifikatora numuru un tiek pārraidīts tālāk.
 - Retranslācijas līmeņa identifikatoriem jābūt pareizi piešķirti, lai izveidotu "sīpolam līdzīgu struktūru";



5.11. att. Ziņojumu retranslācijas metodes apraksts (Zabašta u.c. [88])

Tā kā retranslācijas mezgli darbojas nepārtraukti, tos nevar nodrošināt ar barošanu no baterijām, jo darba laiks būtu pārāk īss. Lai atrisinātu šo problēmu, ir panākta vienošanās ar privāto ēku īpašniekiem, lai instalētu retranslatorus piemērotākās vietās. 5.12. attēlā var redzēt retranslatora ārējo izskatu.



5.12. att. Retranslatora ārējais izskats

5.3.4. Antenas dizains pilsētvidei

Lai konstatētu noplūdes, ir nepieciešams uzstādīt ūdens plūsmas un spiediena mērītājus - sensorus ūdens sadales tīklā. Savukārt, lai nodrošinātu datu pārraidi no ūdensvada kontrolakās uzstādītiem sensoriem – raidītājiem, būtu jāizmanto īpašas antenas. Tomēr šāda veida speciālo antenu piedāvājums ir ļoti ierobežots un dārgs.

Projekta gaitā ir analizēti dažādu antenu tipi: virziena un izkliedētā tipa antenas. Tika izmēģināti divi antenu instalācijas veidi: antenas piestiprināšana pie ūdensvada akas vāka, zemes līmeņa un montēšana uz ugunsdzēsības hidrantiem. Antenu prototipi pirms uzstādīšanas tika aizsargāti ar poliuretānu, kuram ir radio signāla zema vājināšana. Virziena antenas ir sarežģītas mehāniskās struktūras dēļ, to ražošana ir darbietilpīga un ir vairākas reizes dārgāka par izkliedētā tipa antenu izgatavošanu. Papildus tam raidīšanas antenas jākalibrē laboratorijas vidē, lai sasniegtu labus pārraides parametrus (skat. izkliedētā tipa antenas paraugus 5.13. attēlā).



5.13. Att. Izkaldētā tipa antenu paraugi

Tā kā ražošanas prototipi ir jākalibrē atbilstoši frekvencei, pieskaņošanas process aizņem milzīgu laiku pārbaužu un kļūdu korekciju dēļ, tāpēc tika nolemts izmantot par bāzes paraugu gatavu 868MHz $\frac{1}{4}$ viļņu antenu (skat. 5.14 un 5.15. att.).



5.14.att. 868MHz $\frac{1}{4}$ viļņu antenas paraugi



5.15.att. 868MHz $\frac{1}{4}$ viļņu antenas uzstādīšana ūdensvada akas vākā

Vairāki eksperimenti ar antenu pārklājumu materiāliem tika veikti, lai atrastu optimālu cenas un veiktspējas attiecību. Pirmie prototipi bija izveidoti, lai saprastu materiālu nepieciešamās mehāniskās īpašības un izvēlētos atbilstošu aku vāku armatūru.

Kā labāko materiālu izvēlēja TASK®16 uretānu - augstas stiepšanas izturīgu pret triecienu un nodilumu. TASK®16uretānu var iekrāsot ar videi piemērotu krāsas toni. Pārbaudot uretāna ietekmi uz radio signālu, netika konstatēta jebkāda ievērojama vājināšana 868MHz radio frekvenču diapazonā. Projekta finālā stadijā, kad tika uzstādīti atlikušie spiediena dēvēji un

sensori – raidītāji, tika konstatēts, ka UĪ starojuma ietekmes dēļ uretāna pārklājums izmainīja sākotnējo krāsu pret gaiši-pelēko, šādi padarot antenu praktiski nepamanāmu uz betona plākšņu vai vāku fona (5.16. attēla tiek attēlota spiediena mērītāju uzstādīšana ūdensvada akā).



5.16. att. Ūdens spiediena mērītāja uzstādīšana ūdensvada akā

5.3.5. Ethernet vārteja - koncentrators

Pibox Ethernet vārtejas attīstības posmi

Ethernet – vārteja izpilda funkcijas: sensori reģistrē mēraparatūras (ūdens plūsmas, ūdens spiediena) mērījumus un nosūta tos vārtejām - koncentratoriem, kas savāktos datus sagatavo tālākai transportēšanai uz datu apstrādes sistēmu. Savāktie dati tiek pārbaudīti un saglabāti vārtejas iekšējā atmiņā.

Uztveršanas ierīce ir savienota ar mikrodatoru (izmantojot USB seriālo interfeisu). Raspberry Pi ir kredītkaršu lieluma vienas plates dators, kuru izstrādāja “Raspberry Pi Foundation”, un kas tiek izmantots kā mikrodators. Mikrodatoru vadības programmatūra nosūta īpašas pakalpojumu komandas, lai iegūtu mērījumu datus no sensoru iekšējās atmiņas. Atšķirībā no sensoriem – raidītājiem vārtejas iekārtai ir nepieciešams pastāvīgas barošanas avots, sakarā ar lielāku enerģijas patēriņu.

Vārtejas “Etherner gateway” pakalpojumi tiek izmantoti, lai serializētu un nosūtītu datus uz centrālo datu bāzi. C un Python programmēšanas valodas tiek izmantotas, lai nodrošinātu vienkāršāku komunikāciju ar topošiem risinājumiem un platformām.

Kompānijas Mazzy GPRS risinājums bija izvēlēts kā bāzes risinājums, no kura izmantoja ISM diapazona radio daļu un integrēja jaunajā 868MHz dizainā. Jauna risinājuma attīstība tika veikta, saglabājot savietojamību ar veco dizainu, ņemot vērā iespējamās 868MHz signāla pārraides problēmas, ko rada vietnes ar lieliem attālumiem un apgrūtinātu pieejamību. Šajos gadījumos esošais GPRS risinājums var būt joprojām izmantots.

Sensoru signālu uztveršanas aparatūrai kā pirmo versiju pielāgoja 868MHz testēšanas ierīci, kas tiek izmantota, lai diagnosticētu sensoru darbību, rādot reālā laikā uz LCD displeja

datu pārraides vērtības. Šī ierīce tika paplašināta ar USB sērijas saskarnes portu, ko var savienot ar iegulto Ethernet vārtejas kontrolieri vai ar parastu datoru, izmantojot standarta USB interfeisu.

USB ierīce ir pielietota kā vispārējais seriālais ports. Izmantojot standarta “termināl” lietojumprogrammu, var nosūtīt klaviatūras komandas un uztvert rādījumi kā vienkārša teksta (“plain text”) informāciju.

5.17. attēlā kā piemērs ir parādīti uztveršanas aparatūras rādījumi, kas ir attēloti kā vienkārša teksta rindas: mērījumu reģistrēšanas datums, mēness, laiks, seriālais numurs, divu mērītāju rādījumi, baterijas mērījumi (STAT) un saņemta signāla mērījums (RS - tas ir RSSI signāla stiprums).

```
Date Time      SerialNr Count1 Count2 STAT rs fr
00.00 00:00:00 00000000 000000 000000 0000 FA 00
23.01 18:23:39 141B7C9F 000000 000000 031D 6E 00
23.01 12:56:29 141B7C45 000000 000000 0307 65 00
26.01 14:48:10 141B76CC 000CF1 000000 0317 5B 00
24.01 12:12:33 0C00006C 00FFFF 000000 0032 6E 00
24.01 12:06:29 0C000068 00FFFF 000232 0034 79 00
26.01 15:15:47 141B7D21 000001 000000 031B 5D 00
26.01 15:16:59 141B78F6 0058B5 000000 031E 86 00
24.01 12:06:27 0C000066 00FFFF 000000 0032 71 00
24.01 12:13:40 0C000064 000092 000000 0032 77 00
24.01 12:07:27 0C000065 00FFFF 000000 0033 67 00
26.01 15:16:45 141B7C45 0000DD 000000 031C 7A 00
26.01 15:08:42 141B7C9F 00004B 000000 031D 80 00
26.01 07:51:00 B226897E F3744C 57CFE8 7A17 5A 00
```

5.17. att. Uztveršanas aparatūras rādījumu piemērs

Piemērā apakšā var redzēt, ka mērījumu dati pēc apstrādāšanas un šifrēšanas tiek nosūtīti no Ethernet vārtejas uz sistēmas centrālo datu bāzi turpmākas apstrādes mērķiem.

```
Setting DateTime: w30012330
```

```
Date and Time
```

```
30012330
```

```
Hash: 48aeac7f70751d80b09a6ac23eb5375b DateTimeRec: 1359581312 Device
type: 10 Device serial: 1B7C45 Value 1: 958 Value 2: 0 Battery: 796 RSSI: 120
http://exec.bitdev.lv/post.php?hash=48aeac7f70751d80b09a6ac23eb5375b&bat
tery=796&timestamp=1359581312&value2=0&value1=958&rssi=120&serial=1B7C45&typ
e=10
```

```
Hash: 8980347bcdc27e25d50546adc9b4909b DateTimeRec: 1359580835 Device
type: 10 Device serial: 1B78F6 Value 1: 4384 Value 2: 0 Battery: 796 RSSI:
119
```

```
http://exec.bitdev.lv/post.php?hash=8980347bcdc27e25d50546adc9b4909b&bat
tery=796&timestamp=1359580835&value2=0&value1=4384&rssi=119&serial=1B78F6&typ
e=10
```



5.18.att. Viena no pirmajām vārtejas versijām (uzstādīta uz pansionāta “Selga” jumtas)

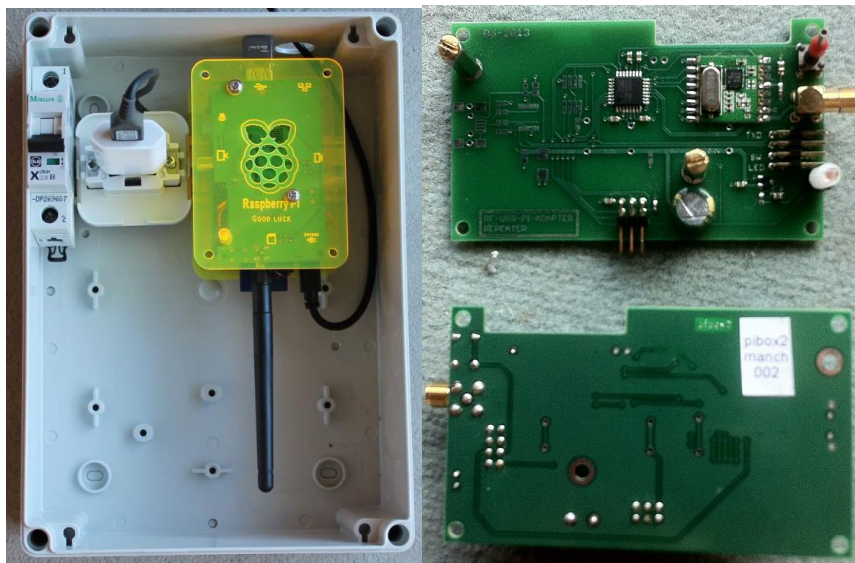
Otrā Ethernet vārtejas versija (skat. 5.18. att.) tika veidota pēc vispārēja iegultās platformas principiem (“generic embedded platform”). Tika izvēlēta Raspberry Pi ARM7 platforma, jo tā nodrošina nepieciešamu skaitļošanas jaudu, un tai ir kompozīta videoizeja. Tātad šo ierīci var izmantot arī ar displeju, lai veiktu diagnostiku klātienē uz objektiem. Galvenais sistēmas process, mērījumu datu nolasīšana un piegāde uz sistēmas serveri tika uzrakstīta Python valodā un papildināta ar papildu atbalsta servisiem.

Pakalpojums nodrošina virtuālo privāto tīklu atbalstu attālinātiem izvietojumiem, pakalpojumu automātisku uzraudzību, kļūdu paziņojumus, uzraudzības funkciju sistēmas līmenī un CPU automātisku restartēšanu.

Otrās vārtejas versijā galvenie uzlabojumi:

- “Aquamon Multi Threaded Daemon” programmatūra apstrādā USB datus un sagatavo nogādāšanai uz serveri;
- MONIT pakalpojuma paziņojumu un Aquamon pakalpojumu kontrole (e-pasta paziņojumu, problēmu noteikšana, pakalpojumu atjaunošana);
- VPN atbalsts (Tinc, PPTP, OpenVPN);
- Watchdog: Broadcom BCM2708 “watchdog” atbalsts (vārteju uzraudzība, pārslodzes gadījumā restartēšana);
- SD kartes atmiņas un log failu kontrole (RAMLOG).

Pēdēja uz Raspberry Pi Ethernet balstīta vārteja tiek aprīkota ar RF 868MHz uztveršanas “meitas” plati, “heartbeat” norādi, bezvadu tīkla adapteri un drošu izslēgšanas pogu. Kompozītu izeja tiek izmantota ērtai diagnostikas un kontrolei (sk. 5.19. att.).



5.19.att. Pibox Ethernet vārtejas ārējais izskats

Lai savienotu Ethernet segmentus ar sistēmas serveriem, tika nolemts izveidot virtuālo privāto tīklu. Tika testēts viens no atvērtā koda virtuālā privātā tīkla risinājumiem - OpenVPN Tinc. Tinc VPN risinājums ir piemērots iegultajām sistēmām, ir savietojams ar lielāko daļu Unix operētājsistēmām un atbalsta multisegmentu pārejas.

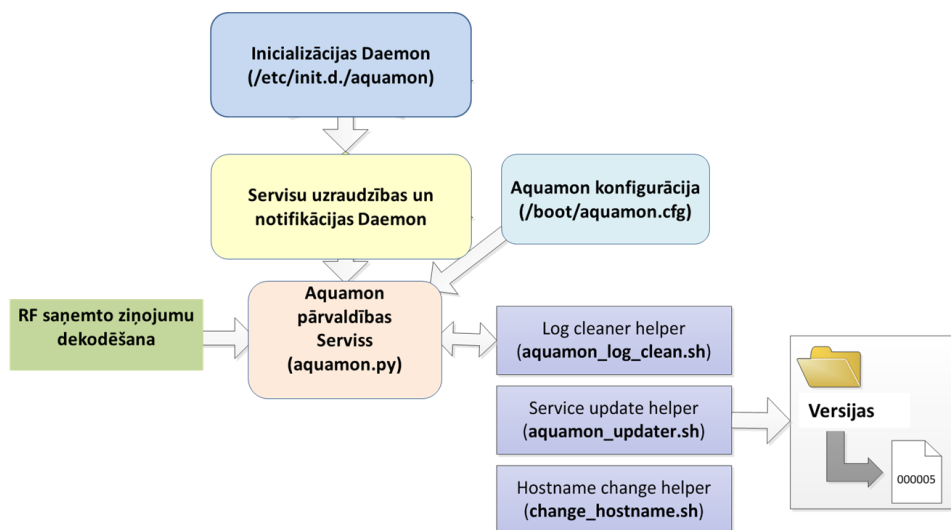
Ethernet vārteja – Aquamon pakalpojumi

Sistēmas pakalpojumu arhitektūra, kuru projektā nosauca par “Aquamon”, ir paredzēta autonomai pakalpojumu atjaunošanai un notikumu reģistrēšanai ar mērķi uzraudzīt vārtejas no centrāla servisu centra. Tiek realizētas galvenās funkcijas:

- Ziņojumu saņemšana no USB ierīces;
- Kļūdu analīze ziņojumos;
- Ziņojumu buferizācija;
- Ziņojumu kodēšana;
- Ziņojumu sagatavošana pārraidei Ethernet;
- Drošība nosūtīšanas procesā.

Datu apstrādes process vārtejas ierīcē tiek veikts Aquamon Daemon servisā, kuru raksturo kā vairākuzdevumu datoru operētājsistēmu datorprogrammu, kas galvenokārt darbojas kā fona process, nevis kā tiešas kontroles [20]. Atbalsta pakalpojumi nodrošina papildu funkcionalitāti (skat. att. 5.20):

- Aquamon pakalpojumu esamības pārbaude un atjaunināšana bojājumu gadījumā;
- Iekšējo notikumu un kļūdu uzraudzība un reģistrācija;
- Pakalpojumu automātiska atjaunināšana un palaišana no centrālās vadības sistēmas;
- Tīkla konfigurācija, lai nodrošinātu vairāku Ethernet vārteju līdzāspastāvēšanu vienā tīkla segmentā.



5.20.att. Aquamon pakalpojumu blokhēma (Zabašta u.c. [88])

Apakšā ir attēloti daži atbalsta pakalpojumu (“helper scripts”) kodu piemēri, kurus izmanto, lai iedarbinātu drošu servisu darbību:

```

aquamon (initialization daemon)
mkdir -p /var/run/aquamon/
chmod 777 /dev/ttyUSB0
case "$1" in
  start)
    echo "Starting server"
    /usr/bin/python /home/administrator/aquamon.py start
    ;;
  stop)
    echo "Stopping server"
    /usr/bin/python /home/administrator/aquamon.py stop
    ;;
  restart)
    echo "Restarting server"
    /usr/bin/python /home/administrator/aquamon.py restart
    ;;
  *)
    echo "Usage: /etc/init.d/aquamon {start|stop|restart}"
    exit 1
    ;;
esac
exit 0

```

```
aquamon_log_clean.sh
#!/bin/bash
echo "" > /var/log/aquamon/aquamon.err
echo "" > /var/log/aquamon/aquamon.log
echo "" > /var/log/aquamon/aquamon.out
```

```
aquamon_updater.sh
#!/bin/bash
PREV_VER=$(echo -n `ls /home/pi/aquamon/versions` | tr -d "\n")

if [ -z "$PREV_VER" ];
then
PREV_VER="000000"
fi

CUR_VER=`curl -s
http://aquamet.bitdev.lv/lv/aquamet/aquamon_versions/version`
#touch versions/`curl -s
http://aquamet.bitdev.lv/lv/aquamet/aquamon_versions/version`

echo Previous version: $PREV_VER
echo Current version: $CUR_VER

if [ $PREV_VER == $CUR_VER ]
then
echo Version match.
else
echo Versions do not match.
rm -fr /home/pi/aquamon/versions/*
curl -s http://aquamet.bitdev.lv/lv/aquamet/aquamon_versions/download >
/home/pi/aquamon/aquamon.py
touch /home/pi/aquamon/versions/`curl -s
http://aquamet.bitdev.lv/lv/aquamet/aquamon_versions/version`
service aquamon restart
fi
```

Ekrāna attēls (skat. 5.21 att.) parāda automātisko Ethernet vārtejas programmatūras atjauninājumu publicēšanas sistēmu, kas ir integrēta uzraudzības informācijas sistēmas Web interfeisā. Uzraudzības sistēma nodrošina automātisku Ethernet vārteju pamata programmatūru atjaunošanu.

Valoda: LV EN RU | testuser@testdomain.com | Ietekums | Kļūdas ziņojums | Iziet

Smart Metering

[Sietēma](#)
[Iestatījumi](#)
[Saskarne](#)

Aquamon versions

[+ Jauns ieraksts](#)

Nosaukums	Versija	Fails	Datums	Iespējas
Version update test nr. 5 - hostname changer, ip detect,	000005	public/aquamons /aquamon.py	25/03/2013 18:51	Lejupielādēt
Version update test nr. 4	000004	public/aquamons /aquamon.py	25/03/2013 11:08	Lejupielādēt
Version update test nr. 3	000003	public/aquamons /aquamon.py	25/03/2013 10:53	Lejupielādēt
Version update test nr. 2	000002	public/aquamons /aquamon.py	25/03/2013 10:39	Lejupielādēt
Aquamon: gwid, tester_v15	000001	public/aquamons /aquamon.py	25/03/2013 08:15	Lejupielādēt

- Vārtejas
- Mērītāji
- Rādījumi
- Rādījumu statistika
- Rādījumu saraksts
- Spiediena devēji
- Spiediena devēju rādījumi
- Spiediena devēju statistika
- Spiediena devēju temperatūra
- Sūkņi
- Sūkņu rādījumi
- Sūkņu rādījumu statistika
- Aquamon versions
- Koda versijas
- Gala lietotāji
- Reģioni
- Cenas
- Kompānijas
- Event Log

Labot izvēni

© 2012-2013 Smart Metering 1.15

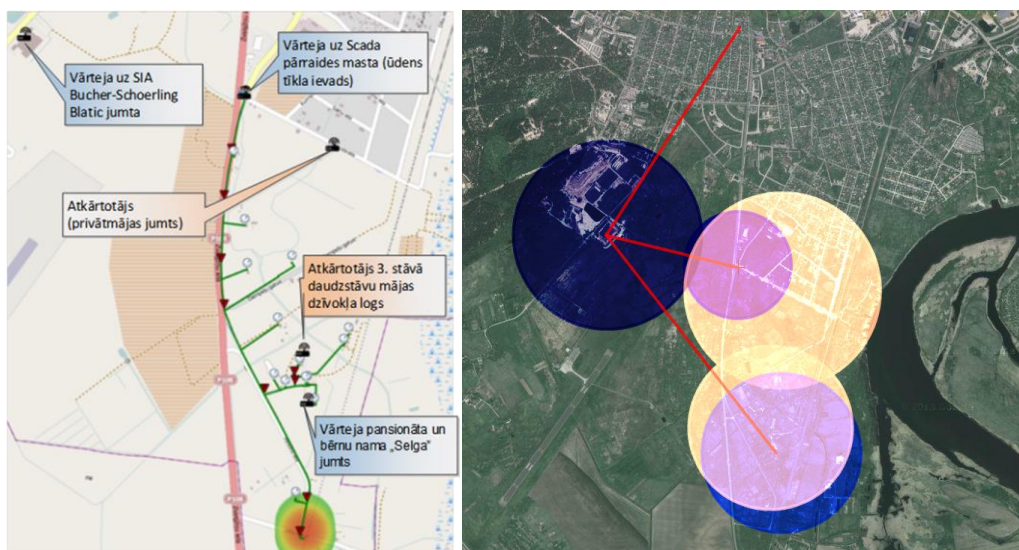
5.21.att. Ethernet vārtejas programmatūras automātiskas atjauninājumu publicēšanas sistēmas ekrāna attēls

5.3.6. Izmēģinājuma tīkla galīgais variants

Izmēģinājuma ūdensvada tīkls atrodas pilsētas nomalē, kur koku zari un lapas traucē gan RF 868MHz sensoru, gan bezvadu 5.8GHz datu pārraides tīklam, tāpēc, lai nodrošinātu uztverama signāla optimālo līmeni, tika pārvietoti vai pacelti augstāk no zemes sensori raidītāji, un tika atrasts Ethernet vārteju un atkārtotāju optimālais izkārtojums.

Bezvadu tīkls tiek būvēts, pielietojot zvaigznes topoloģiju, apvienojot sensoru RF tīklu ar Ethernet vārtejām, kas kopā izveidoja ērti pārvaldāmo homogenu vidi. Kombinējot Ethernet vārtejas ar retranslācijas ierīcēm, ir sasniegts optimālais sensoru - raidītāju pārklājums: tikai trīs Ethernet vārtejas un divi retranslācijas mezgli.

5.22. attēlā var redzēt galīgu tīkla izkārtojumu, kur zili apļi atspoguļo Ethernet vārteju uztveršanas zonas, bet dzeltenie apļi parāda retranslatoru uztveršanas - raidīšanas zonas. Kopējais skaits ūdens plūsmas sensoru ir 14 (sk. 5.2. tabulu), bet ūdens spiediena skaitītāju kopskaits ir 9.



5.22. att. Izmēģinājuma tīkla galīgais variants

5.2.Tabula

Ūdens plūsmas sensoru izvietojums

Nr.	Address	Serial nr.	Meter value	Impulse value (liters)	Date	ICR "on" time	Cold/Hot	ICR prim adr.	ICR port nr.
1	Pērkoņu iela 21 (Katlu māja)	000170	1,621	10L	15.01.2013	10:23	C	1801375	1B7C9F
2	Pērkoņu iela 21 (Veļas mazgātuve)	000157	237,44	10L	30.05.2013	13:42	C	1802610	1B8172
3	Kuldīgas iela 209	23284-1	271,8	10L	30.05.2013	17:00	C	1801897	1B7EA9
4	Kuldīgas iela 215	1239852	40,9	10L	03.06.2013	12:50	C	1801579	1B7D6B
5	Pērkoņu iela 7	011292	92,82	10L	30.05.2013	17:15	C	1799485	1B753D
6	Pērkoņu iela 14	111009067	200,111	10L	21.06.2013	10:53	C	1800737	1B7A21
7	Pērkoņu iela 11	1111009044	30,6	1m3	30.05.2013	16:20	C	1801839	1B7E6F
8	Pērkoņu iela 19	111008959	360,92	1m3	30.05.2013	14:15	C	1799808	1B7680
9	Pērkoņu iela 11A	1243881	1,2	10L	30.05.2013	16:00	C	1800982	1B7B16
10	Kuldīgas iela 201	1243868	9,92	10L	30.05.2013	16:40	C	1799790	1B766E
11	Dampeļu gatve 9	1243953	41,1	10L	30.05.2013	16:30	C	1801794	1B7E42
12	Pērkoņu iela 13	1134000755	4926,10	1L	31.05.2013	09:40	C	1800262	1B7846
13	Pērkoņu iela 17	1134000774	1805,14	1L	30.05.2013	13:55	C	1800499	1B7933
14	Pērkoņu iela 21 (Pansionāts)	1032006285	2861,222	10L	21.06.2013	11:15	C	1801104	1B7D90

Kvalitātes veiktie testi, lai novērtētu sensoru tīkla veiktspēju - kāda mērījumu ziņojumu daļa sasniedz centrālo sistēmu,- atklāja, ka visi dati ir saņemti ar maksimālo kavēšanās laiku 2 stundās. Ziņojumu zaudēšana lielā mērā ir atkarīga no laika apstākļiem, jo tests tika veikts jūlijā mēnesī nelabvēlīgos laika apstākļos (lietains un maksimālas veģetācijas laiks) (skat. 4.Pielikumu).

5.3.7. “Smārt Meter” informācijas sistēmas arhitektūra

Izstrādātā “Smārt Meter” sistēma papildus ūdens sadales tīkla spiediena un plūsmas kontroles sistēmai iekļauj arī saskarni lietotājiem un ūdensvada tīkla elementu datu bāzi. Visiem informācijas sistēmas sastāvdaļām pamatā ir atvērtā koda produkti, līdz ar to nav licencēšanas izmaksas un pastāv plašas iespējas izmantot dažādas virtualizācijas sistēmas atbilstoši klientu vajadzībām.

Smart Meter sistēma sastāv no četriem bāzes komponentiem:

- ***Mērītāju datu saņemšanas komponente***

Šī komponente saņem HTTP šifrētu POST, kuru izveido Ethernet vārteja, kas uzkrāj un sagatavo sensoru rādījumus, un veic HTTP POST uz Smart Meter WEB serveri (Apache), pamatojoties uz DNS adresi. Apache Web serveris novirza pieprasījumus specifiskai programmai - vārtejas daemon (<http://exec.bitdev.lv>). Programma (PHP valoda) pārbauda datu autentiskumu. Ja dati ir akceptēti, tie tiek glabāti sistēmas MySQL datu bāzē.

- ***Smart Meter uzraudzības, statistikas un datu vizualizācijas saskarne***

Smart Meter sistēma ir veidota uz "Ruby on Rails", izmantojot MVC (Modelis, View, un Controller) arhitektūru. MVC ir programmatūras arhitektūra modelis, kas atdala informācijas prezentāciju no lietotāju mijiedarbības ar to. Modelis iekļauj datus, biznesa noteikumus un funkcijas. Modelis izvada pieprasītos datus tabulu un diagrammu formā.

- ***Smart Meter klientu patēriņa statistika uzskaitē un norēķiniem***

Šī komponente darbojas uz atsevišķa servera klastera un ir balstīta arī uz "Ruby on Rails". Tā nodrošina tīmekļa saskarni klientiem. Klienti var redzēt savu ūdens patēriņu par izvēlēto laika posmu, izmantojot dažus vizualizācijas veidus. Ir iespējams iegūt ūdens patēriņa robežvērtības brīdinājumus pa e-pastu vai automātiski izveidot rēķinu.

- ***Smart Meter noplūžu atklāšanas modulis***

Noplūžu atklāšanas komponente sastāv no vairākiem moduļiem, kas veic regulārus pārrēķinus, pamatojoties uz datiem, saņemtiem no sensoriem. Viens no moduļiem veic SCADA sistēmas simulācijas pakalpojumus, kas nodrošina viendabīgu interfeisu starp SCADA aparatūras veiktiem mērījumiem (SCADA ir uzstādīta uz izmēģinājuma tīkla robežpunkta, kas atdala izmēģinājuma tīkla segmentu no pilsētas tīkla) un spiediena mērītāju funkciju loģiku - starpprogrammatūru.

"EPANET Solver" modulis apstrādā mērījumu datus un veic ūdensvada tīkla diagnostiku (detalizētāks apraksts ir dots nākamā sadaļā).

Sākotnēji Smart Meter sistēma tika veidota, izmantojot Ventspils Digitālais centrs serveru infrastruktūru, bet projekta beigās SM sistēma tika pārvietota uz pašu datu centru, kas atrodas pansionāta "Selga" ēkā (sk. att. 5.23).



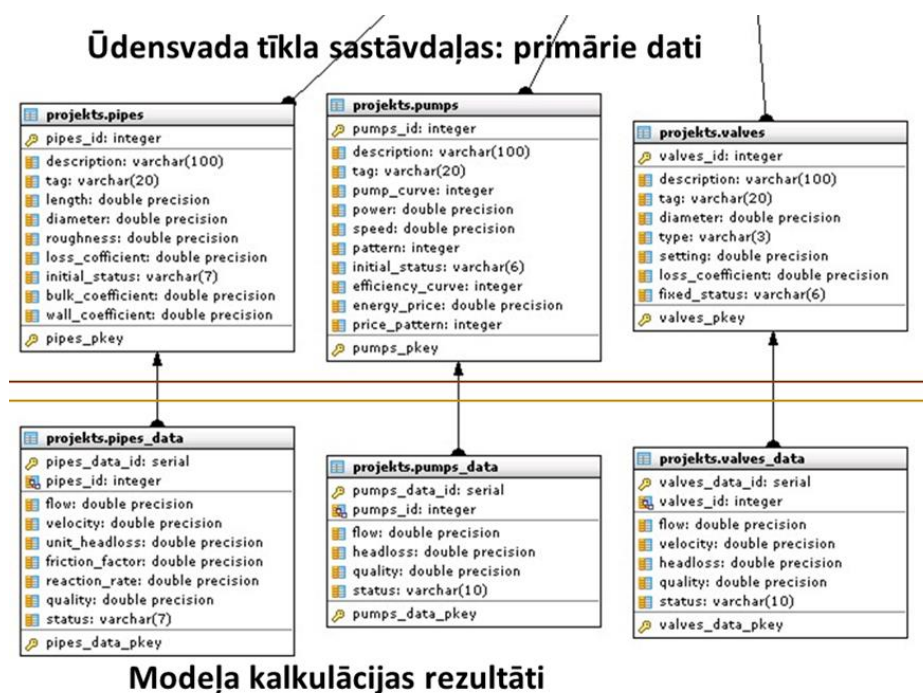
5.23.att. Smart Meter sistēmas serveris, kas tika izvietots pansionāta "Selga" ēkā

5.3.8. *Noplūžu meklēšanas metožu izpēte*

Plānojot projektu, tika izvērtētas piecas noplūžu konstatēšanas metodes, kas pēdējos gados ir apskatītas dažādos pētījumos [72, 34, 73], tomēr, ņemot vērā resursu trūkumu, tika nolemts veikt eksperimentus tikai ar divām pirmajām no piecām metodēm:

- Noplūžu imitācija ar ugunsdzēsības hidrantu.
- “Teorētiskais modelis plus Solver” imitācija (“Solver” ir noplūžu kalkulācijas modulis).
- Ģenētiskie algoritmi.
- Kalmana filtrs, kuru izmanto dažādās cauruļvadu noplūdes atklāšanas sistēmās.
- Neironu tīkli.

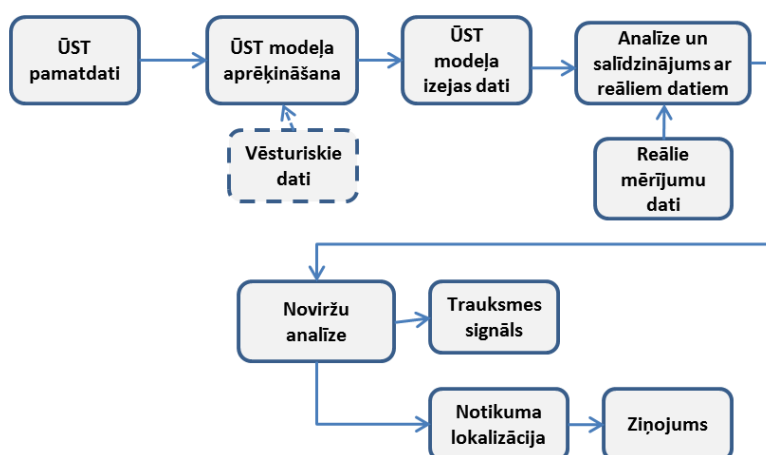
Visi ūdensvada tīkla cauruļvadi un citas tīkla sastāvdaļas tiek glabāti relāciju datu bāzes pārvaldības sistēmā (RDBMS), kas ir viegli paplašināma un kuru pārvalda, izmantojot SQL valodu. Tas ļauj veikt tīkla vizualizāciju un definēt Solver ievada modeli. MySQL izmantošana atvieglo noplūžu moduļa integrāciju ar Aquamet sistēmu (skat. 5.24. attēlu, kurā var redzēt daļu no RDMBS).



5.24. att. Daļa no RDMBS ar primārajiem datiem un kalkulācijas rezultātiem

Ūdensvada tīkls turpmākas paplašināšanas gadījumā var būt papildināts ar tīkla aktīvām sastāvdaļām, piemēram, ar attālināti vadājamiem vārstiem, sūkņiem un citām ierīcēm. Izstrādātais ūdensvada tīkla modelis turpmāk var būt izmantots pētījumiem saistībā ar ūdens kvalitātes monitoringu un piesārņojumu izplatīšanas modelēšanu.

Projekta komanda pētīja “*Teorētiskais modelis plus Solver*” imitācijas metodi (sk. 5.25. att.), kas parādīja labas perspektīvas, tomēr šīs metodes piemērošana prasa vēsturisko datu salīdzināšanu ar faktiskajiem mērījumiem. Tā kā vēsturiskie dati par ūdens spiedienu tīkla segmentos nav pieejami, tika nolemts šīs metodes tālāku izstrādi atlikt uz nākotnes projektiem.



5.25. att. “Teorētiskais modelis plus Solver” imitācijas metodes blokhēma

Lai vienkāršotu procesu noplūdes atklāšanu, tika izvēlēta jauna pieeja, kas prasa mazākas sistēmas uzturēšanas un uzstādīšanas izmaksas ne kā iepriekšēja metode. Šī ir kompromisa pieeja starp uzturēšanas un uzstādīšanas izmaksām (zemas jaudas sensoru barošanas akumulatori) un novēlotu noplūžu konstatēšanas laiku (datu saņemšana no spiediena devējiem atpalciek no reāla laika notikumiem).

Izveidotā metodika paredz izmantot četras ūdensvada tīkla notikumu analīzes metrikas (detektorus), kuras tika izstrādātas projektā:

- Spiediena vidējo fluktuāciju noplūžu detektors;
- Patēriņa minimuma plūsmas noplūžu detektors;
- Plūsmas vidējās fluktuācijas noplūžu detektors;
- Aparatūras dīkstāves detektors.

1. ***Spiediena vidējo fluktuāciju noplūžu detektors*** – rēķina spiediena vidējo aritmētisko vērtību noteiktajā periodā (slīdošais vidējais) un salīdzina to ar vērtību, kas rodas, aprēķinot spiediena vidējo aritmētisko vērtību no aktivizācijas perioda un sareizinot to ar procentuālo negatīvās fluktuācijas vērtību (100% + negatīvās fluktuācijas procents), tādējādi, ja iegūtā vērtība ir mazāka par spiediena vidējo vērtību noteiktajā periodā, tad Smart Metering sistēma signalizē noplūdi un tiek ģenerēts Smart Metering sistēmas notikums ar tipu – `pressure_leak`.
2. ***Patēriņa minimuma plūsmas noplūžu detektors*** – šim detektoram tiek norādīts diennakts laiks (dīkstāves patēriņa laika diapazons), pēc kura beigām nepieciešams veikt pārbaudi, ja vidējais patēriņš šajā norādītajā laika diapazonā pārsniedz minimālo dīkstāves patēriņa robežu un šāda situācija ir atkārtojusies jau tik dienas, cik norādīts aktivizācijas perioda laikā, tad pēc šī perioda beigām tiek ģenerēts Smart Metering sistēmas notikums ar tipu – `consumption_leak`;
3. ***Plūsmas vidējās fluktuācijas noplūžu detektors*** – šis detektors rēķina plūsmas vidējo aritmētisko vērtību no viduvējošanas perioda (slīdošais vidējais) un salīdzina to ar vērtību, kas rodas, aprēķinot plūsmas vidējo aritmētisko vērtību no aktivizācijas perioda un, sareizinot to ar procentuālo pozitīvās fluktuācijas vērtību, tādējādi, ja iegūtā vērtība ir lielāka par plūsmas vidējo vērtību pa viduvējošanas periodu, tad Smart Metering sistēma signalizē noplūdi, un tiek ģenerēts Smart Metering sistēmas notikums ar tipu – `meters_leak`

4. *Iekārtu dīkstāves perioda detektors* tiek aktivizēts periodiski reizi piecās minūtēs un detektora izpildes laikā tiek pārbaudīts, vai Smart Metering sistēmā esošās vārtejas, mērītāji un spiediena devēji ir saņēmuši datus definētā dīkstāves periodā, kuru kontrolē Smart Metering sistēma. Piemēram, ja dīkstāves periods ir uzstādīts uz 24 stundām, tad Smart Metering sistēmā *dīkstāves perioda detektors* pārbaudīs visu iekārtu pēdējo datu saņemšanas laiku un salīdzinās, vai šis laiks, kas pagājis, ir ilgāks par 24 stundām. Ja laiks, kas, pagājis kopš pēdējo datu saņemšanas, būs ilgāks par dīkstāves periodu, tad tiks ģenerēts jauns notikums atkarībā no iekārtas tipa – *gateway_disconnect* vai *meter_disconnect*.

Lai notestētu šo metodi, tika radītas mākslīgas ūdens noplūdes, izmantojot ugunsdzēsības hidrانتus divās attālinātās pozīcijās ar dažādām tīkla sarežģītības īpatnībām. Pirmais tests tika veikts, radot strauju noplūdi, otrais tests tika veikts, radot lēnu noplūdi – netika radīts trieciens.

Projekta ietvaros izstrādātā informācijas sistēmas reģistrēja sensoru – spiediena devēju rādījumus, to vērtības nodod ūdens noplūžu noteikšanas modulim, kas veica atbilstošās skaitļošanas operācijas.

Pēc testa veikšanas tika analizēti iegūtie spiediena izmaiņu rādījumi, lai pielāgotu noplūžu detektoru parametrus šādu noplūžu noteikšanai. Kopumā tika analizēti dati no 8 spiedienu mērītājiem.

Lēnas atvēršanas gadījums (skat. 5.26. att.).

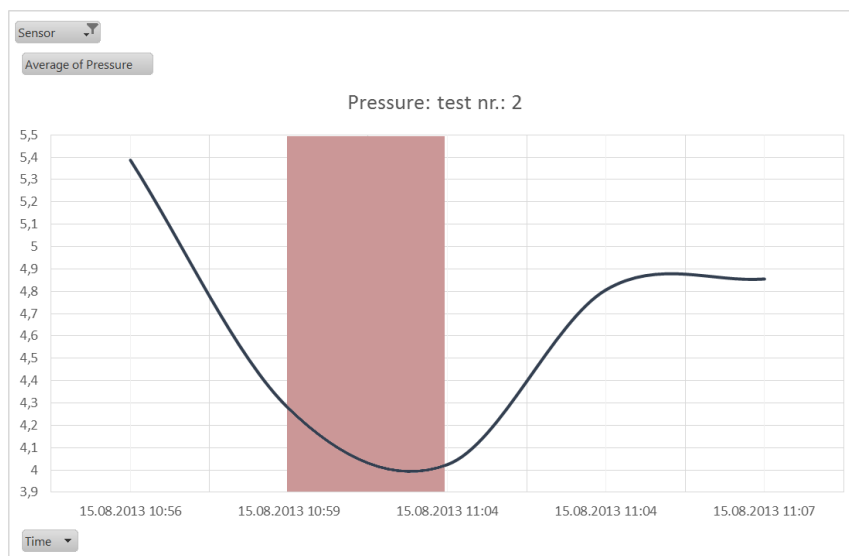
Datu atlase testa punkts nr.: 2 spiediena izmaiņas no datu bāzes:

```
SELECT (
(
(
`readouts`.value -186
) * `meters`.full_pressure_scale
) /744
), `readouts`.when, `meters`.number
FROM `readouts`
LEFT JOIN meters ON `readouts`.meter_id = `meters`.id
WHERE `readouts`.`when` < '2013:08:15 11:43:01'
AND `readouts`.`when` > '2013:08:15 10:55:03'
AND `programm_version` =12
LIMIT 0 , 30
```

Testa punkts nr.: 2 – lēna atvēršana

Sensor	00006B
Row Labels	Average of Pressure
15.08.2013 10:56	5,387096774
15.08.2013 10:59	4,274193548

15.08.2013 11:04	4,024193548
15.08.2013 11:04	4,806451613
15.08.2013 11:07	4,85483871
Grand Total	4,676523297



5.26. att. 2.tests: spiediena izmaiņas, kad hidrants tiek atvērts pakāpeniski (5. Pielikums)

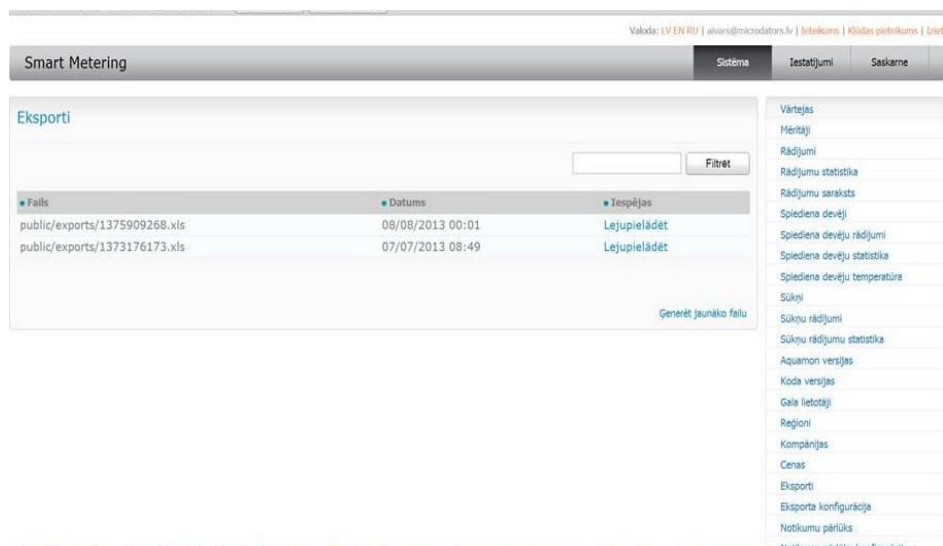
Noslēdzot testēšanu, tika secināts, ka pēc sākotnējo metriku parametru pielāgošanas noplūžu simulācija reālos apstākļos ģenerēja notikumus pārlūkā, tādējādi tiek uzskatīts, ka tests izpildīts veiksmīgi.

Metriku parametrizācija būtu jāautomatizē, ieviešot autonomus pašapmācības algoritmus. Šo funkciju var nodrošināt, kombinējot un papildinot integrēto EPANET Solveri, kas nodrošina tīkla analītisku modelēšanu, izmantojot tekošus un vēsturiskus tā stāvokļa datus.

5.3.9. E-pakalpojumi sistēmas lietotājiem

Atbilstoši projekta uzdevumam divi e-pakalpojumi ir izstrādāti Smart sistēmas lietotājiem:

- Mērīšanas datu eksportēšana no sistēmas Excel faila veidā. Klientu dati par ūdens patēriņu tiek izvēlēti un sagrupēti saskaņā ar iepriekš noteiktiem parametriem (skat. 5.27. attēlu). Rezultātā Ūdeka darbinieki un klienti ir atbrīvoti no manuālas ikmēneša procedūras, kuras mērķis ir vākt mērījumus no ūdens patēriņa skaitītājiem, lai nodrošinātu datu manuālu ievadi norēķinu sistēmā. Turklāt klientu nodaļa var pieprasīt patēriņa datus no sistēmas kā vienreizējo (“ad hock”) pieprasījumu.



5.27.att. Patēriņa datu eksports no sistēmas Excel faila veidā

- Otrs e-pakalpojums nodrošina iespēju sūtīt e-pastu Ūdeka darbiniekiem un klientiem par novirzēm no ierasta ūdens patēriņa. Novirzes robežvērtības lietotājs var definēt atkarīgi no patēriņa paradumiem un objekta nozīmīguma. Robežvērtības var pielāgot, pamatojoties uz lietotāja "reālās dzīves" pieredzi.

5.4. Secinājumi par piekto nodaļu

Šajā nodaļā pētījumā autors analizēja problēmas, ar kurām sastopas tehniskie speciālisti un pētnieki, kas ievieš praksē kritisko infrastruktūru datorvadības pārvaldības metodes, pielietojot bezvadu sensoru tīklus, un aprakstīja tehniskus risinājumus, kuri tiek izstrādāti apskatītos projektos. “Smart” projektā veiktie pētījumi deva šādus rezultātus:

- Ir izstrādāts bezvadu sensoru tīkla vārtejas prototips, kas papildus GSM-GPRS komunikācija kanālam ar centrālo sistēmu piedāvā Ethernet izeju uz bezvada 5.8 GHz tīklu.
- Ir izpētīta un notestēta ūdensvada spiediena mērījumu pārraidīšanas sistēma.
- Ir izgatavota un tiek izmēģināta uretāna apvalkā aizsargāta antena, kas tiek montēta akas vākā, un 868MNz sensors - raidītājs.
- Ir izveidots bezvadu sensoru uzliktais tīkls, kas tiek būvēts, pielietojot zvaigznes topoloģiju, apvienojot sensoru RF 868MHz tīklu ar Ethernet vārtejām (5.8 GHz).
- Vārtejas ierīcēs saziņai ar sensoru mezgliem un to funkcionalitātes kā interneta pakalpojumus “back-end” sistēmām tulkošanai tiek izmantota starpprogrammatūra.

- Piedāvāta tīkla konfigurācija ļāva efektīvi apvienot 14 sensorus-raidītājus, trīs vārtejas, divus RF atkārtotājus un SCADA aparāturu, un integrēt esošā pašvaldības Wi-Fi tīklā, kas pārklāj pilsētas teritoriju.
- Smart Meter sistēma, izveidota un notestēta projektā, sastāv no četriem bāzes komponentiem:
 - Mērītāju datu saņemšanas komponente;
 - Uzraudzības, statistikas un datu vizualizācijas saskarne;
 - Klientu patēriņa statistika uzskaitē un norēķiniem;
 - Noplūžu atklāšanas komponente.
- Ir izpētītas ūdens noplūžu atrašanas metodes un izstrādāta un notestēta ekonomiskā metode, kas ar četru noplūžu detektoru pielietošanu ļauj lokalizēt potenciālu noplūdes atrašanas vietu.
- Viens no projekta nodevumiem ir “The Technology Research and Accommodation Program on Smart Meter Application” [90].

DARBA KOPĒJIE SECINĀJUMI

- ❖ Balstoties uz *datu pieejamības un granularitātes pieeju*, analizēta modelēšanas metožu izmantošana saistībā ar infrastruktūru savstarpējas mijiedarbības veidiem, un ir pierādīts, ka pakalpojumu dekompozīcijas modelis var būt veiksmīgi izmantots, pielietojot datu pieejamības un granularitātes pieeju.
- ❖ Izpētīts pakalpojumu dekompozīcijas modelis KI mijiedarbības modelēšanai četros etapos reālā scenārijā nelielā Latvijas pilsētas teritorijā, kurā ar UML rīkiem tika izveidots PIM modelis un tika aprobētas uz riska novērtēšanu balstītās metrikas. Atšķirībā no eksistējošiem modeļiem, šis scenārijs ļauj izpētīt pilsētas ūdensapgādes tīkla (Talsi Ūdens), pakalpojumu atkarību no elektroenerģijas piegādātāja (Latvenergo) un telekomunikāciju pakalpojumu sniedzēja (GSM operators) pakalpojumiem.
- ❖ Analizētās un klasificētās kritisko infrastruktūru mijiedarbības kvalitatīvi un kvantitatīvi raksturojušas metrikas un ir pierādīts, ka:
 - ✓ metrikas var klasificēt un apkopot matricā saistībā ar savstarpējās atkarības veidiem, piemēram, *Fiziskās atkarības koeficients*, *Kibernētiskās atkarības koeficients*, *Fiziskās atkarības relatīvais ilgums*, *Tīkla topoloģiskais robustums* u.c.;
 - ✓ metriku praktiskai izmantošanai jānosaka parametru pielietošanas kritiskās robežas, jo var pieļaut, ka metrikas konkrētie parametri ir pamatoti tikai noteiktās robežās.
- ❖ Izmantojot *MatLab*[®] *Simulink*[®] *StateFlow* imitācijas modeli, darbā ir izstrādāta un eksperimentāli pārbaudīta metode, kura atšķirībā no eksistējošajām metodēm, ļauj izpētīt ūdens apgādes tīkla mezglu vidēja dīkstāves laika atkarību no rezerves barošanas avota darbības laika un rezerves barošanas avota nomainīšanas laika savstarpējās korelācijas noteikto parametru robežās, apstākļos, kad notiek elektroapgādes un telekomunikācijas tīkla dīkstāves. Ir pierādīts, ka:
 - ✓ ūdens apgādes mezglu vidējais dīkstāves laiks demonstrē ar kvadrātisko polinomu aprakstīto atkarību no rezerves barošanas avota darbības laika (RBDL) un rezerves barošanas avota nomainīšanas laika (RBNL) savstarpējās korelācijas noteikto parametru robežās;
 - ✓ lai gan aproksimācijas grafiki rāda, ka izpētītu parametru robežās polinomiāla funkcija tiecas uz minimumu tad, kad RBDL tiecas uz maksimumu, tomēr analīze atklāj arī funkcijas lokālus minimumus, kas ir saistīti ar telekomunikācijas tīkla mezglu noturību pret ārējas elektroapgādes pārtraukumiem;
 - ✓ rezerves elektrobarošanas avotu izmantošana ūdensvada tīkla mezglos ir efektīvs risinājums, ņemot vērā samērīgās izmaksas, tomēr tas nav pietiekošs, lai nodrošinātu

nepārtrauktu un drošu datu savākšanu no objektiem, jo *fiziskās atkarības koeficients* ir 0.77, bet *laika mērogā fiziskās atkarības koeficients* ir 0.67;

- ✓ risinājumi, kas nodrošinātu nepārtrauktu un drošu datu savākšanu no ūdensapgādes tīkla objektiem, var būt:
 - rezerves barošanas avota darbības laika palielināšana;
 - papildus (“redundant”) tīkla mezglu izveidošana, šādā veidā palienot sensoru tīkla robustumu.
- ❖ Izpētot tehniskus risinājumus un tehnoloģijas, ar kurām tiek kontrolēts ūdens apgādes tīkla mezglu stāvoklis, izmantojot bezvada sensoru tīklus, ir izstrādāts un eksperimentāli pārbaudīts:
 - ✓ bezvadu sensoru tīkla vārtejas prototips, kas papildus GSM-GPRS komunikācijas kanālam ar centrālo sistēmu piedāvā Ethernet izeju uz bezvada 5.8GHz tīklu;
 - ✓ ūdensapgādes tīkla spiediena mērījumu datu pārraidīšanas sistēma, kas, atšķirībā no eksistējošiem modeļiem, iekļauj uretāna apvalkā aizsargātu antenu, kuru montē akas vākā, un 868MHz sensoru – raidītāju;
 - ✓ bezvadu sensoru uzliktais tīkls, kas tiek būvēts, pielietot zvaigznes topoloģiju, apvienojot RF 868MHz sensorus, Ethernet vārtejās (5.8GHz), RF atkārtotājus un SCADA aparāturu, un kas tiek integrēts esošā pašvaldības Wi-Fi tīklā, kas pārklāj pilsētas teritoriju.
 - ✓ “Smart Meter” sistēma, kas sastāv no četriem bāzes komponentiem: Mērītāju datu saņemšanas komponente; Uzraudzības, statistikas un datu vizualizācijas saskarne; Klientu patēriņa statistika uzskaitē un norēķiniem un Noplūžu atklāšanas komponente;
 - ✓ ūdens noplūžu atrašanas ekonomiskā metode, kura, atšķirībā no eksistējošajām metodēm, ļauj ar četru noplūžu detektoru pielietošanu lokalizēt potenciālu noplūdes atrašanas vietu.
- ❖ Turpmāks pētījuma virziens ir saistīts ar bezvada tīkla elementu attīstību ūdensapgādes infrastruktūras tīkla datorvadībai:
 - ✓ Modulārās vārtejas sakaru interfeisu moduļu izstrāde (GSM/GPRS - mobilie platjoslas pieslēgumi, CAN, Ethernet, 802.11b/g)
 - ✓ Pazeminātas temperatūras un paaugstināta mitruma ietekme uz bezvada tīkla elementiem, tai skaitā uz sensoriem-raidītājiem, uzstādītiem akās.

IZMANTOTA LITERATŪRA

1. Aviles-Lopez E. and Garcia-Macias J., "TinySOA: a service-oriented architecture for wireless sensor networks," Service Oriented Computing and Applications, vol. SOCA (2009) 3, pp. 99–108, 2009, Springer-Verlag London Limited;
2. Aubert J., Schaberreiter T., Incoul C., Khadraoui, D.; Gateau, B., "Risk-Based Methodology for Real-Time Security Monitoring of Interdependent Services in Critical Infrastructures," Availability, Reliability, and Security, 2010. ARES '10 International Conference, vol., no., pp.262-267, 15-18 Feb. 2010.
3. Aubert J., Schaberreiter T., Incoul C., and Khadraoui D., "Real-time security monitoring of interdependent services in critical infrastructures. Case study of a risk-based approach," in 21th European Safety and Reliability Conference (ESREL2010), September 2010, p.1-8.
4. Avižienis A., Laprie J., Randell B., Landwehr C., "Basic Concept and Taxonomy of Dependable and Secure Computing", IEE Transactions on Dependable and Secure Computing, Vol.1, No. 1, pp.1-33, 2004.
5. Aquamet HeatMet manual, Riga Heat Project, Micro Dators ltd., IT House / ITH Group, unpublished, 2009, pp.1-32.
6. Barisic D., Krogmann M., Stromberg G., Schramm P., Making Embedded Software Development More Efficient with SOA, 21st International Conference on Advanced Information Networking and Applications Workshops (AINAW'07), 2007, IEEE, Computer Society, pp.1-6.
7. Bagheri E., Ghorbani A., Towards an MDA-Oriented UML Profile for Critical Infrastructure Modeling, Proceedings of the 2006 International Conference on Privacy, Security and Trust: Bridge the Gap Between PST Technologies and Business Services, PST 2006, Canada, 2006, pp.1-1212.
8. Bellifemine F., Poggi A., Rimassa G., Developin Multi-agent Systems with JADE, Lecture Notes in Computer Science, Volume 1986, 2001.
9. Briedis J., Pētījums un pamatojums naturālo resursu patēriņa uzskaites un kontroles sistēmas izveidei, Latvijas – Lietuvas pārrobežu programmas projekts "Inovatīvi e-pakalpojumi ūdens apgādes vadībai", LLIII-127 E-Water, Ventspils Augsto Tehnoloģiju Parks, 2010. gads, lpp.1-94.
10. Bologna S., Setola R., and Tucci S., —Critical Information Infrastructure Protection, The European Journal for the Informatics Professional, UPENET (UPGRADE European NETwork), 7, n. 5, October 2006, pp. 59 – 67, <http://www.upgrade-cepis.org>.
11. Brown T., Beyeler W., and Barton D., Assessing Infrastructure Interdependencies: The Challenge of Risk Analysis for Complex Adaptive Systems, Int. J. Critical Infrastructures, Vol. 1, No. 1, 2004.
12. Brasca C.L., Ciapessoni E., "Coupling identification and measurement methodologies at the service level" MIA project, Activity 3 Report, 2010, pp.1-125.
13. Buschi S., Casalicchio E., Gazzini A., Holt M., "Project MIA, Definition of a methodology for the assessment of mutual interdependencies between ICT and electricity generation / transmission infrastructures", EU JLS/2007/CIPS/019-MIA, 2010 1-147.
14. Buschi S., Casalicchio E., Brasca C., Ciapessoni E., D'Agostino G., Fioriti V., "Definition of a Metric for ICT-PS infrastructures", MIA Activity 4 Report (2010), pp.1-147.

15. Business Dictionary, sasniegts 2014. gada martā,
<http://www.businessdictionary.com/definition/metrics.html#ixzz2xdou5x7U>
16. Casalicchio E., and Galli E., “Metrics for Quantifying Interdependencies”, Second IFIP WG 11.10 International Conference on Critical Infrastructure Protection, George Mason University, Arlington, VA, USA, March 2008, pp. 1-8.
17. Ciancamerla E., Minichino M., Interdependency modelling framework, indicators and models - final report, Tool for systemic risk analysis and secure mediation of data exchanged across linked CI information infrastructures, Project MICIE, ENEA, December 31, 2010, pp. 1-170.
18. Communication from the Commission to the European Parliament, the Council - ICT infrastructures for e-science, COM(2009) 108 final. http://cordis.europa.eu/fp7/ict/e-infrastructure/home_en.html.
19. Cyber war in estonia. http://news.cnet.com/8301-17938_105-9721429-1.html
20. Daemon Tools, http://www.filehippo.com/download_daemon_tools/, apskatīts 2014. gada februārī.
21. David W., Hilt P.E., August 14, 2003, Northeast blackout impacts and actions and the energy policy act of 2005. Technical report, North American Electric Reliability Council.
22. D3.1.2 Refined interdependency metrics and indexes for risk prediction formulation – final version”, Project MICIE, FP7, STREP, 22/06/2010, PP.1-186.
23. De Porcellinis S., Oliva G., Panzieri S. and Setola R., “A Holistic Reductionistic Approach for Modeling Interdependencies”, Critical Infrastructure Protection III, C. Palmer and S. Sheno (Eds.), vol. 311/2009, pp. 215-227, Springer AICT, Vol. 311, 2009.
24. De Porcellinis S., Panzieri S., Setola R., and Ulivi G., Simulation of Heterogeneous and Interdependent Critical Infrastructures, Int. J. Critical Infrastructures (IJCIS), vol. 4, n. 1/2, pp. 110 – 128, 2008.
25. DPWS, Devices Profile for Web Services Version 1.1, OASIS Std., February 2011, <http://docs.oasis-open.org/ws-dd/dpws/1.1/os/wsdd-dpws-1.1-spec-os.pdf>
26. EU project DIESIS (Design of an Interoperable European federated Simulation network for critical InfraStructures) <http://www.diesis-project.eu/>.
27. Eiropas Padomes Direktīva 2008/114/EK (2008. gada 8. decembris) par to, lai apzinātu un noteiktu Eiropas Kritiskās infrastruktūras un novērtētu vajadzību uzlabot to aizsardzību, lpp. 1-8.
28. “ES Communication on Critical Information Infrastructure Protection”, COM(2009) 149 final, Brussels, 30.3.2009, pp.1-12
29. Executive Office of the President, The national plan for research and development in support of critical infrastructure protection, The White House, Washington, DC, 2005, pp.1-97.
30. Fiority V. et al., Methodologies for Interdependency Assessment, EU JLS/2007/CIPS/019-MIA, The Mia Final Report, September 2010, pp.1-67.
31. Galli E., Agent Based Modeling and Simulation for critical and interdependent systems Course, PhD Thesis, Specialty: Computer Science, XXII A.A. 2009/2010, pp. 1-179.
32. Haimes Y.Y. and Jiang P.. Leontief-based Model of Risk in Complex Interconnected Infrastructures. Journal of Infrastructure Systems, pages 1-12, 2001.

33. Harper, M.A.; Thornton, M.A.; Szygenda, S.A, Disaster Tolerant Systems Engineering for Critical Infrastructure Protection, Systems Conference, 2007 1st Annual IEEE, IEEE Xplore, pp. 1-7;
34. Hunaidi O., Wang A. A New system for locating leaks in urban water distribution pipes. International Journal of Management of Environmental Quality, 17, (4), 2006. p. 450-466.
35. ISO 15408-1:2005 2005, "Information technology Security techniques, Evaluation criteria for IT security", 2005, pp.1-178. 12
36. Investopedia, sasniegts 2014. gada martā, <http://www.investopedia.com/terms/m/metrics.asp>
37. Jansson O., Arrowhead, DELIVERABLE D4.2 of Work Package 4: plan and specification for the generation 1 demonstrations, ARTEMIS, Arrowhead project, pp.1-38 82
38. Kaškina B. (2012). "Dealing with the whole country: creating a National CSIRT", 35th TF-CSIRT and FIRST meeting 31st January 2012, Rome, Italy, pp. 1-30, www.cert.lv.
39. Kurant M. and Thiran P., Layered complex networks, Phys. Rev. Lett., Vol. 96, p. /0510151, 2006.
40. Kutjuns A., Krishans Z., "Method of transmission power networks reliability estimation", 7th WSEAS International Conference on Electric Power Systems, High Voltages, Electric Machines, Venice, Italy, November 21-23, 2007, pp. 1-5
41. Krišāns A., Oļeiņikova I., Mutule A., Kalpiņa A., Cities medium voltage safety evaluation method and algorithm, Latvian Journal of Physics and Technical Sciences 2007, N 3, pp.1-13.
42. Kuņicina N., Programmu aģentu modelēšanas metožu izstrāde elektropiegādes un transporta loģistikas sistēmās, Promocijas darbs, Transporta datorvadības, informācijas un elektroniskās sistēmas programmas, 2004, lpp. 1-134.
43. Lauenburg P., "Improved supply of district heat to hydronic space heating systems," Ph.D. dissertation, Dept. och Energy Sciences, Lund University, P.O Box 118, SE-22100, Lund, December 2009.
44. Liting Cao, Jingwen Tian and Yanxia Liu, Remote Real Time Automatic Meter Reading System Based on Wireless Sensor Networks, Beijing Union University, The 3rd International Conference on Innovative Computing Information and Control (ICICIC'08), 2008, p.1-3.
45. Lin J., Sedigh S., and Miller A., Modeling Cyber-Physical Systems with Semantic Agents, 34th Annual IEEE Computer Software and Applications Conference Workshops (COMPSACW 2010), 2010, pp.13-18.
46. Manchester Coding Basics Application Note, ATMEL, 9164A-AUTO-09/09, lpp.1028, <http://www.nesweb.ch/downloads/doc9164.pdf>, apskatīts 2014. gada februārī.
47. Masucci V., Adinolfi F., Servillo P., Dipoppa G, and Tofani A., Ontology-based critical infrastructure modeling and simulation. Critical Infrastructure Protection III, pages 229 – 242, 2009.
48. Martii J., Ventura C., J. Hollman J., Srivastava K., and H. Juárez. I2Sim modelling and simulation framework for scenario development, training, and real-time decision support of multiple interdependent critical infrastructures during large emergencies. Technical report, The University of British Columbia, 2008. ix.
49. Mazzy Aquamet software operation manual, (2009), Micro Dators ltd., IT Hous/ ITH Group, p.1-52.

50. North M., Collier N., and Vos J., Experiences creating three implementations of the Repast agent modeling toolkit, *ACM Transactions on Modeling and Computer Simulation (TOMACS)*, Vol. 16, Issue 1, 2006.
51. Oliva G., Panzieri S., Setola R., Agent-based input–output interdependency model, Elsevier, *International Journal of Critical Infrastructure Protection*, 3 (2010), pp.76-82;
52. Ouyang M., Hong L., Mao Z.-J, Ming-Hui Yu, Fei Qi, *Simulation Modeling Practice and Theory*, Elsevier, *Simulation Modeling Practice and Theory* 17 (2009), pp. 817–828.
53. “OMG Model Driven Architecture”, [Online]. Available: <http://www.omg.org/mda> [Accessed: January 21, 2014]
54. “OMG Unified Modeling Language”, [Online]. Available: <http://www.uml.org> [Accessed: January 21 2014].
55. Newman, D.E., Nkei, B., Carreras, B.A., Dobson, I., Lynch, V.E. and Gradney, P. Risk assessment in complex interacting infrastructure systems, HICSS '05, Proceedings of the 38th Annual Hawaii International Conference on System Sciences, IEEE Press, 3–6 January, p.63, 2005.
56. Pederson P., Dudenhoefter D., Hartley S., and Permann M., Critical infrastructure and interdependency modeling: A survey of US and international research. In Idaho National Laboratory, 2006
57. Pētījums un pamatojums naturālo resursu patēriņa uzskaites un kontroles sistēmas izveidei, Latvijas – Lietuvas pārrobežu programmas projekts “Inovātīvi e-pakalpojumi ūdens apgādes vadībai”, LLIII-127 E-Water, WP 2, 2011, lpp.1-94. <http://kraslava.lv/zinas/pilnsraksts/article/projekts-inovativ-e-pakalpojumi-udens-apgades-vadibai-tuvojas-noslegumam/>.
58. Polycarpou M., IntelliCIS COST Action ICO806, Limassol, Cyprus, September 2009, p.1-5;
59. Projekts „Talsu novada datorizētas ūdenssaimniecības vadības kontroles sistēmas paplašināšana - piegāde un uzstādīšana”, Identifikācijas Nr. TNP 40/10.
60. RFM 22B Datasheet, <https://www.sparkfun.com/datasheets/Wireless/General/RFM22B.pdf>, apskatīts 2014. gada februārī.
61. Rinaldi S. M., Modeling and Simulating Critical Infrastructures and Their Interdependencies, Proceedings of the 37th Hawaii International Conference on System Sciences, 2004, pp.1-8.
62. Rinaldi S. M., “Modeling and simulating critical infrastructures and their interdependencies”. In HICSS '04: Proceedings of the Proceedings of the 37th Annual Hawaii International Conference on System Sciences (HICSS'04) - Track 2, Washington, 2005, 4.1. IEEE Computer Society, pp.1-8.
63. Rinaldi S. M., Peerenboom J.P., and Kelly T.K., 2001. Critical infrastructure interdependencies. *IEEE Control Systems Magazine*. December, Volume 21, issue 6.
64. Rome E., Bologna S., Gelenb E., Luijff E, and Masucci V., Design of an interoperable European federated simulation network for critical infrastructures (DIESIS). 2009. ix.
65. Rosato V., D' Agostino G., “Determination of the topological properties of network structure and nature of interdependency couplings”, MIA Activity 2 Report (2009), pp.1-55.
66. „Sadales Tīkls” AS 2011. gada darbības pārskats, http://www.st.latvenergo.lv/files/newnode/parskati/ST_gada_parskats_2011.pdf
67. Su W., Akyildiz I., Sankarasubramaniam Y., E. Cayirci, Wireless sensor networks: a survey, 2002, *Computer Networks* 38 (2002) 393–422.

68. Satumtira G., and Dueñas-Osorio L., *Synthesis of Modeling and Simulation Methods on Critical Infrastructure Interdependencies Research*, (2010), *Sustainable Infrastructure Systems: Simulation, Imaging, and Intelligent Engineering*", York: Springer-Verlag, pp.1-51.
69. Schaberreiter T., Bonhomme C., Aubert J., Incoul C. and Khadraoui D., "Support tool development for real-time risk prediction in interdependent critical infrastructures service", *International Workshop on Risk and Trust in Extended Enterprises (RTEE'2010)*, San Jose, California – USA, November 1-4, 2010. (ISSN proceeding: 0929-0672), pp.1-8
70. Setola R. and De Porcellinis S., —A Methodology to Estimate Input-output Inoperability Model Parameters, *Critical Information Infrastructures Security 2007*, *Lecture Notes in Computer Science*, Springer-Verlag, Berlin, pp. 149 – 160, 2008.
71. Setolaa R., De Porcellinisa S., Sforma M., "Critical infrastructure dependency assessment using the input–output inoperability model", *International Journal of Critical Infrastructure Protection* 2 (2009), pp. 170 – 178, 2009.
72. Stoianov I., Nachman L., and Madden S. PIPENET: A Wireless Sensor Network for Pipeline Monitoring Proceeding of IPSN '07 Proceedings of the 6th international conference on Information processing in sensor networks, ACM New York, 2007. p. 264-273.
73. Savic D., Bicik J, Morley M., Duncan A., Z. Kapelan, S. Djordjevic and E. C. Keedwell, „Intelligent Urban Water Infrastructure Management”, *Journal of the Indian Institute of Science A Multidisciplinary Reviews Journal*, VOL 93:2 Apr.–Jun. 2013, pp.1-18
74. StarUML - The Open Source UML/MDA Platform, [Online]. Available: <http://staruml.sourceforge.net/en/download.php>, [Accessed: January 21, 2014]
75. Yick J., Mukherjee B., Ghosal D., *Wireless sensor networks: a survey*, *Computer Networks* 52 (2008), pp. 2292–2330.
76. The IRRIS European Integrated Project: www.irriis.org/
77. Usov Andrij and Beyel Césaire, *Simulating interdependent critical infrastructures with SimCIP*, 2008. ix.
78. Zimmerman R., "Decision-making and the vulnerability of interdependent critical infrastructure". *IEEE International Conference on Systems, Man and Cybernetics*, 5, October 2004. 4059–4063.
79. Zimmerman R. and Restrepo C.E., "The next step: quantifying infrastructure interdependencies to improve security", *International Journal of Critical Infrastructures (IJCIS)*, 2006.
80. Wilson C., *Computer attack and cyberterrorism: Vulnerabilities and policy issues for congress*. Technical report, CRS Report for Congress, 2005.
81. Zabašta A., Juhna T., Tihomirova K., Rubulis J, Ribickis L., „Latvian Practices for Protecting Water and Wastewater Infrastructure”, R. M.Clark, S.Hakim, *Securing Water and Wastewater Systems, Global Experiences*", Springer, 2014, lpp.315-342.
82. Zabasta A., Kunicina N., *Approach for Monitoring and Measurement of Interdependent Services in Critical Infrastructures*, *Proceeding of the 11th International Symposium, Faculty of Power Engendering, Tallin University of Technology, Pärnu, Estonia*, 2012, pp.51-56.
83. Zabasta A., Nikiforova O., Kunicina N., "A Risk Based Modeling of Interdependencies in Critical Infrastructures through UML", *53rd International Scientific Conference of Riga Technical University (RTUCON2012)*, Riga Technical University, 2012, pp.1-6.

84. Zabasta A., Nikiforova O., Kunicina N., “Application of UML for Risk Based Interdependencies Modelling in Critical Infrastructures”, The 6th International Conference on Integrated Modeling and Analysis in Applied Control and Automation” IMAACA 2012 - DHSS 2012 workshop, pp.1-6. IEEE Xplore, Proceedings of the International Defence and Homeland Security Simulation Workshop 2012, p.1-6.
85. Zabasta A., Kunicina N., Chaiko Y., Ribickis L., “Automatic Meters Reading for Water Distribution Network in Talsi City”, in proceeding of EUROCON 2011, 27-29 April 2011, Lisbon, Portugal, 2011, pp.1-6.
86. Zabašta A., Kuldīgas novada komunālo pakalpojumu pārvaldes sistēmas priekšizpēte un modeļa izstrāde, izmantojot informācijas un komunikāciju tehnoloģiju (IKT) risinājumus”, http://www.kurzemesregions.lv/wp-content/uploads/2010/12/3.2. kuldiga_novads_modelis_17.05.10.pdf
87. Zabasta A., Kunicina N., Chaiko Y., Ribickis L., Automatic Meters Reading for Water Distribution Network in Talsi City, in proceeding of EUROCON 2011, 27-29 April 2011, Lisbon, Portugal, IEEE, Instituto Superior Tecnico, Instituto de Telecomunicacoes.
88. Zabašta A., Dambrauskas V., Deksnis J., Deksnis V., et al., Proceeding of the Project (LLIV-312) „Smart Metering”, Engineering Research Institute, Ventspils International Radio Astronomy Centre of Ventspils University College, 2013, pp.1-110.
89. Zabasta A., Casaliccio E., Kunicina N., Interdependencies impact on sustainable water infrastructure services, 3rd International Exergy, Life Cycle Assessment, and Sustainability Workshop & Symposium (ELCAS-3), 07 – 09 July, 2013, NISYROS – GREECE, lpp.661-670
90. Zabašta A., Kondratjevs K., Nolendorfs A., Kuņicina N., et al, The Technology Research and Accommodation Program on Smart Meter Application in Water, Heat and Other Areas, Project “Smart Metering” LLIV-312, 2013, lpp.1-131, <http://www.smartmeteringproject.eu/lv/lejupielades/>
91. Zabašta A., Riekstiņa L., Kunicina N., Deksnys V., et al., Research of existing technologies and products – Problems and technology assessment report, Project “Smart Metering” LLIV-312, Ventspils University College, Kaunas University of Technology, Latvian Internet Association August 2012, lpp.1-107, <http://www.smartmeteringproject.eu/lv/lejupielades/>

PIELIKUMI

- 1. Pielikums:** Konferenču un semināru saraksts, kuros notika pētījumu prezentācija
- 2. Pielikums:** Detalizētie dati par Talsu un Ventspils sadales tīklu iecirkņos plānotām un neplānotām dīkstāvēm 2011. gadā.
- 3. Pielikums:** Ūdens sadales tīkla, elektroapgādes un telekomunikācijas tīkla mijiedarbības simulācijas rezultāti.
- 4. Pielikums:** “Smart Metering” sistēmas testēšanas atskaite 1.sadaļa. Mērījumu reģistrēšana, pārraide un apstrādes tests Projekts “Smart Metering” LLIV-312
- 5. Pielikums:** „Smart Metering” sistēmas testēšanas atskaite 2.sadaļa. Ūdens noplūžu vietu lokalizācijas tests Projekts “Smart Metering” LLIV-312

1.Pielikums: Konferenču un semināru saraksts, kuros notika pētījumu prezentācija

Darba rezultāti tika prezentēti un apspriesti šādās starptautiskās zinātniskās konferencēs un semināros:

1. A.Zabasta, N. Kunicina, Y. Chaiko, L. Ribickis, “Automatic Meters Reading for Water Distribution Network in Talsi City”, EUROCON 2011, Lisbon, Portugal, 2011. g. 27–29. aprīlī.
2. A.Zabašta, N.Kunicina, “Approach for Monitoring and Measurement of Interdependent Services in Critical Infrastructures”, Konference “Topical Problems in the Field of Electrical and Power Engineering” and “Doctoral School of Energy and Geotechnology II, Pērnavā, Igaunijā, 2012. g. 16 - 20. janvārī.
3. A. Zabašta, V. Šeļmanovs-Plešs, N. Kuņicina, “Wireless Sensor Networks Application at Water Distribution Networks in Latvia”, The 7th International Conference on Electrical and Control Technologies ECT 2012, Lietuva, Kaunas, 2012. g. 3-4. maijā,
4. A.Zabasta, O.Nikiforova, N.Kunicina, “A Risk Based Modeling of Interdependencies in Critical Infrastructures through UML”, 53rd International Scientific Conference of Riga Technical University (RTUCON2012), 2012. g. 13-15. oktobrī.
5. A.Zabasta, O.Nikiforova, N.Kunicina, “Application of UML for Risk Based Interdependencies Modelling in Critical Infrastructures”, The 6th International Conference on Integrated Modeling and Analysis in Applied Control and Automation” IMAACA 2012 - DHSS 2012, 2012. g. 19-21. septembrī.
6. N. Kunicina, A.Zabasta, A. Zhiravecka, A.Galkina, J.Soboleva, A.Patlins, „Embedded Systems for Emergency Situations in Automated Manufacturing of Wooden Briquettes”, The 15th International Conference on Mechatronics – Mechatronika 2012, 5-7. decembrī, Prāgā, Čehijā.
7. N. Kunicina, A.Zabasta, J. Soboleva, „Control System Development for Emergency Situations in Automated Manufacturing Line of Wooden Briquettes”, The 9-th International Conference Mechatronic Systems and Materials (MSM 2013), 1-3. jūlijs 2013, Viļņa, Lietuva.
8. A.Zabasta, E.Casaliccio, N.Kunicina, Interdependencies impact on sustainable water infrastructure services, 3rd International Exergy, Life Cycle Assessment, and Sustainability Workshop & Symposium (ELCAS-3), 07 – 09. jūlijā, 2013, NISYROS – GREECE.
9. A.Zabašta, V.Dambrauskas, J.Deksnis, V.Deksnis, I.Gudele, K.Kondratjevs, A.Kriaučeliūnas, N.Kuņicina, K.Navalinskaite, A.Nolendorfs, V.Šeļmanovs-Plešs, Final Conference of the Project LLIV-312 “Smart Metering for Saving of Heat and Water Resources”, Proceeding of the Project „Smart Metering”, Engineering Research Institute, Ventspils International Radio Astronomy Centre of Ventspils University College, 2013.

2.Pielikums. Detalizētie dati par Talsu un Ventspils sadales tīklu iecirkņos plānotām un neplānotām dikstāvēm 2011. gadā.

2.1. Neplānotās dikstāves 2011. g.

Gads	Ekspluatācijas rajons	Mē-ness	Spriegu- ma līmen.	SAIFI	SAIDI (min)	CAIDI (min)
2011	Talsi	1	4	0.000267	0.1046772	392.049929
2011	Talsi	1	20	0.010099	0.6053689	59.94203213
2011	Talsi	1	4	0.000449	0.141201	314.1328734
2011	Talsi	1	20	0.001158	0.0632727	54.64448001
2011	Talsi	2	4	0.0011	0.4576002	415.8632462
2011	Talsi	2	20	0.014367	1.0698503	74.46716547
2011	Talsi	3	4	0.000779	0.1950107	250.4876815
2011	Talsi	3	20	0.005352	0.2040659	38.13118613
2011	Talsi	4	4	0.000742	0.3498886	471.7604964
2011	Talsi	4	20	0.009454	1.8976979	200.7346027
2011	Talsi	4	4	0.000854	0.1548209	181.2807965
2011	Talsi	4	20	0.003576	0.0546102	15.27055072
2011	Talsi	5	4	0.00089	0.1541264	173.1759204
2011	Talsi	5	20	0.006391	0.3647253	57.06937808
2011	Talsi	6	2	4.49E-06	0.0003996	88.89888689
2011	Talsi	6	4	0.000685	0.2066497	301.6654762
2011	Talsi	6	20	0.010357	0.611093	59.00147546
2011	Talsi	7	2	8.99E-07	0.0002172	241.6350063
2011	Talsi	7	4	0.001128	0.2058579	182.4608385
2011	Talsi	7	20	0.006274	0.166897	26.60119216
2011	Talsi	8	4	0.000875	0.1625099	185.7858473
2011	Talsi	8	20	0.004401	0.3105644	70.55957749
2011	Talsi	9	4	0.001834	0.3745385	204.2264586
2011	Talsi	9	20	0.027014	2.8400197	105.1325205
2011	Talsi	9	110	0.015006	2.6474288	176.4256273
2011	Talsi	10	4	0.000624	0.082509	132.2474698
2011	Talsi	10	20	0.00749	0.3489648	46.58842795
2011	Talsi	11	4	0.000524	0.1371405	261.6633334
2011	Talsi	11	20	0.008375	0.7705362	92.0045578
2011	Talsi	11	4	0.000405	0.11641	287.1174472
2011	Talsi	11	20	0.006531	0.2936695	44.96442074
2011	Talsi	12	4	0.001533	0.4128538	269.3504017
2011	Talsi	12	20	0.015783	1.8335911	116.1776758
2011	Talsi	12	4	0.001409	0.2726575	193.5504943
2011	Talsi	12	20	0.008054	0.099796	12.39080606
		35		0.173785	17.71122	5797.45828
2011	Ventspils	1	4	0.000387	0.3814321	984.4320772
2011	Ventspils	1	20	0.00928	1.6953	182.6780596
2011	Ventspils	1	1	2.7E-05	0.0186377	691.0617876
2011	Ventspils	1	4	0.000225	0.0650534	289.4513764
2011	Ventspils	1	20	0.001209	0.0615503	50.90421817
2011	Ventspils	2	1	1.35E-05	0.0125991	934.3131374

2011	Ventspils	2	4	0.000293	0.1318799	449.993948
2011	Ventspils	2	10	6.29E-06	0.000773	122.8397178
2011	Ventspils	2	20	0.005391	0.5041396	93.51095153
2011	Ventspils	3	4	0.000313	0.0220806	70.5794186
2011	Ventspils	3	10	8.09E-05	0.0077431	95.70141527
2011	Ventspils	3	20	0.001017	0.1626855	160.0044565
2011	Ventspils	4	4	0.000182	0.0503948	276.1439502
2011	Ventspils	4	20	0.007282	0.919436	126.264782
2011	Ventspils	4	4	0.000297	0.047902	161.467555
2011	Ventspils	4	10	0.000372	0.0298016	80.07291456
2011	Ventspils	4	20	0.004008	0.2386397	59.54541483
2011	Ventspils	5	4	0.000343	0.0495397	144.6352024
2011	Ventspils	5	10	0.007512	0.951306	126.6390252
2011	Ventspils	5	20	0.002158	0.2871976	133.0559794
2011	Ventspils	6	2	2.7E-06	0.0002653	98.38032394
2011	Ventspils	6	4	0.000389	0.0736054	189.0896263
2011	Ventspils	6	10	6.29E-06	0.0007831	124.4441588
2011	Ventspils	6	20	0.006273	0.3838895	61.19570965
2011	Ventspils	7	4	0.000439	0.072931	166.240898
2011	Ventspils	7	10	0.0013	0.065557	50.43090045
2011	Ventspils	7	20	0.004118	0.295075	71.65028102
2011	Ventspils	7	110	0.018052	0.1571687	8.706592015
2011	Ventspils	8	2	4.49E-06	0.0009607	213.7372525
2011	Ventspils	8	4	0.000539	0.0898214	166.5229454
2011	Ventspils	8	10	0.00143	0.1239637	86.67023143
2011	Ventspils	8	20	0.007315	0.2485272	33.97468268
2011	Ventspils	8	110	0.001682	0.1332919	79.24573111
2011	Ventspils	9	2	4.49E-06	0.0003986	88.68559621
2011	Ventspils	9	4	0.000808	0.2919862	361.2837314
2011	Ventspils	9	10	0.003604	0.3215894	89.23012105
2011	Ventspils	9	20	0.00417	0.3826239	91.76712164
2011	Ventspils	10	4	0.000224	0.0287208	128.3045934
2011	Ventspils	10	10	0.001299	0.1430721	110.136923
2011	Ventspils	10	20	0.00276	0.293014	106.1685329
2011	Ventspils	11	4	0.000355	0.1417402	399.1551901
2011	Ventspils	11	20	0.005166	0.9371969	181.3992169
2011	Ventspils	11	4	0.000118	0.0371491	315.4446719
2011	Ventspils	11	20	0.003622	0.2808255	77.53273123
2011	Ventspils	12	4	0.000235	0.0279007	118.9107006
2011	Ventspils	12	10	1.17E-05	0.0006911	59.13817237
2011	Ventspils	12	20	0.00288	0.4845848	168.2375916
2011	Ventspils	12	4	0.000394	0.0878394	223.0803078
2011	Ventspils	12	20	0.006177	0.6938678	112.3317567
		49		0.113776	11.437133	9214.39168

2.2. Plānotās dīkstāves 2011. g.

Gads	Ekspluatācijas rajons	Mēness	Sprieguma līmenis	SAIFI	SAIDI (min)	CAIDI (min)
2011	Talsi	1	4	1.79798E-05	0.003401018	189.1580017
2011	Talsi	1	20	0.000689524	0.102357039	148.4458649
2011	Talsi	2	4	4.58484E-05	0.006932244	151.1991719
2011	Talsi	2	20	0.000443201	0.133122042	300.3646397
2011	Talsi	3	4	0.000287676	0.084782523	294.7149112
2011	Talsi	3	20	0.004111974	1.492389687	362.9374912
2011	Talsi	4	2	8.98989E-07	5.70294E-05	63.43731254
2011	Talsi	4	4	0.000414434	0.080603211	194.4899523
2011	Talsi	4	20	0.002426371	0.485783776	200.2100506
2011	Talsi	5	4	0.000379373	0.075750601	199.6730196
2011	Talsi	5	20	0.001117443	0.310357747	277.7392229
2011	Talsi	6	4	0.000266101	0.075299743	282.9746551
2011	Talsi	6	20	0.003277713	0.565802042	172.6209887
2011	Talsi	7	1	4.49494E-06	0.000961726	213.9572086
2011	Talsi	7	4	9.07979E-05	0.017898058	197.119817
2011	Talsi	7	20	0.000913373	0.247454077	270.9234892
2011	Talsi	8	4	9.34948E-05	0.016393586	175.3421752
2011	Talsi	8	20	0.001119241	0.371295182	331.7383779
2011	Talsi	9	4	0.000175303	0.041687224	237.8012432
2011	Talsi	9	20	0.001506705	0.428928956	284.6800966
2011	Talsi	10	4	0.000215757	0.050645009	234.7313871
2011	Talsi	10	20	0.001978674	0.478907872	242.0347295
2011	Talsi	11	4	0.000214858	0.04587524	213.513922
2011	Talsi	11	20	0.003648096	0.769627542	210.9668957
2011	Talsi	12	4	0.000149232	0.028556314	191.3550021
2011	Talsi	12	20	0.002547734	0.351730328	138.0561397
		27		2.61E-02	6.27E+00	2.22E+02
2011	Ventspils	1	4	4.85454E-05	0.014624221	301.2483923
2011	Ventspils	1	10	1.79798E-06	0.000307842	171.2157568
2011	Ventspils	1	20	0.000694019	0.185806973	267.7259453
2011	Ventspils	2	4	3.95555E-05	0.003025316	76.4828095
2011	Ventspils	2	20	0.001585816	0.419572983	264.5785847
2011	Ventspils	3	4	0.00016901	0.029360449	173.7203091
2011	Ventspils	3	10	0.000376676	0.079657379	211.4743718
2011	Ventspils	3	20	0.001881583	0.530820427	282.113684
2011	Ventspils	4	4	0.000410838	0.040786588	99.27660711
2011	Ventspils	4	20	0.002525259	0.282472409	111.8587722
2011	Ventspils	5	4	6.65252E-05	0.008783566	132.0337284
2011	Ventspils	5	20	0.001427594	0.417520763	292.4646179
2011	Ventspils	6	4	0.000341616	0.107251398	313.9533497
2011	Ventspils	6	10	8.98989E-07	4.87903E-05	54.27247884
2011	Ventspils	6	20	0.000626595	0.139957064	223.361234
2011	Ventspils	7	4	0.000205868	0.031592146	153.4579547

2011	Ventspils	7	10	3.77575E-05	0.0063766	168.8828901
2011	Ventspils	7	20	0.001254089	0.323218715	257.7318228
2011	Ventspils	8	4	0.000197778	0.033670313	170.2433756
2011	Ventspils	8	20	0.001362867	0.404700122	296.9476465
2011	Ventspils	9	4	4.04545E-05	0.006817136	168.5137047
2011	Ventspils	9	10	0.000584343	0.010418439	17.82933157
2011	Ventspils	9	20	0.00083606	0.260390755	311.4500218
2011	Ventspils	10	4	9.43938E-05	0.010633614	112.6515967
2011	Ventspils	10	10	1.79798E-06	0.000455292	253.2243551
2011	Ventspils	10	20	0.001297241	0.22871042	176.3053026
2011	Ventspils	11	4	2.87676E-05	0.003123721	108.5845331
2011	Ventspils	11	20	0.001786291	0.487353171	272.8297236
2011	Ventspils	12	4	0.000122262	0.019211742	157.1352396
2011	Ventspils	12	10	8.98989E-07	0.000276938	308.0550557
2011	Ventspils	12	20	0.000433313	0.18247314	421.1120432
			31	0.018480511	4.269418432	204.2172658

3.Pielikums. Ūdens sadales tīkla, elektroapgādes un telekomunikācijas tīkla mijiedarbības simulācijas rezultāti (1–4. mēģinājums)

Mēģinājumi		1		
Parametri		RBDL	RBNL	
Vērtības		0.1	48	
Stāvoklis	state	water up W1	Power down	Power up
	0	0.0000	0.0000	
	0	286,404043860054	0.0000	286.9934
	0	286,993381735779	0.0000	
	2	614,152064782396	614.1521	
	1	614.1810	0.0000	
	0	614.4427	0.0000	
	0	616.7597	0.0000	616.7597
	2	618.6997	0.0000	
	2	627,785442043852	0.0000	
	2	629,387286014283	0.0000	
	2	635,183122854733	0.0000	
	2	637,098690891231	0.0000	
	2	660,118496845109	0.0000	
	2	882,841539931762	882.8415	
	1	882.9814	0.0000	
	0	883.5764	0.0000	
	0	883,809899210374	0.0000	
	0	884.0897	0.0000	884.0897
	2	885.2080	0.0000	
	2	888,032694750638	0.0000	

2	900,488723677750	0.0000	
2	901,163100247747	0.0000	
2	911,192424359949	0.0000	
2	1116,68573605727	1116.6857	
1	1116.7785	0.0000	
0	1117.3379	0.0000	
0	1120.2530	0.0000	1120.2530
2	1120.7283	0.0000	
2	1124,74039662184	0.0000	
2	1128,67259797093	0.0000	
2	1128,90208003827	0.0000	
2	1148,61353026435	0.0000	
2	1176,17240488541	0.0000	
2	1322,79521825330	1322.7952	
1	1322.8148	0.0000	
0	1322.8411	0.0000	
0	1323.3389	0.0000	1323.3389
2	1324.5391	0.0000	
2	1324,90343803311	0.0000	
2	1325,55972850457	0.0000	
2	1325,63515245906	0.0000	
2	1343,67869792230	0.0000	
2	1424,83757459531	0.0000	
2	1820,99288927838	1820.9929	
1	1821.0567	0.0000	
0	1822.1409	0.0000	
0	1822,41709833110	0.0000	
0	1823.5549	0.0000	1823.5549
2	1824.1409	0.0000	
2	1827,05522026488	0.0000	
2	1838,89922746436	0.0000	
2	1851,89436261396	0.0000	
2	1959,61212617264	0.0000	
2	2266,12553453592	2266.1255	
1	2266.3051	0.0000	
0	2266.3930	0.0000	
0	2266,83836967928	0.0000	
0	2268,76192321138	0.0000	
0	2271.1008	0.0000	2271.1008
2	2272.3622	0.0000	
2	2277,99400223830	0.0000	
2	2278,67658237332	0.0000	
2	2290,63969506905	0.0000	
2	2745,46227330205	2745.4623	
1	2745.4950	0.0000	
0	2746.0217	0.0000	
0	2746.5336	0.0000	2746.5336
2	2746.5961	0.0000	

2	2746,88658939551	0.0000	
2	2750,13005828197	0.0000	
2	2753,35319524931	0.0000	
2	2761,15725133206	0.0000	
2	2768,67161984189	0.0000	
2	3214,75310418008	3214.7531	
1	3214.8275	0.0000	
0	3215.0094	0.0000	
0	3215.5270	0.0000	3215.5270
2	3215.7292	0.0000	
2	3219,91763780322	0.0000	
2	3220,59621573584	0.0000	
2	3229,57581499533	0.0000	
2	3255,90934744212	0.0000	
2	3276,51271806451	0.0000	
2	3686,89115224489	3686.8912	
1	3686.9314	0.0000	
0	3687.9955	0.0000	
0	3690.6311	0.0000	3690.6311
2	3691.6457	0.0000	
2	3692,04540729463	0.0000	
2	3696,43370612103	0.0000	
2	3699,11302325949	0.0000	
2	3715,08046759867	0.0000	
2	3825,53999393627	0.0000	
2	4000.0000		
9	2.6545	9	2.3432

116	2.2686
-----	--------

2.2686

PW	150
VN	116
Koef.	0.7733

Mēģinājumi

2

Parametri

RBDL	RBNL
------	------

Vērtības

3	24
---	----

Stāvoklis

state	water up W2	Power down	Power up
0	0.0000	0.0000	
0	286,404043860054	0.0000	286.9934
0	286,993381735779	0.0000	
2	614,152064782396	614.1521	
1	614,180997740873	0.0000	
1	614.4427	0.0000	
0	616.7597	0.0000	616.7597
2	618.6997	0.0000	
2	627,785442043852	0.0000	

2	629,387286014283	0.0000	
2	635,183122854733	0.0000	
2	637,098690891231	0.0000	
2	660,118496845109	0.0000	
2	882,841539931762	882.8415	
1	882,981436701762	0.0000	
1	883,576393811772	0.0000	
1	883,809899210374	0.0000	
1	884,089693355320	0.0000	884.0897
2	885,208046927564	0.0000	
2	888,032694750638	0.0000	
1	900,488723677750	0.0000	
1	901,163100247747	0.0000	
1	911,192424359949	0.0000	
1	1116.6857	1116.6857	
0	1116.7785	0.0000	
0	1117,33793338770	0.0000	
0	1120.2530	0.0000	1120.2530
2	1120.7283	0.0000	
2	1124,74039662184	0.0000	
2	1128,67259797093	0.0000	
2	1128,90208003827	0.0000	
2	1148,61353026435	0.0000	
2	1176,17240488541	0.0000	
2	1322,79521825330	1322.7952	
1	1322,81484949960	0.0000	
1	1322,84113415576	0.0000	
1	1323,33887743436	0.0000	1323.3389
2	1324,53912214580	0.0000	
1	1324,90343803311	0.0000	
1	1325,55972850457	0.0000	
1	1325,63515245906	0.0000	
1	1343,67869792230	0.0000	
1	1424,83757459531	0.0000	
1	1820.9929	1820.9929	
0	1821.0567	0.0000	
0	1822,14087020709	0.0000	
0	1822,41709833110	0.0000	
0	1823.5549	0.0000	1823.5549
2	1824.1409	0.0000	
2	1827,05522026488	0.0000	
2	1838,89922746436	0.0000	
2	1851,89436261396	0.0000	
2	1959,61212617264	0.0000	
2	2266,12553453592	2266.1255	
1	2266,30513092002	0.0000	
1	2266,39301602311	0.0000	
1	2266,83836967928	0.0000	

1	2268,76192321138	0.0000	
1	2271,10081743959	0.0000	2271.1008
2	2272,36221809139	0.0000	
1	2277,99400223830	0.0000	
1	2278,67658237332	0.0000	
1	2290,63969506905	0.0000	
1	2745.4623	2745.4623	
0	2745.49504	0.0000	
0	2746,02173380161	0.0000	
0	2746.53362	0.0000	2746.5336
2	2746.59614	0.0000	
2	2746,88658939551	0.0000	
2	2750,13005828197	0.0000	
1	2753,35319524931	0.0000	
1	2761,15725133206	0.0000	
1	2768,67161984189	0.0000	
1	3214.7531	3214.7531	
0	3214.82747	0.0000	
0	3215,00938867288	0.0000	
0	3215.52696	0.0000	3215.5270
2	3215.7292	0.0000	
2	3219,91763780322	0.0000	
1	3220,59621573584	0.0000	
1	3229,57581499533	0.0000	
1	3255,90934744212	0.0000	
1	3276,51271806451	0.0000	
1	3686.89115	3686.8912	
0	3686.9314	0.0000	
0	3687,99554860928	0.0000	
0	3690.63109	0.0000	3690.6311
2	3691.6457	0.0000	
1	3692,04540729463	0.0000	
1	3696,43370612103	0.0000	
1	3699,11302325949	0.0000	
1	3715,08046759867	0.0000	
1	3825,53999393627	0.0000	
1	4000		
9	1.7435	6 un 9	2.3432
6	2.6152		
6	2.3386		
9	1.5590		

Mēģinājumi

			3	
Parametri	RBDL		RBNL	
Vērtības		6	4	
Stāvoklis	state	water up W3	Power down	Power up
	0	0.0000	0.0000	

0	0.0000	0.0000	
0	0.0000	0.0000	286.9934
2	614,152064782396	614.1521	
1	614,180997740873	0.0000	
1	614,442658331133	0.0000	
1	616.7597	0.0000	616.7597
2	618.6997	0.0000	
2	627,785442043852	0.0000	
1	629,387286014283	0.0000	
1	635,183122854733	0.0000	
1	637,098690891231	0.0000	
1	660,118496845109	0.0000	
1	882.8415	882.8415	
0	882.9814	0.0000	
0	883,576393811772	0.0000	
0	883,809899210374	0.0000	
0	884.0897	0.0000	884.0897
2	885.2080	0.0000	
2	888,032694750638	0.0000	
2	900,488723677750	0.0000	
2	901,163100247747	0.0000	
2	911,192424359949	0.0000	
2	1116,68573605727	1116.6857	
1	1116.7785	0.0000	
1	1117,33793338770	0.0000	
1	1120,25298653380	0.0000	1120.2530
2	1120.7283	0.0000	
2	1124,74039662184	0.0000	
2	1128,67259797093	0.0000	
1	1128,90208003827	0.0000	
1	1148,61353026435	0.0000	
1	1176,17240488541	0.0000	
1	1322.7952	1322.7952	
0	1322.8148	0.0000	
0	1322,84113415576	0.0000	
0	1323.3389	0.0000	1323.3389
2	1324.5391	0.0000	
2	1324,90343803311	0.0000	
2	1325,55972850457	0.0000	
2	1325,63515245906	0.0000	
2	1343,67869792230	0.0000	
2	1424,83757459531	0.0000	
2	1820,99288927838	1820.9929	
1	1821.0567	0.0000	
1	1822.1409	0.0000	
0	1822.4171	0.0000	
0	1823.5549	0.0000	1823.5549
2	1824.1409	0.0000	

2	1827,05522026488	0.0000	
2	1838,89922746436	0.0000	
2	1851,89436261396	0.0000	
2	1959,61212617264	0.0000	
2	2266,12553453592	2266.1255	
1	2266,30513092002	0.0000	
1	2266.3930	0.0000	
0	2266.8384	0.0000	
0	2268,76192321138	0.0000	
2	2271.1008	0.0000	2271.1008
2	2272,36221809139	0.0000	
2	2277,99400223830	0.0000	
2	2278,67658237332	0.0000	
2	2290,63969506905	0.0000	
2	2745,46227330205	2745.4623	
1	2745.49504	0.0000	
1	2746.0217	0.0000	
0	2746.5336	0.0000	2746.5336
2	2746.5961	0.0000	
2	2746,88658939551	0.0000	
2	2750,13005828197	0.0000	
2	2753,35319524931	0.0000	
2	2761,15725133206	0.0000	
2	2768,67161984189	0.0000	
2	3214,75310418008	3214.7531	
1	3214.82747	0.0000	
1	3215.0094	0.0000	
0	3215.5270	0.0000	3215.5270
2	3215.7292	0.0000	
2	3219,91763780322	0.0000	
2	3220,59621573584	0.0000	
2	3229,57581499533	0.0000	
2	3255,90934744212	0.0000	
2	3276,51271806451	0.0000	
2	3686,89115224489	3686.8912	
1	3686.9314	0.0000	
1	3687,99554860928	0.0000	
1	3690,63109103241	0.0000	3690.6311
2	3691.6457	0.0000	
2	3692,04540729463	0.0000	
1	3696,43370612103	0.0000	
1	3699,11302325949	0.0000	
1	3715,08046759867	0.0000	
1	3825,53999393627	0.0000	
1	4000		
9	1.1335	6 un 9	2.3432
6	1.7003		

6	1.4905
---	--------

9

0.9937

4			
	RBDL	RBNL	
	1.5	36	
state	water up W1	Power down	Power up
0	0.0000	0.0000	
0	407,388756140899	0.0000	
0	412,493166830115	0.0000	412.4932
2	900,288977247922	900.2890	
1	900,883281826773	0.0000	900.8833
2	902,761069694807	0.0000	
2	902,869503133047	0.0000	
2	903,419268965638	0.0000	
1	903,519052722974	0.0000	
1	913,153391225633	0.0000	
1	922,281909340603	0.0000	
1	928,600274388802	0.0000	
1	929,001844298968	0.0000	
1	1236.0012	1236.0012	
0	1236.4470	0.0000	
0	1236,60047429514	0.0000	
0	1238.2435	0.0000	1238.2435
2	1239.0787	0.0000	
2	1239,63530055781	0.0000	
2	1244,09991740719	0.0000	
2	1252,40305511332	0.0000	
2	1259,16287021745	0.0000	
2	1262,21264629153	0.0000	
2	1603,51551993077	1603.5155	
1	1603,68768184923	0.0000	
1	1603.7330	0.0000	
0	1603.7411	0.0000	
0	1604,43857388979	0.0000	
0	1606,00341608831	0.0000	
0	1606.0527	0.0000	1606.0527
2	1610.6144	0.0000	
2	1613,55099100460	0.0000	
2	1681,41592732177	0.0000	
2	1947,22465852170	1947.2247	
1	1947.7407	0.0000	
0	1948.0004	0.0000	
0	1950.6013	0.0000	1950.6013
2	1953.6675	0.0000	
2	1956,38750385597	0.0000	
2	1961,34858578212	0.0000	

2	1972,28287305780	0.0000	
2	1984,13966713182	0.0000	
2	2168,27288495594	0.0000	
2	2276,38354443584	2276.3835	
1	2278,41912210855	0.0000	
1	2280.1228	0.0000	
0	2280.3884	0.0000	
0	2281.3901	0.0000	2281.3901
2	2283.4671	0.0000	
2	2289,64760896810	0.0000	
2	2297,62607916072	0.0000	
2	2306,21821942771	0.0000	
2	2362,99115689246	0.0000	
2	2744,78550282489	2744.7855	
1	2745.2361	0.0000	
0	2745.4683	0.0000	2745.4683
2	2747.4842	0.0000	
2	2748,85776916950	0.0000	
2	2749,81898659305	0.0000	
2	2757,44995149726	0.0000	
2	2768,85554287105	0.0000	
2	2769,51734186078	0.0000	
2	2770,50388689612	0.0000	
2	2996,31874247218	2996.3187	
1	2996.37751	0.0000	
0	2998.22322	0.0000	
0	2998,28335648062	0.0000	
0	2998.67414	0.0000	2998.6741
2	2999.72327	0.0000	
2	3000,77570726987	0.0000	
2	3008,28677808680	0.0000	
2	3013,69844653235	0.0000	
2	3077,23681840967	0.0000	
2	3444,54768238215	3444.5477	
1	3444.72414	0.0000	
0	3445.14585	0.0000	
0	3445,19740835993	0.0000	
0	3447.59652	0.0000	3447.5965
2	3452.83436	0.0000	
2	3454,04209081114	0.0000	
2	3459,72810962466	0.0000	
2	3466,45007079538	0.0000	
2	3525,28965013667	0.0000	
2	3789,45423429878	3789.4542	
1	3789,88385546773	0.0000	
1	3789,96904084106	0.0000	
1	3790,80712074005	0.0000	
1	3792.14573	0.0000	

0	3792.52388	0.0000	3792.5239
2	3792.53953	0.0000	
2	3816,51125942636	0.0000	
2	3818,57623255745	0.0000	
2	3866,85783833691	0.0000	
2	4000		

9	3.2745	8 un 9	2.5460
---	---------------	--------	--------

8	1.8087
---	---------------

9	1.9211
---	--------

„Smart Metering” sistēmas testēšanas atskaite

1.sadaļa. Mērījumu reģistrēšana, pārraide un apstrādes tests

Projekts “Smart Metering” LLIV-312

Projekta mājas lapa: <http://www.smartmeteringproject.eu>

Testēšanas dalībnieki:

Ventspils augstskolas: pētnieks, Kaspars Kondratjevs



PSIA Ūdeka: PSIA „Ūdeka” tehniskās daļas vadītājs Viesturs Otomers



Septembris 2013

Versija 1.0

Satura rādītājs

1. Ievads	126
1.1. Testēšanas mērķi	126
1.2. Testēšanas norises vieta	126
1.3. Testēšanas norises laiks	126
1.4. Testēšanas dalībnieki	126
2. Testēšanas laikā izmantotās ierīces un aparatūra	126
3. „Smart Metering” sistēmas testēšanas rezultāti	139
3.1. Testēšanas metodika	139
3.2. Testēšanas rezultāti	140
3.3. Secinājumi	141

1. Ievads

1.1. Testēšanas mērķi

Datu pārraides testēšanas mērķis ir novērtēt izveidotās sakaru infrastruktūras darbības efektivitāti un funkcionalitāti dažādos ārējās vides apstākļos (negaiss, paaugstināts gaisa mitrums, veģetācijas blīvums un gada perioda raksturīgās veģetācijas izmaiņas). Testēšanas rezultātā iegūtā informācija norāda uz tīkla trūkumiem, iespējamiem uzlabošanas uzdevumiem, kā arī snigt vadlīnijas cita jauna datu pārraides tīkla izveides gadījumā. Testēšanas pamata mērķis ir pārbaudīt plānoto ūdens tīkla spiediena un ūdens patēriņa mēriekārtu bezvadu radio sensoru signāla pārraides kvalitāti un piegādi līdz datu apstrādes sistēmai.

1.2. Testēšanas norises vieta

Testēšana tika veikta izmēģinājuma tīkla atrašanās vietā (Ventspils pansionāta un bērnu nama „Selga” rajonā) izmantojot testēšanas mobilo iekārtu, kā arī attālināti izmantojot datu apstrādes servisu vidi.

1.3. Testēšanas norises laiks

Testēšana veikta periodiski sistēmas izstrādes procesa laikā, kur pēdējais pilnais apsekojums veikts: 06.09.2013 09:00

1.4. Testēšanas dalībnieki

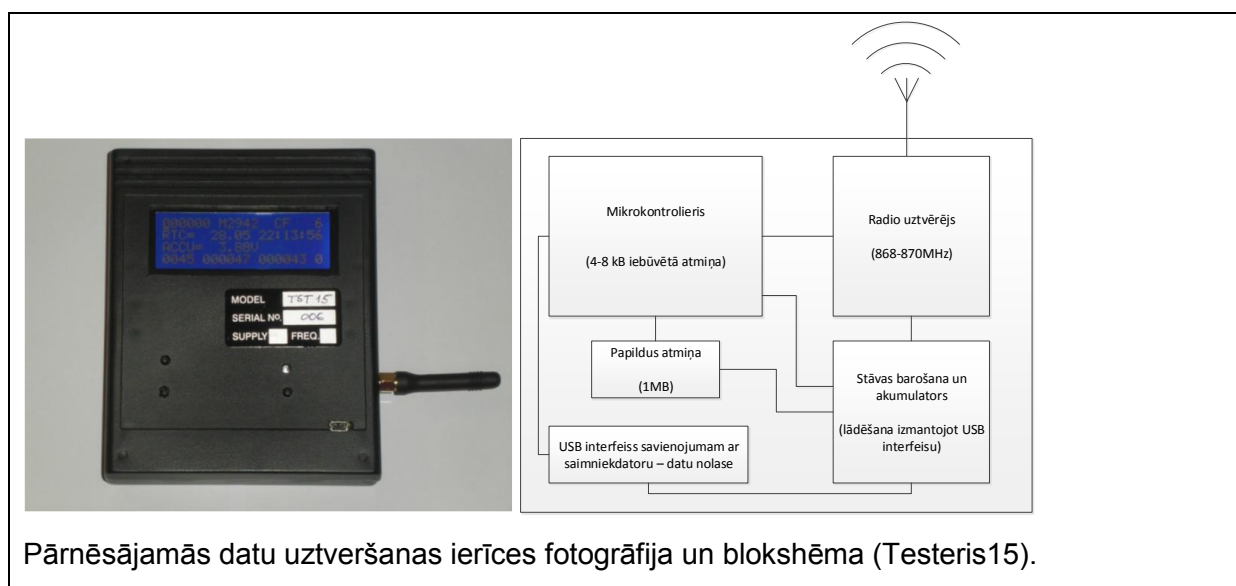
No Ventspils augstskolas: pētnieks, Kaspars Kondratjevs

No PSIA Ūdeka: PSIA „Ūdeka” tehniskās daļas vadītājs Viesturs Otomers

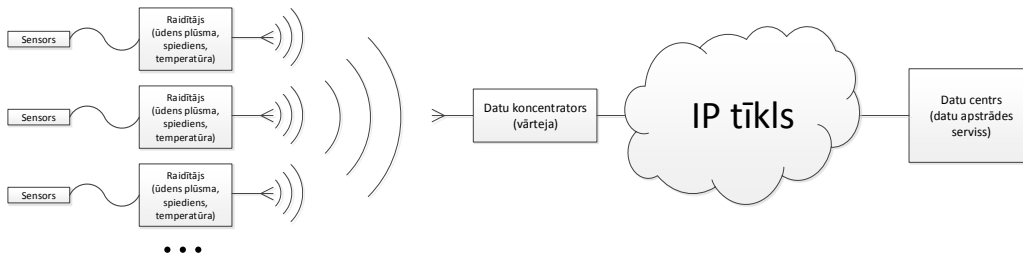
2. Testēšanas laikā izmantotās ierīces un aparatūra

Testēšanas procesā izmantots Testeris15, kas nodrošina 868MHz frekvenču diapazonā raidīto sensoru datu uztveršanu un vizuālu attēlošanu LCD displejā. Analogiskas iekārtas pievienotas Ethernet vārtējām (datu koncentratori) dažādos stratēģisko tīkla posmos nodrošina datu pārraidi līdz datu apstrādes serveriem, kur iespējams nolasīt sensoru rādījumus. Testēšanas procesos tika lietotas abas metodes.

Testēšanas aparatūras un iekārtas saslēgšanas blokhēma



Pārnēsājamās datu uztveršanas ierīces fotogrāfija un blokhēma (Testeris15).



Datu piegāde

līdz apstrādes serverim – blokshēma.

Valoda: LV EN RU | testuser@email.com | Ieteikums | Kļūdas ziņojums | Iziet

Smart Metering
Sistēma
Iestatījumi
Saskarne

Mēritāji

Mēritāju pārvaldīšana
melns: zems baterijas spriegums (drīz nepieciešama maiņa)
zils: nostrādāja tamperis
sarkans: mēritājam drīz beigsies derīguma termiņš
oranžs: novērotas patēriņa izmaiņas virs 20%
pelēks: mainījās baterijas patēriņš

▼ Atlase Saglabātie atlasē nosacījumi: -Jauns filtrs-

Pievienot jaunu atlasē lauku

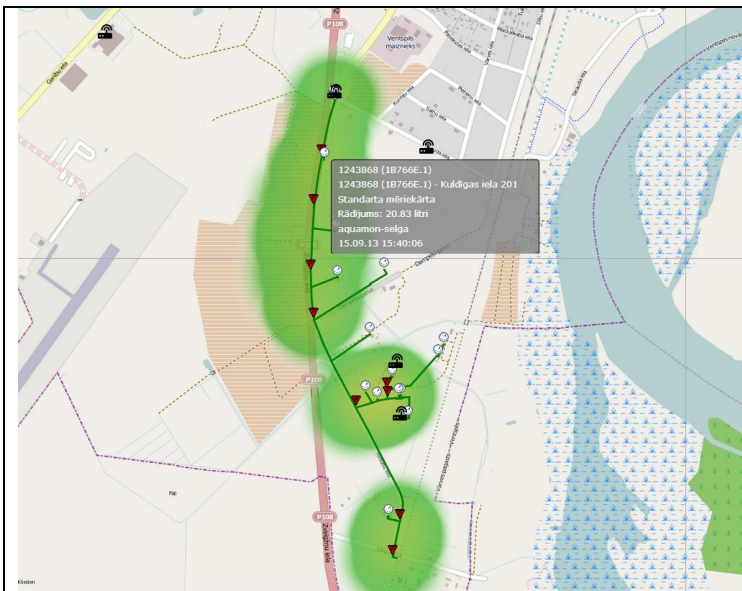
✓ Filtrēt
 ↻ Attīrīt
 💾 Saglabāt

Sērījas Nr	Iekārtas Nr	Adrese	Skalā m ³	Pat. m ³ /mēn	Ubat	RSSI	GWID	Iespējas
00000000053168								
1243953	1B7E42.1	Dampeļu gatve 9	81.68	5.12	85	132	aquamon-selga	🔗 🗑️ 🇺🇸 🇩🇪 🇬🇧
1243868	1B766E.1	Kuldīgas iela 201	20.83	1.1	86	131	aquamon-selga	🔗 🗑️ 🇺🇸 🇩🇪 🇬🇧
23284-1	1B7EA9.1	Kuldīgas iela 209	298.6	5.87	85	96	aquamon-bsbv	🔗 🗑️ 🇺🇸 🇩🇪 🇬🇧
1239852	1B7D6B.2	Kuldīgas iela 215	78.0	2.21	85	131	aquamon-selga	🔗 🗑️ 🇺🇸 🇩🇪 🇬🇧
1111009044	1B7E6F.1	Pērkoņu iela 11	58.647	4.28	85	32	aquamon-bsbv	🔗 🗑️ 🇺🇸 🇩🇪 🇬🇧
1243881	1B7B16.1	Pērkoņu iela 11a, Sūkņu stacija	1.585	0.008	79	106	aquamon-selga	🔗 🗑️ 🇺🇸 🇩🇪 🇬🇧
1134000755	1B7846.1	Pērkoņu iela 13	1605.215	163.623	78	94	aquamon-selga	🔗 🗑️ 🇺🇸 🇩🇪 🇬🇧
111009067	1B7A21.1	Pērkoņu iela 14	224.59	3.78	78	0	aquamon-bsbv	🔗 🗑️ 🇺🇸 🇩🇪 🇬🇧
1134000774	1B7933.1	Pērkoņu iela 17	2118.436	83.683	79	96	aquamon-selga	🔗 🗑️ 🇺🇸 🇩🇪 🇬🇧
111008959	1B7680.1	Pērkoņu iela 19	396.629	2.817	85	131	aquamon-selga	🔗 🗑️ 🇺🇸 🇩🇪 🇬🇧
000170	1B7C9F.1	Pērkoņu iela 21, Katlu māja	1638.0	0.62	79	128	aquamon-selga	🔗 🗑️ 🇺🇸 🇩🇪 🇬🇧
1032006285	1B7D90.1	Pērkoņu iela 21, Pansionāts	4688.97	291.54	79	113	aquamon-selga	🔗 🗑️ 🇺🇸 🇩🇪 🇬🇧
000157	1B8172.1	Pērkoņu iela 21, Veļas mazgātuve	426.07	29.81	79	111	aquamon-selga	🔗 🗑️ 🇺🇸 🇩🇪 🇬🇧
011292	1B753D.1	Pērkoņu iela 7	179.069	11.09	84	103	aquamon-selga	🔗 🗑️ 🇺🇸 🇩🇪 🇬🇧
FFF001.1	FFF001.1	SCADA plūsmas simulācija	4291.034	402.032	80	200	aquamon-scada-sim	🔗 🗑️ 🇺🇸 🇩🇪 🇬🇧

Vārtējas

- Mēritāji
- Rādījumi
- Rādījumu statistika
- Rādījumu saraksts
- Spiediena devēji
- Spiediena devēju rādījumi
- Spiediena devēju statistika
- Spiediena devēju temperatūra
- Sūkņi
- Aquamon versijas
- Koda versijas
- Gala lietotāji
- Reģioni
- Kompānijas
- Cenas
- Eksporti
- Eksporta konfigurācija
- Notikumu pārliks
- Notikumu pārlika konfigurācija
- Noplūžu detektora konfigurācija
- Labot izvēlni

Reālā laika datu reprezentācija datu apstrādes servera informācijas sistēmā.



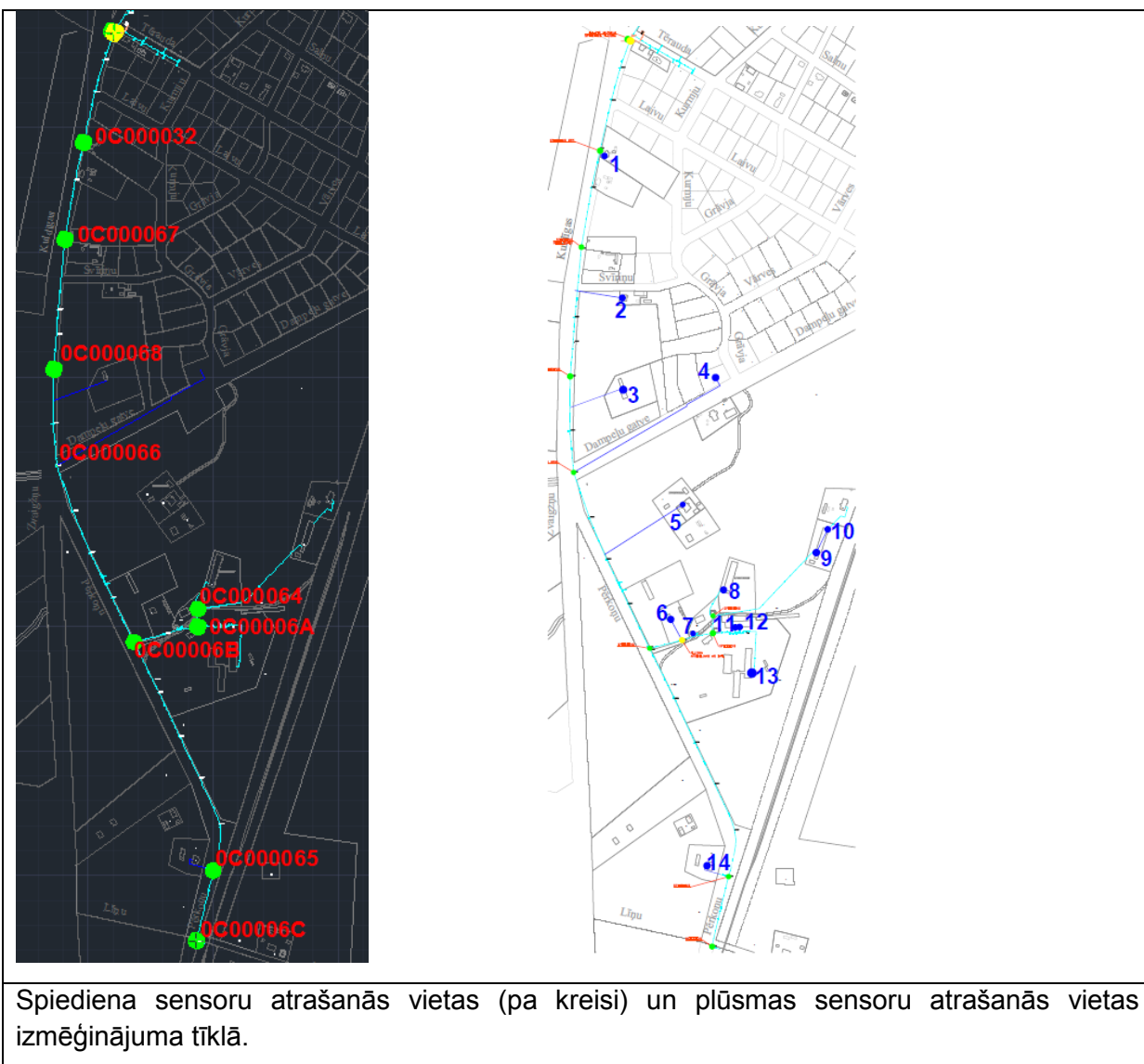
Reālā laika datu reprezentācija datu

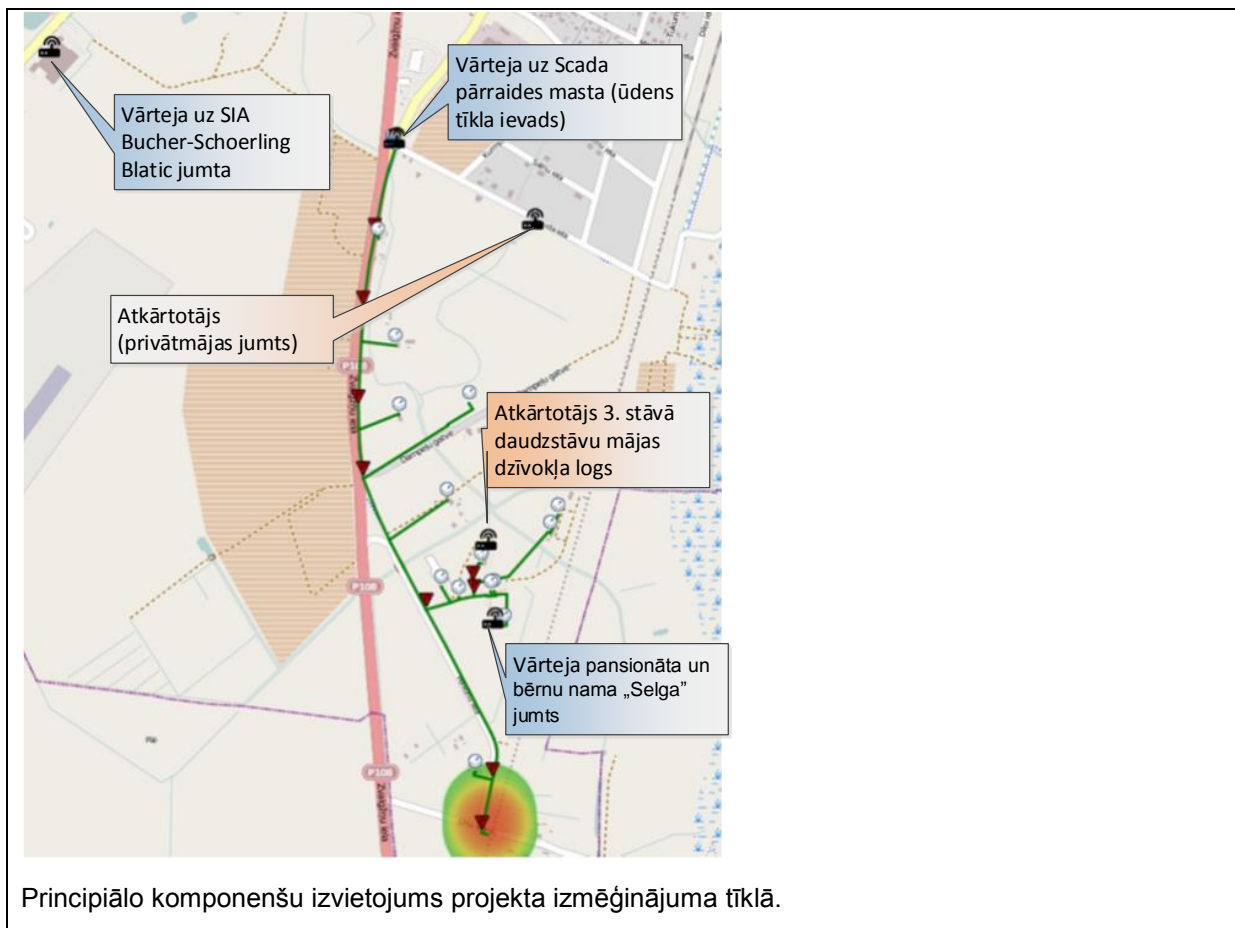
apstrādes servera informācijas sistēmas vizualizācijas sadaļā - kartē.

Testēšanas aparātūras un iekārtas izvietošanas shēma



Datu pārraides topogrāfija ar datu piegādes bezvadu savienojumiem (no datu koncentratoriem izmantjot bezvadu 5.8GHz tiltus) līdz galējam koncentratoram. Iezīmētie apļi apzīmē koncentratoru uztveršanas pus-diametrus (zili) un signāla atkārtotāju pilnos diametrus (dzeltēni).





Testēšanā izmantotas aparatūras apraksts

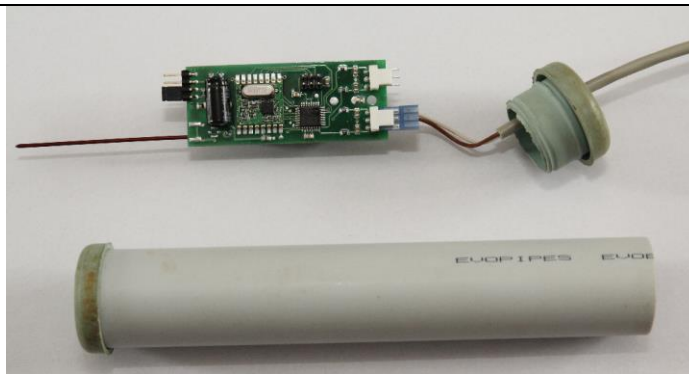
Testēšanas aprīkojums:

- Pārbaudes izmantojot Testeris15 mobilais nolasītājs
- Ūdens plūsmas nolasītāji (ICR20wt)
- Ūdens spiediena nolasītāji (ICR10w4)
- Ethernet vārteja
- Datu apstrādes serveris

Aparatūras izvietojanas adreses un objektu fotogrāfijas

Ūdens plūsmas nolasītāji

Ūdens plūsmas nolasītāja ICR20wt izskats



1. Kuldīgas iela 201 (ICR 1B787B)

Pieejot pa verandu, koridors, ēkas vidu pagrabs, koka vāks, nav iespējams iznest, 30cm zem vāka, bija pa īsu vads, varētu pielikt pie koka vāka



2. Kuldīgas iela 209 (ICR 1B7A97)

Galā iekšā, pa labi, katla telpā, 40 cm virs zemes, priekšā siena, varētu uzlikt augstāk.



3. Kuldīgas iela 215 (ICR 1B75B9)

Dzeltenā saimniecības ēka, pa vidu 1m virs grīdas, ir logs, ja vajag pārlikt, tad kabelis 4-5m



4. Dampelu gatve 9 (ICR 1B7B85)

Mazie lodziņi garāžā, pretējā pusē ir kambaris, 1m virs zemes, iespējams garāks vads, bet diez vai iespējama izvešana.



5. Pērkonu iela 7 (ICR 1B7577)

Mazā ieeja, aiz durvīm pagrabs, koka vāks, 30cm zem vāka, varētu pielikt pie vāka, jautājums par virziena orientāciju (guļus, vertikāli, pagrieziens – tas aktuāli visās vietās)



6. Pērkonu iela 11 (ICR 1B78F7)

No kreisās puses trešais logs, 1m virs grīdas, iespējams uzlikt uz SCADA pusi pie mazā lodziņa, vads 3-4m.



7. Pērkonu iela 11a (ICR 1B7D21)

Sūkņu stacija, pieder Ūdekai, 20cm virs grīdas, pie pretējās sienas, ja neuztver, nepieciešams vads 5-6m.



8. Pērkonu iela 13 (ICR 1B76CC)

Daudzstāvu ēka, no kreisās puses stūrī, zemes līmenī, bet ir caurums, pa kuru izlaist, nepieciešams 4-5m un hermētiska.



9. Pērkonu iela 17 (ICR 1B7469)

Tur kur atrodas gāzes ievads, 20cm zem zemes, var izlaist ārā, jāurbj (40cm), vada garums 6-7m, hermētiska.



10. Pērkonu iela 19 (ICR 1B75D0)

Tā pati ēka, kas iepriekš, tikai otrs gals, pie gāzes ievada zemes līmenī, ir caurums, vajadzīgs vads 4-5m, hermētiska.



11. Pērkona iela 12 (Katlu māja) (ICR 1B7C9F)

No dzelzs durvīm trešais logs, 70cm virs grīdas, varētu pielikt pie loga, vads 3m.



12. Pērkonu iela 21 (Veļas mazgātuve) (ICR 1B7C45)

No kreisās puses pirmais zaļais logs (tā pati ēka, kas iepriekš), 20cm virs grīdas, nepieciešami 4m, ja jāpietuvina logam.



13. Pērkonu iela 21 (Pansionāts) (ICR 1B78F6)

Pansionātā pirmajā stāvā (kapelā), 40cm virs zemes.



14. Pērkoņu iela 14 (ICR 1B7B2D)

Pa durvīm koridorā 3m, 70cm virs grīdas, iespējams urbt un pielikt pie putnu barotavas, vai pie jumta, ēka pieder pašvaldībai, nepieciešams vads 10-12m, hermētiska.



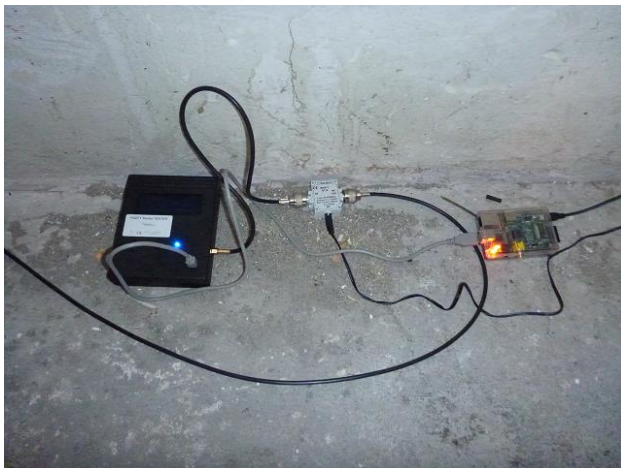
Ūdens spiediena nolasītāji

Nav noteicamas adreses, jo atrodas izmēģinājuma tīkla visā garumā: Pērkoņu ielā, Kuldīgas ielā, Kuldīgas ielā (skat.: „Testēšanas aparātūras un iekārtas izvietojuma shēma”).





Ethernet vārtejas



Datu apstrādes serveris



3. „Smart Metering” sistēmas testēšanas rezultāti

3.1. Testēšanas metodika

1. Pārnesamā testera izmantošana
1. Mēriekārtas sensora pievienošana
2. Mēriekārtas raidītāja pievienošana
3. Mērījums ar testeru tiešā tuvumā novērtējot RSSI (received signal strength indicator) rādījumu, kurš variē diapazonā no 0-200, kur 200 maksimālais signāla stiprums:
 - Spiediena devējiem mērījums tiek veikts tiešā tuvumā ~3m attālumā tiešās redzamības apstākļos – novērotajam signāla stipruma RSSI vērtībai jābūt vismaz 160
 - Ūdens plūsmas raidītāji tiek uzstādīti abonentu dzīvojamās telpās pie ūdens skaitītāja. Mērījums tiek veikts tiešā ēkas tuvumā virzienā uz tuvāko koncentratoru, tā, ka raidītājus ne vienmēr iespējams izvietot ārpus telpām tiešās redzamības apstākļos, tiek samazināta tiešā tuvumā iegūtās RSSI vērtības robeža, raidītājs tiek uzskatīts par pietiekamu, ja RSS vērtība ir vismaz 80, pieņemot, ka tuvākais koncentrators vai atkārtotājs atrodas ne tālāk par 300 metriem.
4. Mērījums pie koncentratora, atkārtotāja plānotās uzstādīšanas vietas – testeris tiek ieslēgts plānotajā atrašanās vietās 10 garāko signālu pārraides ciklu garumā, kas atbilst 10 x 10 min. = 1 h 40 min., uztveramība tiek uzskatīta par pietiekamu, ja no plānotajiem uztveramības rādīsajiem raidītājiem tiek uztverts vismaz viens ziņojums.
5. Datu apstrādes sistēmas izmantošana

Datu apstrādes sistēmas informācijas sistēma vāc datus par visiem reģistrētajiem raidītājiem, attēlojot pēdējo uztverto rādījumu un reģistrē raidīšanas laiku kā arī RSSI vērtību. Projekta ietvaros sistēmā izstrādāti – noplūžu detektori, kas papildināti ar sensoru uzraudzības funkciju – tiek ģenerēts notikums, ja:

1. Reģistrēts sensors nav sūtījis vērtību ilgāk par definētu periodu
2. Reģistrēts sensors raida nemainīgu sensora lasījumu ilgāk par definētu laika periodu
3. Reģistrēts sensors raida rādījumu, kas neatbilst rādījuma vērtības loģikai (pārāk straujas izmaiņas, nekorektas vērtības, pārāk augstas vērtības)

Veicot sistēmas uzraudzību tiek novērtēta datu pārraides sistēmas kopējā darbībā, signalizēti to komponentu darbības traucējumi.

- Pēc 3 mēneša datu uzskaites perioda, ūdens apgādes tīkla uzturētājs (PSIA „Ūdeka”) veic objektu apsekošanu reģistrējot ūdens skaitītāju rādījumu un to salīdzinot ar informācijas sistēmā reģistrētajiem rādījumiem – kas atbilst perioda un ikmēneša patēriņiem. Tiek analizētas rādījumu atšķirības, lai noteiktu un novērstu to cēloņus.

3.2. Testēšanas rezultāti

Ūdens plūsmas nolasītāji

Nr.	Address	Serial nr.	Meter value	Impulse value	Date	ICR "on" time	ICR port nr.
1	Pērkoņu iela 21 (Katlu māja)	000170	1,621	10L	15.01.2013	10:23	1B7C9F
2	Pērkoņu iela 21 (Veļas mazgātuve)	000157	237,44	10L	30.05.2013	13:42	1B8172
3	Kuldīgas iela 209	23284-1	271,8	10L	30.05.2013	17:00	1B7EA9
4	Kuldīgas iela 215	1239852	40,9	10L	03.06.2013	12:50	1B7D6B
5	Pērkoņu iela 7	011292	92,82	10L	30.05.2013	17:15	1B753D
6	Pērkoņu iela 14	111009067	200,111	10L	21.06.2013	10:53	1B7A21
7	Pērkoņu iela 11	1111009044	30,6	1m3	30.05.2013	16:20	1B7E6F
8	Pērkoņu iela 19	111008959	360,92	1m3	30.05.2013	14:15	1B7680
9	Pērkoņu iela 11A	1243881	1,2	10L	30.05.2013	16:00	1B7B16
10	Kuldīgas iela 201	1243868	9,92	10L	30.05.2013	16:40	1B766E
11	Dampeļu gatve 9	1243953	41,1	10L	30.05.2013	16:30	1B7E42
12	Pērkoņu iela 13	1134000755	4926,10	1L	31.05.2013	09:40	1B7846
13	Pērkoņu iela 17	1134000774	1805,14	1L	30.05.2013	13:55	1B7933
14	Pērkoņu iela 21 (Pansionāts)	1032006285	2861,222	10L	21.06.2013	11:15	1B7D90

Tabula nr.:1

Nr.	Address	Serial nr.	Meter value	Impulse value	Date	ICR „on” time	ICR port nr.
1	Pērkoņu iela 21 (Katlu māja)	000170	16,225	10L	20.08.2013	16:00	1B7C9F
2	Pērkoņu iela 21 (Veļas mazgātuve)	000157	378,95	10L	15.08.2013	11:05	1B8172
3	Kuldīgas iela 209	23284-1	299,34	10L	16.08.2013	10:37	1B7EA9
4	Kuldīgas iela 215	1239852	69,44	10L	15.08.2013	13:42	1B7D6B
5	Pērkoņu iela 7	011292	161,63	10L	28.08.2013	11:27	1B753D
6	Pērkoņu iela	111009067	215,50	10L	15.08.2013	10:58	1B7A21

	14						
7	Pērkoņu iela 11	1111009044	53,39	1m3	22.08.2013	17:53	1B7E6F
8	Pērkoņu iela 19	111008959	388,67	1m3	15.08.2013	10:57	1B7680
9	Pērkoņu iela 11A	1243881	1,2	10L	30.05.2013	16:00	1B7B16
10	Kuldīgas iela 201	1243868	18,32	10L	22.08.2013	09:25	1B766E
11	Dampeļu gatve 9	1243953	73,41	10L	22.08.2013	09:19	1B7E42
12	Pērkoņu iela 13	1134000755	4926,10	1L	31.05.2013	09:40	1B7846
13	Pērkoņu iela 17	1134000774	2066,93	1L	15.08.2013	10:55	1B7933
14	Pērkoņu iela 21 (Pansionāts)	1032006285	4309,67	10L	22.08.2013	09:09	1B7D90

Tabula nr: 2

Tabulās redzami sākotnējie rādījumi uzstādot (tabula nr.: 1) un apsekojums pēc trijiem mēnešiem (apsekojuma datumi variē, jo piekļuve privātajiem tīpašumiem ne vienmēr iespējama plānojama un atkarīga no tīpašniekiem). Dzeltēni iekrāsotās ailes atbilst rādījumiem, kas koriģējami, baltās ailes atbilst sistēmas rādījumiem. Redzams, ka nobīdes ir gandrīz visos ūdens patēriņa rādījumos. Cēlonis atšķirībām ir defektīvi raidītāji, problemātiska raidīšanas programmatūrā (kas izstrādes procesā tika novērstas), datu apstrādes servera darbības problēmas izstrādes periodā, kā arī pieļaujamās nolasīšanas kļūdas 3% ietvaros.

Pēc pilnā apsekojuma veikšanas tika veiktas gadījuma rādītāja pārbaudes (patvaļīgi izvēlētai pieejamai adresei) un konstatēts, ka reģistrētās patēriņa vērtības atšķiras pieļaujamo 3% kļūdas diapazonā.

Spiediena mērītāju rādījumus nav tiešā veidā iespējams pārbaudīt, tādēļ to rādījumi tiek interpretēti veicot salīdzinājumu ar SCADA ūdens tīkla segmenta ievades mēriekārtas rādījumiem. Spiediena mērījumu rādījumu interpretāciju un rādījumu atbilstību novērtē PSIA „Ūdekas” tehniskie darbinieki – novērtējums ir pozitīvs. Spiedienu mērījumi aktualizējas ik minūti un ir apskatāmi, kā arī eksportējami izmantojot izstrādāto informācijas sistēmu.

Sērijas №	Rādījums uz skalas bar	Pilna spiediena skala bar	Pēd. saņemš. laiks	Tehn. iek. numurs	Programmas versija
00006B	5,177	6	15.09.2013 17:57	00006B	12
000068	4,387	6	15.09.2013 17:56	000068	12
00006A	4,677	6	15.09.2013 17:55	00006A	12
000066	5,629	6	15.09.2013 17:57	000066	12
000064	5,613	6	15.09.2013 13:39	000064	12
000065	4,653	6	15.09.2013 17:56	000065	12
00006C	4,702	6	15.09.2013 17:56	00006C	12
000067	5,613	6	15.09.2013 17:56	000067	12
000032	4,073	6	15.09.2013 17:56	000032	12
FFF002	4,718	6	15.09.2013 17:57	FFF002	12

3.3. Secinājumi

Kopējā atbilstība vērtējama kā augsta, un atbilst produkcijas vides prasībām. Nobīdes un neprecizitātes projekta laikā skaidrojamas ar sistēmas aktīvo izstrādes fāzi. Ieteicamā metodoloģija sistēmas darbības traucējumu novēršanā, secīgi neatrisinot problēmu, ir:

1. Notikuma reģistrācija;

2. Datu saņemšanas traucējuma veida novērtēšana;
3. Vārteju darbības pārbaude/diagnostika;
4. Pārnēsāmā testera izmantošana raidītāja darbības pārbaudei (signāla stipruma novērtēšana - RSSI);
5. Raidītāja atvienošana un pārbaude;
6. Sensora atvienošana

„Smart Metering” sistēmas testēšanas atskaite

2.sadaļa. Ūdens noplūžu vietu lokalizācija

Projekts “Smart Metering” LLIV-312

Projekta mājas lapa: <http://www.smartmeteringproject.eu>

Testēšanas dalībnieki:

Ventspils augstskolas: pētnieks, Kaspars Kondratjevs

PSIA Ūdeka: PSIA „Ūdeka” tehniskās daļas vadītājs Viesturs Otomers

Septembris 2013
Versija 1.0

Satura rādītājs

1. Ievads.....	145
1.1. Testēšanas mērķi.....	145
1.2. Testēšanas norises vieta	145
1.3. Testēšanas norises laiks.....	146
1.4. Testēšanas dalībnieki.....	146
2. Testēšanas laikā izmantotās ierīces un aparatūra.....	146
3. „Smart Metering” sistēmas testēšanas rezultāti.....	148
3.1. Testēšanas metodika.....	148
3.2. Testēšanas rezultāti.....	149
3.3. Secinājumi.....	154
Pielikumi:.....	154

4. Ievads

4.1. Testēšanas mērķi

Ūdens noplūžu vietu lokalizācijas mērķis ir veikt izstrādāto noplūžu noteikšanas metožu praktisku pārbaudi izveidotajā izmēģinājuma tīklā.

Nesaistītās metrikas: sensoru vērtību izmaiņu temporālā analīze:

1. Spiediena vidējās, negatīvās fluktuācijas detektors:

Darbības principa pamatā spiediena vērtības novērošana lietotāja definētā laika periodā (dienas) un analizējot spiediena vērtības kritumus kā procentuālas daļas no lietotāja definētas vidējās vērtības robežas. Definētajam kritērijam jābūt patiesam lietotāja definētu laika periodu jeb aktivizācijas periodu, lai novērstu momentānās spiediena izmaiņas pie „lielajiem” patērētājiem vai ūdensvada atzariem.

2. Ūdens patēriņa minimālās plūsmas noplūžu detektors

Detektors mēra dienas ūdens patēriņu pie abonenta lietotāja definētā diennakts laika periodā, kad ūdens patēriņam vajadzētu būt minimālas (nakts stundas). Ja ūdens patēriņš pārsniedz lietotāja definēto robežvērtību procentos no vidējās vērtības lietotāja definētajā aktivizācijas periodā (dienās) tiek ģenerēts ūdens noplūdes notikums, kas liecina par patstāvīgu noplūdi abonenta ūdens apgādes sistēmā, piemēram tualetes ūdens rezervuāra vārsta defekts. Tā, ka ne visiem ūdens patērētājiem ir raksturīga ūdens patēriņa samazināšanās nakts stundās (uzņēmumi, iekārtas), tad iespējams atsevišķiem abonentiem šo funkciju deaktivizēt vai arī piemērot, lai novērstu nepatīkamas trauksmes.

3. Ūdens patēriņa (plūsmas) pozitīvās fluktuācijas noplūžu detektors

Darbības principa pamatā tiek veikta abonenta ūdens patēriņa analīze lietotāja definētā laika diapazonā (dienās). Perioda vidējā vērtība tiek salīdzināta ar lietotāja definētu procentuālu vērtības attiecību ar novēroto momentāno vērtību, ja lietotāja definētā aktivizācijas periodā (stundas) šī vērtība pārsniedz vidējo novērošanas perioda laiku, tiek ģenerēta noplūdes trausme, kas liecina par pēkšņu ūdens patēriņa pieaugumu. – noplūdi

4. Iekārtu dīkstāves, traucējumu detektors

Saistītās metrikas pamatā tiek pielietots hidrodinamiskais ūdens apgādes tīkla modelis. Šī modeļa ietvaros ūdens apgādes segments tiek uzskatīts kā izolēta sistēma, kur sensoru mērījumi ir sistēmas stāvokļa parametri un norāda uz tekošā momenta sistēmas stāvokli. Veicot tuvināto tīkla stāvokļa modelēšanu no faktiski zināmajiem tīkla struktūras elementiem (sistēmas ievada spiediena un plūsmas, kā arī patērētāju plūsmas) un novērotajiem datiem (spiediena mērījumiem), iespējams ekstrapolēt neatbilstības, kas norāda uz sistēmas anomālijām jeb potenciālām noplūdēm.

4.2. Testēšanas norises vieta

Testa punkts nr.: 1 - Kuldīgas ielas un Dampļu gatves krustojums (Kuldīgas iela 221A) – ugunsdzēsības hidrants

Testa punkts nr.: 2 – Kuldīgas ielas pagrieziens uz pansionātu un bērnu namu „Selga” (Kuldīgas iela 229A) – ugunsdzēsības hidrants



1

4.3. Testēšanas norises laiks

Testa punkts nr.: 1 – 15.08.2013 10:40:00 - 11:20:00

Testa punkts nr.: 2 – 15.08.2013 11:30:00 - 12:00:00

4.4. Testēšanas dalībnieki

No Ventspils augstskolas: pētnieks, Kaspars Kondratjevs

No PSIA Ūdeka: SIA „Ūdeka” tehniskās daļas vadītājs Viesturs Otomers

5. Testēšanas laikā izmantotās ierīces un aparātūra

Testēšanas laikā sensoru rādījumu novērošanai, interpretācijai un noplūžu analīzei tika izmantota projekta ietvaros izstrādātā informācijas sistēma un noplūžu noteikšanas moduļi.

Smart Metering

Sistēma Iestatījumi Saskaņe

Noplūžu detektora konfigurācija

Skatītāji

• Konfigurācija • Vērtība

Spiediena vidējo fluktuāciju noplūžu detektors

Viduvējošanas periods (dienas)

Procentuālās negatīvās fluktuācijas vērtība %

Aktivizācijas periods (sekundes)

Patēriņa minimāla plūsmas noplūžu detektors

Minimālā dīkstāves patēriņa robeža

Dīkstāves patēriņa laika diapazona sākums

Dīkstāves patēriņa laika diapazona beigas

Ne nulles mērtāji (iekārtu numuri atdalīti ar komatiem)

Aktivizācijas periods (dienas)

Plūsmas vidējās fluktuācijas noplūžu detektors

Viduvējošanas periods (dienas)

Procentuālās pozitīvās fluktuācijas vērtība %

Aktivizācijas periods (sekundes)

Visu iekārtu dīkstāves perioda detektors

Dīkstāves periods (stundas)

Vērtības

- Mērtāji
- Rādījumi
- Rādījumu stabilitāte
- Rādījumu saraksts
- Spiediena devāji
- Spiediena devāju rādījumi
- Spiediena devāju stabilitāte
- Spiediena devāju temperatūra
- Sūkņi
- Aquamon versijas
- Koda versijas
- Gala lietotāji
- Reģioni
- Kompānijas
- Cenas
- Eksporti
- Eksporta konfigurācija
- Notikumu pārlūks
- Notikumu pārlūka konfigurācija
- Noplūžu detektora konfigurācija
- Labot izvēni

Noplūžu detektora konfigurācijas parametri dažādām metrikām, iespējams definēt kopējo parametrus katrai sistēmas reģistrētajai iekārtai. Ja nepieciešams modificēt kādas iekārtas parametrus (būtiski tīkla gala iekārtām – spiediena gadījumā) – atbilstoši izvēlas vēlamo iekārtu no saraksta.

Notikumā pārlūka noplūžu un sistēmas notikumu saraksts:

- Vārtejas dīkstāves notikums
- Skaitītāja dīkstāves notikums
- Parsējamā e-pasta notikums (satur diagnostikas informāciju no vārtējām)
- Jauna eksporta notikums
- Spiediena noplūdes notikums
- Patēriņa noplūdes notikums
- Mērtāju noplūdes notikums
- Vārtejas savienojuma kļūdas notikums
- Rēķinu ģenerēšanas notikums
- Ienākošo datu samazināšanās notikums
- Ienākošo datu pārsniegšanas notikums
- Dienas limita pārsniegšanas notikums
- Mēneša limita pārsniegšanas notikums
- Spiediena apakšējās robežas notikums
- Spiediena augšējās robežas notikums

Limenis	Tips	Kods	Apraksts	Tekārta	Izraisītājs	Pazinojums	Datums	Iespējas
5	meters_leak	ML	Meters leak has been detected	Informācija		Values avg par 2 dienām = 33.4035087719298.		
5	decrease	DNV	Decrease of next values			Values delay par 7200 sekundēm = 787.333333333333.		
5	decrease	DNV	Decrease of next values			Values delay thresh par 7200 sekundēm ar 0.35% = 275.566666666667.		

Katra notikuma ģenerēšanas mainīgos iespējams apskatīt. Katrā jaunā tīklā, nepieciešams veikt parametru pielāgošanu, lai nodrošinātu maksimāli efektīvu metriku darbību.

6. „Smart Metering” sistēmas testēšanas rezultāti

6.1. Testēšanas metodika

Testēšanas veikšanai tika radītas mākslīgas ūdens noplūdes izmantojot ugunsdzēsības hidrانتus divās attālinātās pozīcijās ar dažādām tīkla sarežģītības īpatnībām. Pirmais tests tika veikts radot strauju noplūdi, otrais tests tika veikts radot lēnu noplūdi – netika radīts trieciens.

Projekta ietvaros izstrādātā informācijas sistēmas reģistrēja sensoru – spiediena devēju rādījumus, to vērtības nodod ūdens noplūžu noteikšanas modulim, kas veica atbilstošās skaitļošanas operācijas.

Pēc testa veikšanas tika analizēti iegūtie spiediena izmaiņu rādījumi, lai pielāgotu noplūžu detektoru parametrus šādu noplūžu noteikšanai.

Datu atlase testa punkts nr.: 1 spiediena izmaiņas no datu bāzes:

```
SELECT (
(
`readouts`.`value` -186
) * `meters`.`full_pressure_scale`
) /744
), `readouts`.`when`, `meters`.`number`
FROM `readouts`
LEFT JOIN meters ON `readouts`.`meter_id` = `meters`.`id`
WHERE `readouts`.`when` < '2013:08:15 11:24:40'
AND `readouts`.`when` > '2013:08:15 10:42:47'
AND `programm_version` =12
LIMIT 0 , 30
```

Datu atlase testa punkts nr.: 2 spiediena izmaiņas no datu bāzes:

```
SELECT (
(
`readouts`.`value` -186
) * `meters`.`full_pressure_scale`
) /744
), `readouts`.`when`, `meters`.`number`
FROM `readouts`
LEFT JOIN meters ON `readouts`.`meter_id` = `meters`.`id`
WHERE `readouts`.`when` < '2013:08:15 11:43:01'
AND `readouts`.`when` > '2013:08:15 10:55:03'
AND `programm_version` =12
LIMIT 0 , 30
```

Pārējās ūdens noplūžu metrikas tika testētas izmantojot references datus, kas savākti no izmēģinājuma tīkla un izvērtējot vērtību dinamiku, pielāgotas noplūžu noteikšanas metriku parametri. Šis attiecas uz

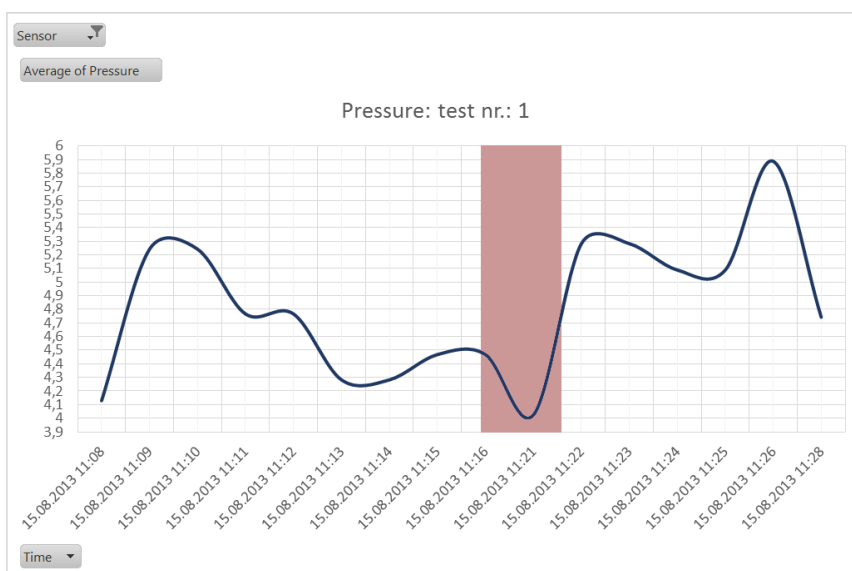
abonentu patēriņa dinamikā, kā pēkšņs patēriņa pieaugums vai iespējama nepamanīta noplūde, kuru konstatē izvērtējot vidējo nakts patēriņa izmaiņas – šīs metrikas ir lietotājam viegli interpretējamas un to vērtību robežvērtības tika noteiktas sadarbībā ar PSIA „Ūdeka” tehniskajiem speciālistiem.

Metrikas, kas atbilst spiediena kritiskajām robežām – minimuma, maksimuma sliekšņiem, tika noteiktas sadarbībā ar PSIA „Ūdekas” speciālistiem.

6.2. Testēšanas rezultāti

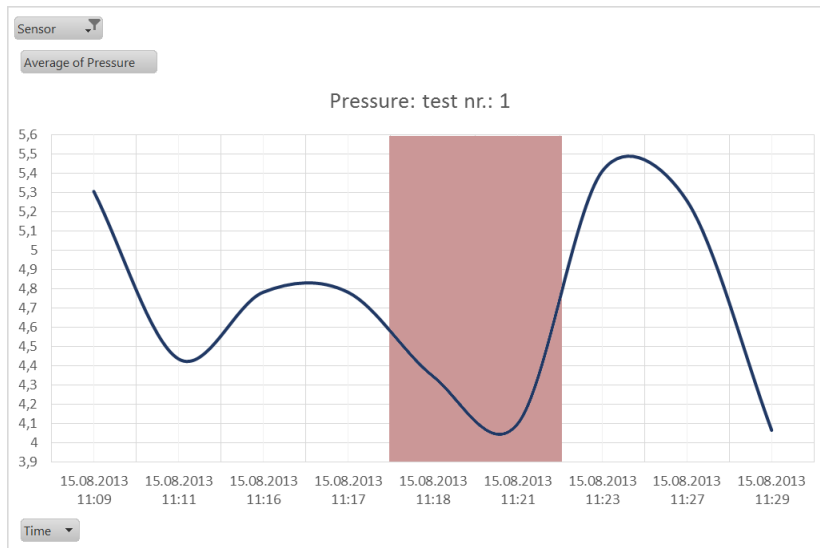
Testa punkts nr.: 1 – Strauja atvēršana

Sensor	000064
Row Labels	Average of Pressure
15.08.2013 11:08	4,129032258
15.08.2013 11:09	5,241935484
15.08.2013 11:10	5,241935484
15.08.2013 11:11	4,766129032
15.08.2013 11:12	4,766129032
15.08.2013 11:13	4,282258065
15.08.2013 11:14	4,282258065
15.08.2013 11:15	4,467741935
15.08.2013 11:16	4,467741935
15.08.2013 11:21	4,024193548
15.08.2013 11:22	5,282258065
15.08.2013 11:23	5,282258065
15.08.2013 11:24	5,088709677
15.08.2013 11:25	5,088709677
15.08.2013 11:26	5,887096774
15.08.2013 11:28	4,741935484
Grand Total	4,845430108

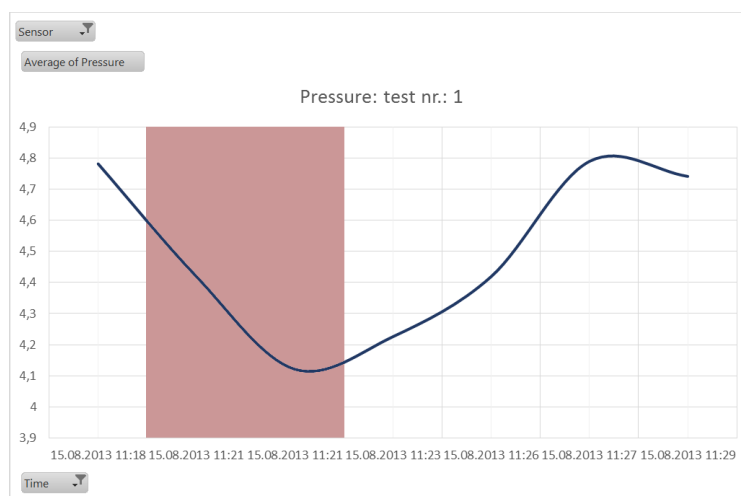


Sensor	000065
Row Labels	Average of Pressure
15.08.2013 11:09	5,306451613
15.08.2013 11:11	4,435483871

15.08.2013 11:16	4,782258065
15.08.2013 11:17	4,782258065
15.08.2013 11:18	4,346774194
15.08.2013 11:21	4,096774194
15.08.2013 11:23	5,411290323
15.08.2013 11:27	5,258064516
15.08.2013 11:29	4,064516129
Grand Total	4,752971138

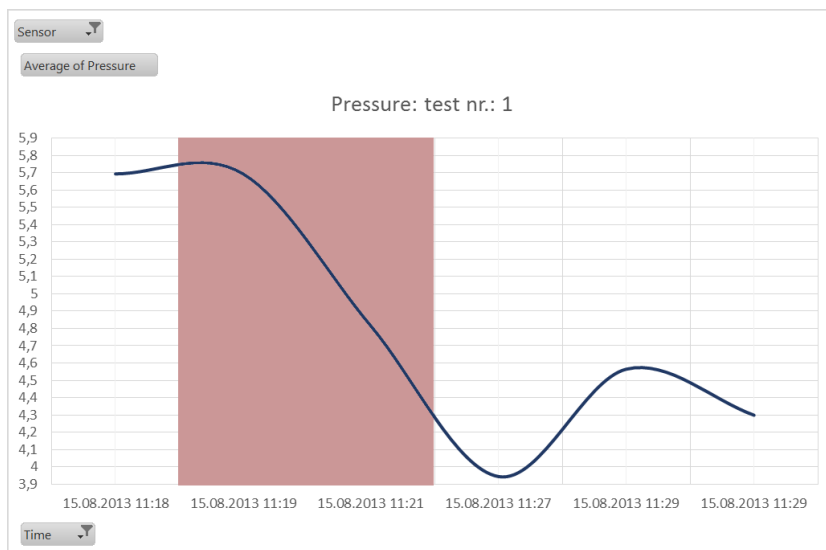


Sensor	00006A
Row Labels	Average of Pressure
15.08.2013 11:18	4,782258065
15.08.2013 11:21	4,419354839
15.08.2013 11:21	4,120967742
15.08.2013 11:23	4,225806452
15.08.2013 11:26	4,419354839
15.08.2013 11:27	4,790322581
15.08.2013 11:29	4,741935484
Grand Total	4,443548387



Sensor	00006B
--------	--------

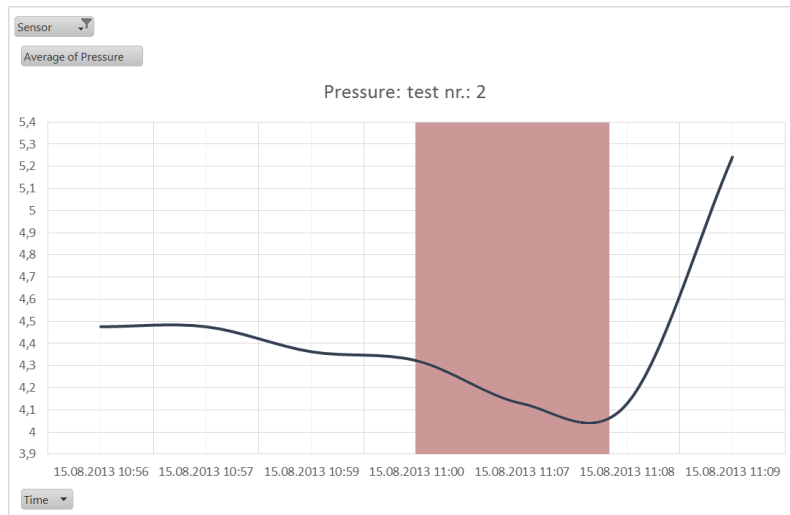
Row Labels	Average of Pressure
15.08.2013 11:18	5,693548387
15.08.2013 11:19	5,693548387
15.08.2013 11:21	4,814516129
15.08.2013 11:27	3,943548387
15.08.2013 11:29	4,564516129
15.08.2013 11:29	4,298387097
Grand Total	5,042521994



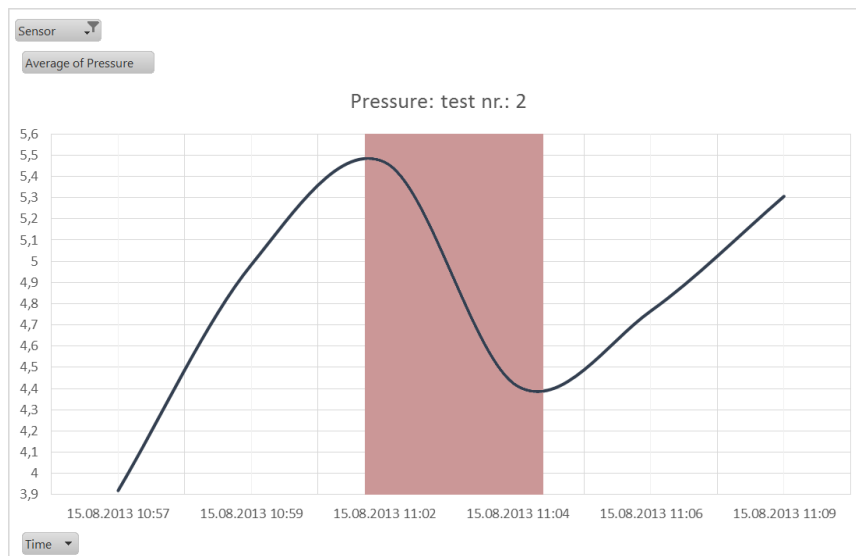
Testa punkts nr.: 2 – lēna atvēršana

Sensor	000064
--------	--------

Row Labels	Average of Pressure
15.08.2013 10:56	4,475806452
15.08.2013 10:57	4,475806452
15.08.2013 10:59	4,362903226
15.08.2013 11:00	4,322580645
15.08.2013 11:07	4,129032258
15.08.2013 11:08	4,129032258
15.08.2013 11:09	5,241935484
Grand Total	4,451612903

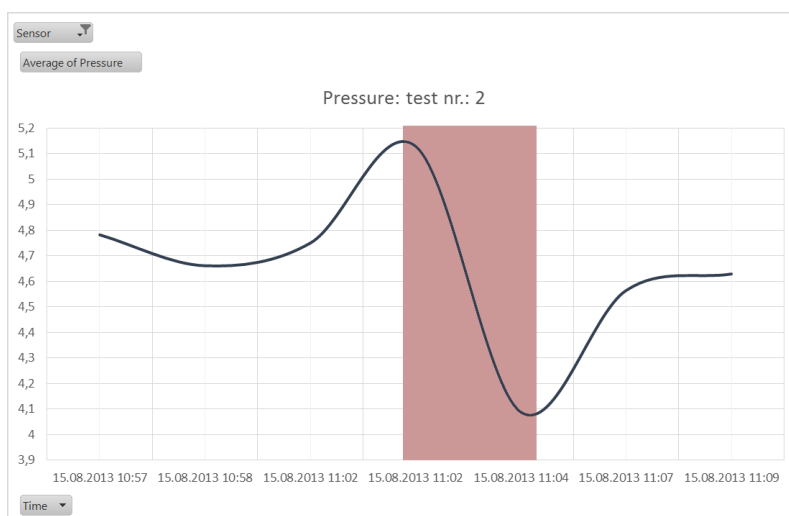


Sensor	000065
Row Labels	Average of Pressure
15.08.2013 10:57	3,919354839
15.08.2013 10:59	4,983870968
15.08.2013 11:02	5,467741935
15.08.2013 11:04	4,411290323
15.08.2013 11:06	4,766129032
15.08.2013 11:09	5,306451613
Grand Total	4,809139785

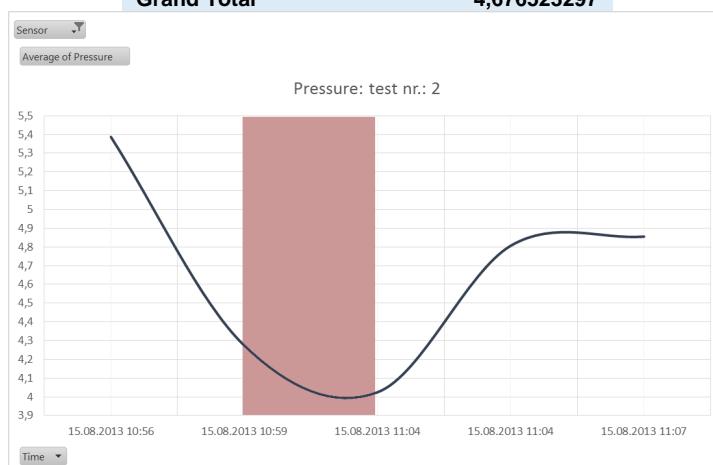


Sensor	00006A
Row Labels	Average of Pressure
15.08.2013 10:57	4,782258065
15.08.2013 10:58	4,661290323
15.08.2013 11:02	4,75
15.08.2013 11:02	5,129032258
15.08.2013 11:04	4,088709677
15.08.2013 11:07	4,564516129

15.08.2013 11:09	4,629032258
Grand Total	4,799193548



Sensor	00006B
Row Labels	Average of Pressure
15.08.2013 10:56	5,387096774
15.08.2013 10:59	4,274193548
15.08.2013 11:04	4,024193548
15.08.2013 11:04	4,806451613
15.08.2013 11:07	4,85483871
Grand Total	4,676523297



Testēšanas rezultātos attēlotās atlasēs vērtības un periodu nobīdes radušās dēļ iztrūkstošiem datiem, testa momenta. Izslēgti arī rādījumi, kas nekvalificējas noplūžu detektora aktivizācijai, kā īpaši raksturīgs pēkšņas noplūdes gadījumā, kad tīklā parādās īslaicīgs triecienvilnim līdzīgs uzvedības spiediena izmaiņas, kas norims un pāriet spiediena krituma turpinoties ūdens noplūdei. Svarīgi ir ņemt vērā lēnās noplūdes pieauguma tempu, nekorekta parametru izvēle, kā viduvējošanas periods var novest pie noplūdes nenoteikšanas.

6.3. Secinājumi

Pēc sākotnējo metriku parametru pielāgošanas, noplūžu simulācija reālos apstākļos ģenerēja notikumu pārliūkā, tādējādi tiek uzskatīts, ka tests izpildīts veiksmīgi.

Metriku parametrizācija būtu jāautomatizē ieviešot autonomus pašapmācības algoritmus. Šo funkciju var nodrošināt kombinējot un papildinot integrēto EPANET solveri, kas nodrošina tīkla analītisku modelēšanu izmantojot momentānos un vēsturisko tā stāvokļa datus.

3. Pielikumi:

PSIA Ūdeka Tehniskās daļas vadītājs V.Otomers veic mākslīgas noplūdes ar hidranta palīdzību.



