LAUREA AMMATTIKORKEAKOULU Uuden edellä

Automaattisen hälytys- ja häiriöilmoitushallinnan laadun kehittäminen

Pekki, Teemu

2013 Espoo

Laurea-ammattikorkeakoulu
Laurea Leppävaara

Automaattisen hälytys- ja häiriöilmoitushallinnan laadun kehittäminen

Teemu Pekki
Tietojenkäsittely
Opinnäytetyö
Kesäkuu, 2013

Laurea-ammattikorkeakoulu **Tiivistelmä**
Laurea Leppävaara
Tietojenkäsittely

Teemu Pekki

Automaattisen hälytys- ja häiriöilmoitushallinnan laadun kehittäminen

Vuosi 2013 Sivumäärä 39

Opinnäytetyön aiheena oli tutkia keinoja vähentää tietoliikenneoperaattori Elisa Oyj:n automaattisesti luotuja aiheettomia häiriöilmoituksia ja parantaa hälytys- ja häiriöilmoituskäsittelyn laatua. Lisäksi tavoitteena oli avata hälytyshallintajärjestelmän logiikkaa.

Teoreettisessa osuudessa selvitettiin tietoliikenneoperaattorin verkonhallinnan sekä automaattisen hälytys- ja häiriöilmoitushallinnan toimintaa. Lisäksi hälytysten korrelaatiotekniikoiden selvittäminen oli keskeistä hälytyshallinnan paremmaksi ymmärtämiseksi. Tutkimuksessa käytettiin kvantitatiivista tutkimusmenetelmää.

Häiriöilmoitushallinta osoittautui problemaattiseksi, jos automaattisen hälytyshallinnan toimintatapaa ei tunneta tarpeeksi hyvin. Häiriöilmoituksien vähentäminen edellyttää jatkuvaa optimointia hälytyshallinnan korrelaatiotekniikoissa, koska verkon tiedot ja monimuotoistuva rakenne ovat nopeasti muuttuvia. Myös eri teknologioiden erityispiirteet muodostavat haasteita hälytyshallinnan tehokkaaseen optimoimiseen.

Hälytyshallintajärjestelmän tietokannan tiedosta ei ollut aikaisempaa analyysia, joten pääkomponenttien löytämiseksi tehtiin pääkomponenttianalyysi. Suuresta joukosta muuttujia noin 93 % muuttujien varianssista selittyi neljällä eri pääkomponentilla. Pääkomponentit nimettiin seuraavasti: kohde, aika, viesti ja ryhmä. Lisäksi analyysin avulla löydettiin häiriöilmoituksia, joiden alkuperäinen hälytysviesti oli kuittautunut. Tämän pohjalta tehtiin kehityshanke hälytys- ja häiriöilmoitushallintajärjestelmien integroimiseksi, jotta kahdensuuntaiset toiminnot näiden kahden eri järjestelmän välillä onnistuu. Tämä tuo noin 19 % säästön turhissa häiriöilmoituksissa sekä turhan manuaalisen työn määrässä noin 1,26 työkuukauden säästön vuositasolla.

Verkonhallinta, Tietoliikenneoperaattori, Palvelunhallinta, Hälytyshallinta, Vikatiketti, Häiriöilmoitus, Häiriöilmoitushallinta, Vianhallinta, Pääkomponenttianalyysi

Laurea University of Applied Sciences **Abstract**
Laurea Leppävaara
Bachelor's Degree Program in Business information Technology

Teemu Pekki

Improving the quality of the automatic alarm and fault notification management

Year 2013 Pages 39

The purpose of this thesis was to reduce a network operator Elisa Oyj's automatically generated unnecessary fault notifications, to improve the quality of the alarm and fault notification management and also to clarify the logic of the alarm management.

The theoretical part of the thesis examines the topics of the network management as well as the topics of the automatic alarm management and the fault notification management. In addition, the theoretical section also studies the correlation techniques for better understanding of the alarm management. Methods of quantitative research were used in this thesis.

The fault notification management was problematic, if the procedures of the alarm management were unclear. Reducing unnecessary fault notifications require continuous optimizing of the alarm correlation techniques, because of the nature of the volatile information and the growing diverse structure of the network. Also the individual features of the technologies bring challenges for the efficient alarm management optimization.

There was no previous data analysis of the alarm data; therefor principal component analysis was made. Four different principal components were found from a large amount of the variables. These components explained circa 93 % of the total variance and they were named in the following way: object, time, message and group. Also the data analysis revealed fault notifications where the alarm message was acknowledged. Based on this finding a proposal for the integration of the alarm management and the fault notification management systems were made. This procedure will reduce unnecessary fault notifications by circa 19 % per year and savings on the unnecessary manual work will be circa 1,26 working months per year.

Alarm management, Fault management, Fault notification, Trouble ticket, Principal component analysis, Network operator, Network management, Service management

Sisällys

1 Johdanto

Tietoliikenneoperaattorin alati kasvavassa palvelutarjonnassa automaattisten toimintojen merkitys kasvaa jatkuvasti. Automaattiset toiminnot tulevat tulevaisuudessa syrjäyttämään monia manuaalisia töitä, kuten esimerkiksi viankorjauksen eri tehtäviä. Suuressa merkityksessä tällöin ovat automaattiset hälytyshallintajärjestelmät ja niihin integroidut verkonhallinnan eri järjestelmät. Automaattisten hälytyshallintajärjestelmien tehokkaaseen hyödyntämiseen liittyy vianhallinnan häiriöilmoitushallintajärjestelmä. Vianhallinta ottaa viankorjaukseen tehtäviä vastaan häiriöilmoitushallintajärjestelmän avulla, jolloin hälytysviestejä ei tarvitse monitoroida reaaliajassa. Nämä järjestelmät liittyvät vahvasti toisiinsa ja niiden jatkuva optimointi on välttämätöntä, jotta vianhallinnan voimavarat suuntautuvat aitoihin vikoihin.

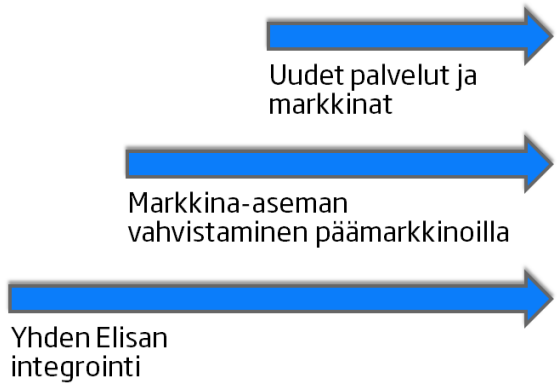
Tutkimus tehtiin Elisa Oyj:n tilaamana ja tutkimuksessa pureudutaan ongelmakohtiin verkonhallinnan automaattisessa hälytys- ja häiriöilmoitushallinnassa pyrkimällä löytämään ratkaisuja laadun parantamiseksi mahdollisimman kattavalla tavalla. Tutkimusta tehtiin kvantitatiivisen tutkimuksen menetelmien mukaisesti.

1.1 Elisa Oyj

Elisa Oyj kuuluu Suomen suurimpiin tietoliikenne ja ICT-alan yrityksiin. Sen asiakkaana on noin 2,3 miljoonaa kuluttajaa, yritystä ja julkishallinnon organisaatiota (Elisa Oyj 2012). Elisan keskeisimmät tuotteet ja palvelut liittyvät matkapuhelinverkkoihin ja liittymiin, kaapelitelevisioliittymiin sekä tietoliikenneverkkoihin ja liittymiin. Liikevaihtoa Elisalla oli vuonna 2012 1,553 miljardia euroa ja liikevaihto kasvoi 2 % vuodesta 2011 (Tilinpäätös 2012).

Kuvio 1: Elisa Oyj Toimintamalli (Elisa Oyj 2012)

Elisan toimintamallissa (Kuvio 1) asiakasyksiköt ovat jaoteltu maantieteellisiin alueisiin, joita tukee eri tulos- ja tukiyksiköt sekä segmentit. Toimintamallin ulkopuolelle jäävät Elisa Eesti sekä muut erillisyhtiöt, joista Elisa omistaa eri osuuksia (Organisaatio 2012).



Kuvio 2: Elisa Oyj Strategia (Elisa 2012)

Yritysostojen takia Elisalla on monia eri järjestelmiä ja osastoja jotka eivät osin täysin pysty hyödyntämään toisiaan tai omaavat päällekkäisiä toimintoja. Tämän takia Elisan yhtenä strategiana on yhden Elisan integrointi (Kuvio 2).

1.2 Aikaisemmat tutkimukset

Toisesta Elisan automaattisen hälytyshallintajärjestelmän kehittämisestä valmistui diplomityö vuoden 2012 elokuussa (Mäkelä 2012). Tutkimusta ei suoranaisesti voi käyttää apuna tässä työssä johtuen järjestelmän erilaisesta luonteesta, mutta pääpiirteet hälytyskeräilyssä ovat samankaltaisia. Kyseinen järjestelmä keskittyy Elisan yritysasiakkaiden IP-pohjaisiin laitteisiin ja palveluihin. Näillä kahdella eri järjestelmällä on vähäistä hälytysviestien välitystä, mutta ei varsinaista integraatiota. Kummastakin hälytyshallintajärjestelmästä muodostuneet häiriöilmoitukset esitetään samassa raportissa. Tässä työssä tutkittava hälytyshallintajärjestelmä käsittää laajan joukon erilaisia tietoliikennelaitteita ja järjestelmiä. Kyseisen hälytyshallintajärjestelmän piirissä olevien häiriöilmoituskäsittelyryhmien hälytyskeräilyn optimointipyyntöprosessit ja annetut rikastustiedot poikkeavat toisistaan. Tästä hälytyshallintajärjestelmästä ei ole tehty aikaisempia tutkimuksia, joten työlle oli selkeä tilaus. Yhteistyötä integraation ja korrelaation lisäämiseksi näiden kahden eri hälytyshallintajärjestelmien välille kannattaa tutkia lisää.

1.3 Työn sisältö ja rakenne

Aihetta rajattiin kahdesta automaattisesta hälytyshallintajärjestelmästä toiseen. Rajaus oli välttämätön, koska nämä järjestelmät ovat toiminnaltaan erilaisia. Jotta työstä on mahdollisimman suuri hyöty työn tilaajalle, esitellään riittävän kattavasti työhön liittyvät järjestelmät, työkalut ja käsitteet Tämä auttaa tapahtuma-, ongelma-, ja palvelunhallintaa hahmottamaan mahdollisuuksia kohti parempaa järjestelmien optimointia ja automaation tuomaa hyötyä.

Työssä viitataan häiriöilmoituslukujen osalta raportteihin, joita on kerätty marraskuun 2012 ja maaliskuun 2013 aikana. Häiriöilmoitusaportit ovat haettu vuoden 2012 jokaiselta kuukaudelta erikseen ja koottu yhdeksi isoksi koko vuoden raportiksi analysointia varten. Hälytysviestien osalta työssä viitataan hälytyshallintajärjestelmän tietokantaraporttiin, joka on haettu 10.1.2013. Raportti pitää sisällään 1067320 kappaletta hälytysviestejä, joka on tarpeeksi suuri otanta kuvatakseen verkon toimintaa (Asiantuntijahaastattelu 2012).

Hypoteesit:

1. Aiheettomia ja monistuvia häiriöilmoituksia muodostuu.
2. Hälytyshallintajärjestelmän tapahtumien optimointia korrelaatiossa ja suodatuksessa ei ole täysin hyödynnetty.

Tutkimuskysymykset:

1. Millä keinoin hälytyshallintajärjestelmästä muodostuneiden aiheettomien ja monistuvien häiriöilmoitusten määrää saadaan vähennettyä?
2. Millä keinoin hälytyshallintajärjestelmän hälytyskeräilyn ja tapahtumahallinnan optimointia saadaan kehitettyä

Luvuissa 2. ja 3. paneudutaan tutkielman kannalta välttämättömiin teoriaosuuksiin, keskeisiin käsitteisiin ja järjestelmiin sekä tekemääni kehityshankkeeseen. Järjestelmien esitteleminen on tärkeää, jotta tutkimuksen kokonaiskuvasta saa riittävän selkeän kuvan. Luvussa 4. käydään läpi tiedon hakuun ja esiprosessointiin liittyvät asiat, jonka jälkeen pääkomponenttianalyysi esitellään luvussa 5. Viimeiseksi luvussa 6. esitellään työn tulokset sekä jatkokehitysideat.

2 Katsaus tietoliikenneoperaattorin toimintaan ja keskeisiin käsitteisiin

Tietoliikenneoperaattorin toimintaan liittyy monia eri osa-alueita ja käsitteitä, joista tässä esitellään tutkimuksen ja verkonhallinnan kannalta keskeisimmät. Teoriaosuuden käsitteistössä on esitetty ITIL (Information Technology Infrastucture Library) prosessikehyksen käytäntöjä. Kyseinen prosessikehys on käytössä useimmissa suurissa yrityksissä, kuten myös tutkimuksen tilaajayrityksessä. Suurta joukkoa teknologioista ei koettu tarpeelliseksi käsitellä, koska tutkimuksen kannalta se ei tuo oleellista informaatiota työhön.

2.1 Verkonhallinta ja palvelunhallinta

Verkonhallintaan kuuluu joukko toimintoja, joilla verkon eri osa-alueita hallitaan, allokoidaan, suunnitellaan, monitoroidaan, otetaan käyttöön ja koordinoidaan. Verkonhallinta voidaan käsittää rakenteeksi, joka sisältää useita eri tasoja. Näitä tasoja ovat: liiketoiminnan hallinta, palvelunhallinta, verkonhallinta, elementinhallinta ja verkkoelementinhallinta. Nämä tasot ovat hierarkkisesti tarkentuvia liiketoiminnan hallinnasta alaspäin. (Farrel 2011, 91-92).

Palvelunhallinnan tehtävänä on taata organisaation vaatimusten mukainen palveluiden toimitus ja tuki. Palvelunhallinta hyödyntää informaatio teknologian eri voimavaroja sekä ihmisiä että prosesseja tukeakseen liiketoiminnan operatiivisia tarpeita. Lisäksi palvelunhallinta takaa organisaation kyvyn nopeaan reagointiin suunnittelemattomiin tapahtumiin ja jatkuvan kehityksen prosesseissa ja suorituskyvyssä. (Abby 2007, 45-46).

2.1.1 Tapahtumanhallinta

Tapahtuma on tapaus, joka aiheuttaa tai voi aiheuttaa häiriön palvelun laatuun. Tapahtumanhallinnalla pyritään palauttamaan palvelu normaalitasolle mahdollisimman nopeasti ja minimoimaan mahdolliset vaikutukset liiketoimintaan. (Thejendra 2008, 72-73). Tapahtumanhallintaan kuuluu seuraavat vaiheet: tapahtuma, tunnistus, tallennus, tutkimus, diagnoosi, eskalointi ja ratkaisu (Computer Associates 2007, 29-34). Tapahtumanhallinta on usein ensimmäinen kontakti viankorjauksessa.

Liikaa muodostuvissa häiriöilmoituksissa on riskinä, että tärkeät häiriöilmoitukset jäävät vähemmälle huomiolle. Lisäksi itse häiriöilmoituksen sisällön liika informaatio tai sen puute tekee tapahtumanhallinnan vaikeaksi ja hitaaksi. Tapahtumanhallinnan toimintaa auttavat yhä

älykkäämmät järjestelmämonitorit ja työkalut, jotka osaavat tulkita muutoksia reaaliajassa. (Abby 2007, 145-158)

2.1.2 Ongelmahallinta

Ongelma on tapahtuma tai joukko tapahtumia joiden juurisyytä ei tunneta. Ongelmanhallinta on prosessi, joka tutkii tapahtuman tai tapahtumajoukon juurisyyn. Tehokas ongelmahallinta estää tapahtumien uudelleensyntymisen. Ongelmanhallinnalla on sekä proaktiivinen että reaktiivinen rooli. Proaktiivisella ongelmahallinnalla pyritään tunnistamaan ongelmat ennen tapahtumien syntymistä. Reaktiivisella ongelmanhallinnalla puututaan ongelmiin näiden syntymisen jälkeen. Ongelmanhallinnan osaston päävastuut ovat Thejandran (2008) mukaan 1) Ongelman kontrollointi 2) Virheen kontrollointi 3) Ongelmien proaktiivinen estäminen 4) Kehityssuuntien tunnistaminen 5) Hallintaraportit 6) Merkittävien ongelmien tilannekatsaus (Thejendra 2008, 82-84).

Yleisin tapa tutkia tapauksia ja tapahtumia on analysoida aineistoja tilastollisesti, jotta ongelmakohdat liiketoiminnalle löytyvät. Usein analyyseja esitetään vain yksinkertaisilla kuvaajilla ja kunnolliset tilastollisen menetelmän analyysit jäävät hyödyntämättä. Tilastollisilla menetelmillä voidaan ennustaa, löytää kehityssuuntia ja tunnistaa korrelaatioita useista tekijöistä. Nämä menetelmät ovat korvaamaton voimavara informaatioteknologian suorituskykytiedon, juurisyyn ja mahdollisten ongelmien analysoinnissa. (Abby 2007, 174-175).

2.1.3 Palveluehtohallinta

Palveluehtohallinnan prosessin tarkoituksena on valvoa ja taata, että palvelujen laatu täyttää niille asetetut kriteeri. Lisäksi palveluehtohallinta monitoroi suorituskykyä ja pyrkii ehkäisemään palveluehtosopimusten rikkeitä. (Abby 2007, 276).

Palveluehtosopimus on palvelun tuottajan ja asiakkaan kirjallinen sopimus, jossa määritellään mittarit palveluille ja hyväksyttävät sekä hyväksymättömät palvelutasot. Yritysten toiminta on riippuvainen suurilta osin luotettavasta tietoliikennepalvelusta. Tietoliikennepalvelut vaikuttavat suoranaisesti yrityksen luotettavuuteen, maineeseen ja tietoturvaan. Tämän takia asiakkaat vaativat palveluehtosopimusta tietoliikennepalveluista. (Thejendra 2008, 127-128).

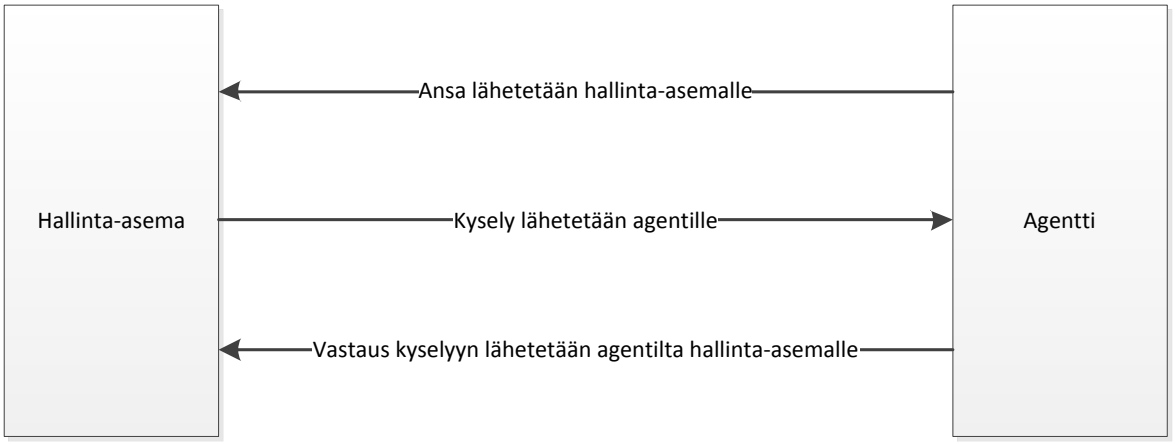
2.2 Yksinkertainen verkonhallintaprotokolla

Yksinkertainen verkonhallintaprotokolla eli SNMP (Simple Network Management Protocol) on joukko toimintoja ja tietoa, jolla ylläpitäjä valvoo ja hallinnoi tietoverkon eri laitteita. Kaikki laitteet jotka pystyvät vastaanottamaan SNMP – tietoa ovat hallinnoitavissa. SNMP:n avulla

voidaan mm. sammuttaa ja käynnistää laitteita, seurata verkon nopeutta ja valvoa lämpötiloja. (Douglas & Schmidt 2008, 1)

NMS (Network Management Station) eli verkon hallinta-asema on palvelin mihin on asennettu ohjelmisto, mikä vastaanottaa ja käsittelee SNMP trap –viestejä agenteilta. Esimerkiksi laitteen agentti lähettää viestin SNMP trap –muodossa NMS:lle vikaantuneesta laitteesta ja NMS eskaloi viestin eteenpäin vianhallintaan. (Douglas & Schmidt 2008, 3-4)

Agentti on ohjelma, joka asennetaan valvottavaan laitteeseen tietoverkossa. Agentti lähettää SNMP trap –muodossa olevan tiedoston NMS:lle jatkokäsittelyyn. NMS voi lähettää agentille kyselyn laitteen tilasta ja suorittaa tämän jälkeen tarvittavat jatkotoimet (Hakala & Vainio 2005, 323). SNMP agentit ovat yleensä esiasennettuina IP-pohjaisiin laitteisiin jo valmiiksi.



Kuvio 3. SNMP trap kulku agentin ja hallinta-aseman välillä. (Muokattu kuviosta Douglas & Schmidt 2008, 4)

Ansa eli trap on keino agentille lähettää tarvittavaa tietoa hälytyshallintajärjestelmälle (Kuvio 3.). NMS:n voi määritellä reagoimaan erilaisiin trap-viesteihin (Douglas & Schmidt 2008, 182). Hälyttävän laitteen tiedot näkyvät trap-viestissä, kuten: IP-osoite, trap-tapahtuman aikaleima, lähettäjän ja vastaanottajan tiedot, yhteisö sekä objektin tunniste (Hakala & Vainio 2005, 327).

Hallintatietokantaan eli MIB-tietokantaan (Management Information Base) määritellään kohteet, jotka pitävät sisällään hälyttävien laitteiden tiedot ja tietotyypit. Näitä kohteita on standardin mukaisia pakollisia sekä yksityisiä laite- ja ohjelmistovalmistajille että omia järjestelmäkohtaisia. Luvussa 2.4.1 esitelty hallinta-asema suorittaa sille määritellyn MIB-

tietokannan kohteen perusteella kyselyn, johon agentti vastaa palauttamalla sille määritellyn kohteen. (Hakala & Vainio 2005, 325).

2.2.1 Lokitieto

Lokiviesti on viesti esimerkiksi tietokonejärjestelmältä, laitteelta tai ohjelmistolta jonkinlaisen ärsykkeen seurauksena. Tämä ärsyke voi olla esimerkiksi kirjautumisloki Unix järjestelmästä, palomuurin ACL-viesti tai levytallennusjärjestelmän häiriö. Lokiviestin lokitieto sisältää tarvittavan informaation. Tämä informaatio voi olla luonteeltaan informatiivinen tai kertoa testistä, virheestä ja hälytyksestä. Tyypillisesti lokiviesti sisältää perustietona aikaleiman, lähteen ja tiedon. Nämä perustiedot ovat mukana erilaisissa lokiviesteissä, kuten järjestelmälokissa, Microsoftin tapahtumalokissa ja tietokantaan tallennetussa lokissa. (Chuvakin, Schmidt & Phillips 2012, 2-6).

2.3 Rakenteellinen kyselykieli

Rakenteellinen kyselykieli eli SQL (Structured Query Language) on IBM:n kehittämä standardoitu kyselykieli, jolla voidaan manipuloida relaatiotietokantaa. Tämä kyselykieli soveltuu hyvin relaatiotietokantaan, koska kyselyt tehdään tauluina. Tämän avulla uusia tauluja voidaan tallentaa relaatiotietokantaan kyselyn avulla. (Beaulieu 2009, 7).

SQL kyselykieli koostuu useista lausekkeista, jotka tekevät kolmea erilaista toimintoa. Näillä toiminnoilla voidaan määritellä tietoa, muokata tietoa ja hallita tietoa. Useimmiten käytetty muokkaustapa on hakea valittua tietoa tietokannasta. SELECT lauseella voidaan hakea tietokannasta erilaista informaatiota. Lauseella voidaan määritellä taulukot ja rivit mitä halutaan hakea, mutta yleisesti on tapana hakea taulun kaikki rivit. (Taylor 2010, 26 & 140).

2.4 Juurisyyanalyysi

Juurisyyanalyysilla ei ole yleisesti hyväksyttyä määritelmää, mutta sillä tarkoitetaan ongelman todellisen syyn löytämistä ja tarvittavien toimien tekemistä ongelman poistamiseksi. Vaikka juurisyyanalyysi on vianselvityksen osa, sillä on olennainen osa organisaation jatkuvassa kehityksessä. Juurisyyanalyysissa käytetään laajaa joukkoa eri menetelmiä ja tekniikoita ongelmien syiden paljastamiseksi. (Andersen & Fagerhaug 2006, 11-13)

Juurisyyanalyysi tuottaa myös tärkeää tietoa tulevaisuuden suunnittelun varalle. Tehokkaalla juurisyyanalyysilla voidaan oppia ongelmista ja estää jatkossa samankaltaisten ongelmien synty. Juurisyyanalyysia voidaan käyttää täten hyväksi proaktiivisessa viankorjauksessa. (Wilson, Dell & Anderson 1993, 32)

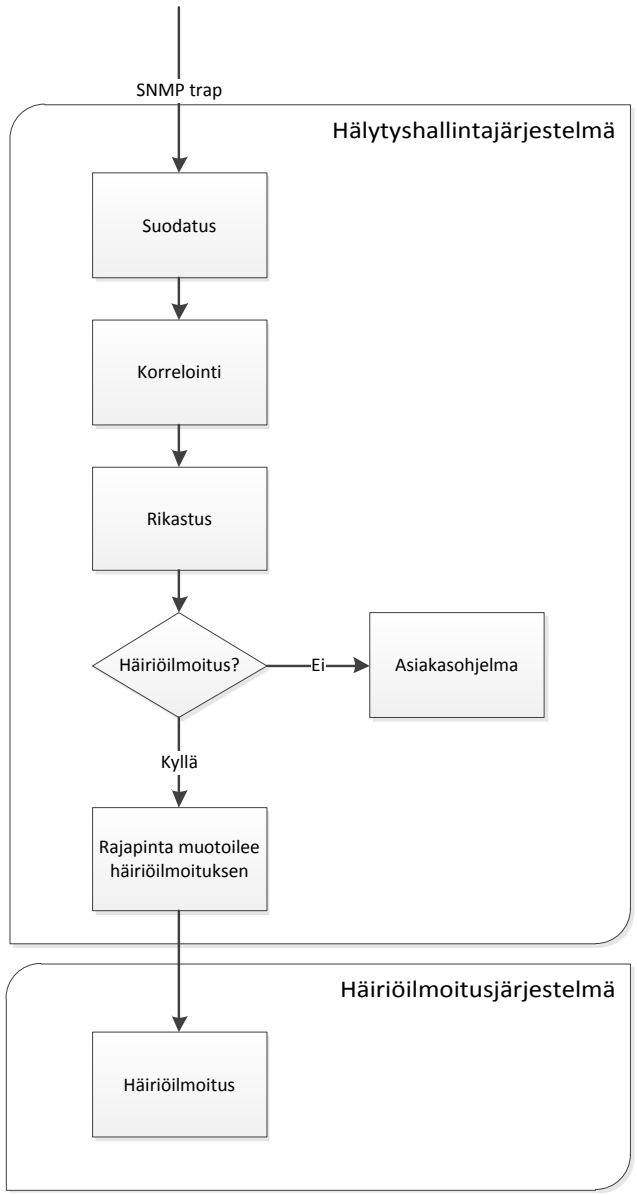
Juurisyyanalyysista voidaan kehittyä kohti automaattista ennakointi- ja vaikutusanalyysia. Ennakoiva analyysi on tilastollisen tiedon analysoinnin ja tiedonlouhinnan yhdistelmä. Tavalla pyritään löytämään tulevia ongelmia etukäteen, etsimällä tiettyjä kaavoja ja ennustamaan niiden syntymistä. Juurisyyanalyysissa käytetään yleensä häiriöitä tiedon lähteenä, mutta ennakoivassa analyysissa käytetään suorituskykyä ja tilastollisia yhteenvetoja tiedon lähteenä. (Comprehensive report 2003, 86)

3 Automaattinen hälytys- ja häiriöilmoitushallinta

Tämän luvun kappaleissa viitataan julkaisemattomiin sisäisiin dokumentteihin, tiedostoihin, raportteihin ja asiantuntijahaastatteluihin. Tietoturvan takia tarkat nimet ovat korvattu yleisnimillä ja asiaa tai tapahtumaa parhaiten kuvaavilla nimillä.

Automaattiseen hälytys- ja häiriöilmoituskäsittelyyn tarvitaan kahden eri järjestelmän tehokasta yhteistoimintaa. Yhteistyö täytyy olla saumatonta teknisesti, mutta myös järjestelmiä käyttävien ryhmien välillä. Valvottavilla laitteilla ja palveluilla ovat omat erityisominaisuutensa, joiden hälytyshallintaan tarvitaan häiriöilmoituskäsittelyryhmien osaamista. Tämän takia häiriöilmoituskäsittelyryhmien tulee olla selvillä hälytysten suodatus- ja korrelointitekniikoista. Ongelmanhallinnan prosessia voidaan hyödyntää, jos säännöstöjen luomisessa muodostuu ongelmia.

Yksinkertaistettuna hälyttävän laitteen SNMP trap kulkee verkosta hälytyshallintajärjestelmään, jossa siitä muodostuu hälytysviesti, joka muotoillaan häiriöilmoitukseksi häiriöilmoitushallintajärjestelmään. Prosessi voi olla hyvin yksinkertainen tai monimutkainen riippuen monista eri muuttujista. Keskeisiä muuttujia ovat esimerkiksi laitteiden asetukset ja toimintatapa, hälytysten määrä ja tapahtumien korrelaatiot. Nämä vaikuttavat siihen miten hälytyshallintajärjestelmän korrelaatiosäännöt muodostetaan.

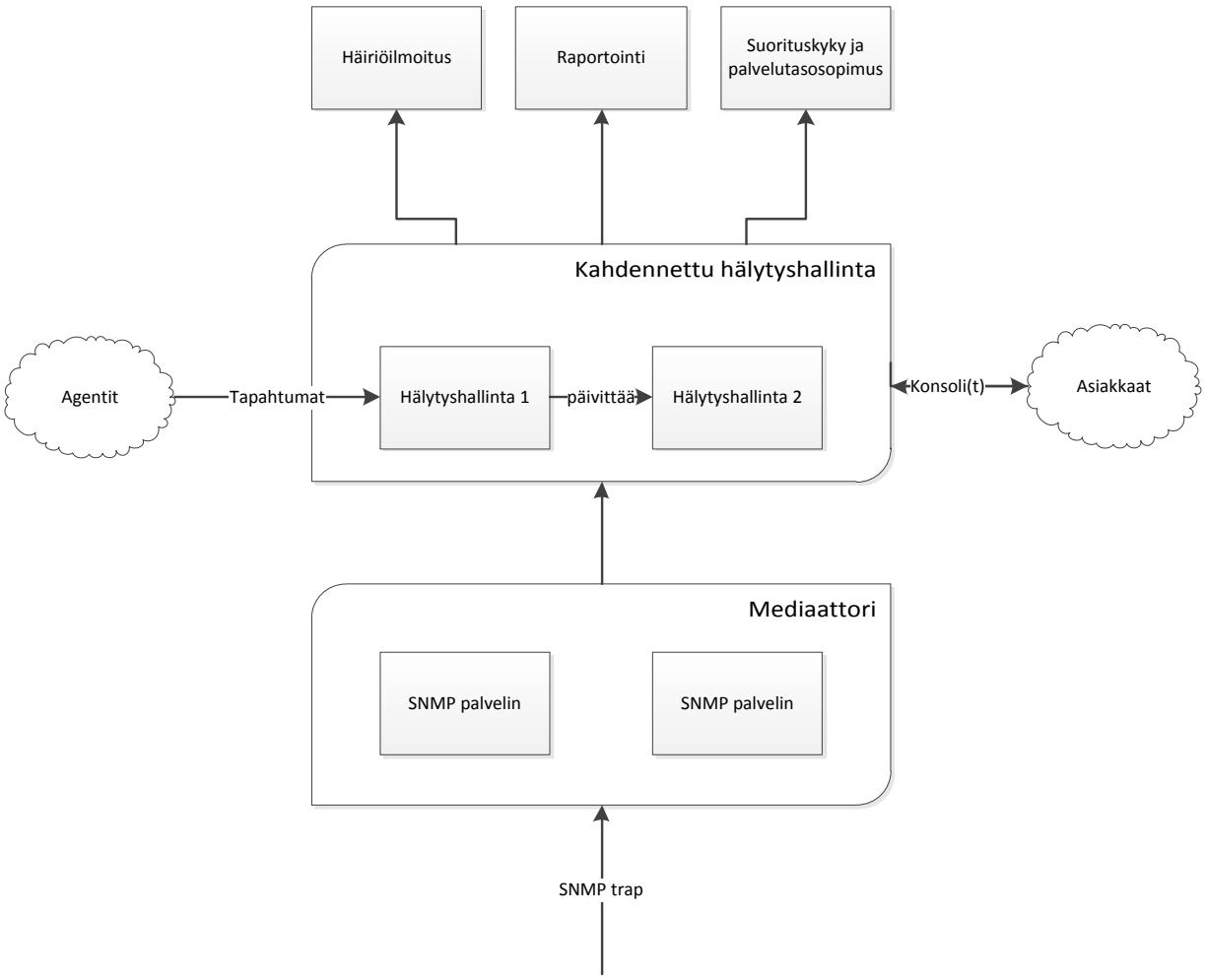


Kuvio 4. SNMP trap muodostus hälytysviestiksi ja häiriöilmoitukseksi

Hälytysviesti jää vain hälytyshallintajärjestelmän asiakasohjelmaan monitoroitavaksi, jos siitä ei muodostu häiriöilmoitusta. Hälytysviesti täytyy ensin muotoilla rajapinnassa, jotta se saadaan sellaiseen muotoon jonka häiriöilmoitusjärjestelmä tunnistaa. Häiriöilmoituksen muodostuttua, hälytyshallintajärjestelmä ei pysty häiriöilmoituksen tilaa muuttamaan. Lisäksi hälytysviestiin häiriöilmoitushallintajärjestelmä ei pysty enää vaikuttamaan. (Kuvio 4).

3.1 Automaattinen hälytyshallinta

Verkon eri osa-alueilta tulleita hälytyksiä otetaan vastaan hälytyshallintajärjestelmällä, joka suodattaa, korreloi, rikastaa ja eskaloi hälytysviestejä. Laitteisiin asennetut agentit lähettävät tietoa hälytyshallintajärjestelmään SNMP:n avulla. Agentit keräävät laitteista tietoa, joko itsenäisesti tai rikastamalla tietoa laitteen lokitiedostoilla.



Kuvio 5. Automaattinen hälytyshallintajärjestelmä. (Muokattu kuviosta sisäinen dokumentti 2013).

Itse hälytyshallinta on kahdennettu, jotta palvelu toimisi mahdollisimman luotettavasti esimerkiksi vikatilanteissa ja toisen hälytyshallinnan uudelleen käynnistyessä (Kuvio 5). Hälytyshallintajärjestelmästä ohjataan tietoa häiriöilmoitushallintaan, raportointiin ja suorituskykyhallintaan sekä palveluehtohallintaan.

3.1.1 Hälytysten keräily ja suodatus

Hälytyksiä kerätään SNMP trap -muodossa verkosta, joko suoraan laitteilta tai palvelimen kautta jäsennettynä SNMP trap –muotoon. Hälytysten sisäänotossa tapahtuu ensimmäinen suodatus, jolloin otetaan vastaan vain määritellyt hälytykset, joita halutaan seurata. Tämä on välttämätöntä suorituskyvyn kannalta, koska joissakin teknologioissa hälytyksiä voi olla useita tuhansia. Hälytykset ohjataan omiin ryhmiin tekniikoiden mukaisesti, jolloin erityisominaisuudet otetaan huomioon jatkosuodatuksessa ja korreloinnissa.

Seuraava suodatus tapahtuu, kun hälytys on ohjattu omaan ryhmäänsä. Hälytykselle voidaan asettaa aikasuodatus, jonka tarkoituksena on odottaa laitteen tai palvelun elpymistä määritellyn ajan puitteissa. Jos kuittausviestiä ei saavu tässä ajassa, ohjataan hälytys eteenpäin korrelointipiiriin.

3.1.2 Hälytysviestien ja tapahtumien korrelointi

Korreloinnissa voidaan käyttää erilaisia korrelointitekniikoita. Järjestelmässä on yleisiä valmiita säännöksiä, mutta näitä voidaan myös muokata häiriöilmoituskäsittelijäryhmien luomien määritysten mukaisesti. Laitteiden ja palvelujen yksilöllisten ominaisuuksien takia sääntöjen muokkaaminen on tarpeellista. Korrelaatiotekniikoita voidaan rakentaa erittäin monimutkaisiksi, joten seuraavissa kappaleissa esitellään vain keskeisimmät mahdollisuudet.

Identtiset hälytysviestit tunnistetaan samoiksi hälytysviestiavaimen perusteella. Häiriöilmoituskäsittelyryhmät määrittelevät tämän hälytysviestiavaimen, jotta identtisten hälytysviestien tunnistus onnistuu parhaalla mahdollisella tavalla. Identtisen hälytysviestin tunnistettua, järjestelmä aloittaa laskurin ja lisää tiedon identtisten hälytysviestien määrästä alkuperäiseen hälytysviestiin. Täten vain alkuperäinen hälytysviesti muodostaa häiriöilmoituksen. Monistuvia hälytysviestejä voidaan tukahduttaa ajastimella, laskurilla tai näiden yhdistelmällä.

Hälytystapahtumaan liittyy yleensä useita erilaisia uniikkeja hälytysviestejä. Tapahtumakorrelaatiolla saavutetaan reaaliaikainen tapahtumien prosessointi, jonka avulla voidaan tunnistaa eri tapahtumien suhteita. Tapahtumia seurataan hälytysviestien lähteiden eri tietolähteistä.

Hälytysmyrskyllä tarkoitetaan tilannetta, jossa hälytysviestejä muodostuu todella paljon esimerkiksi laitteen toiminnan takia tai laajan verkkoelementin vikaannuttua. Hälytysmyrskyn tunnistettua järjestelmä pysäyttää tämän automaattisesti ja muodostaa tapahtumasta yhden suurella vakavuustasolla olevan ilmoituksen. Tälle tunnistukselle voidaan tehdä asetuksen tarpeen mukaisesti.

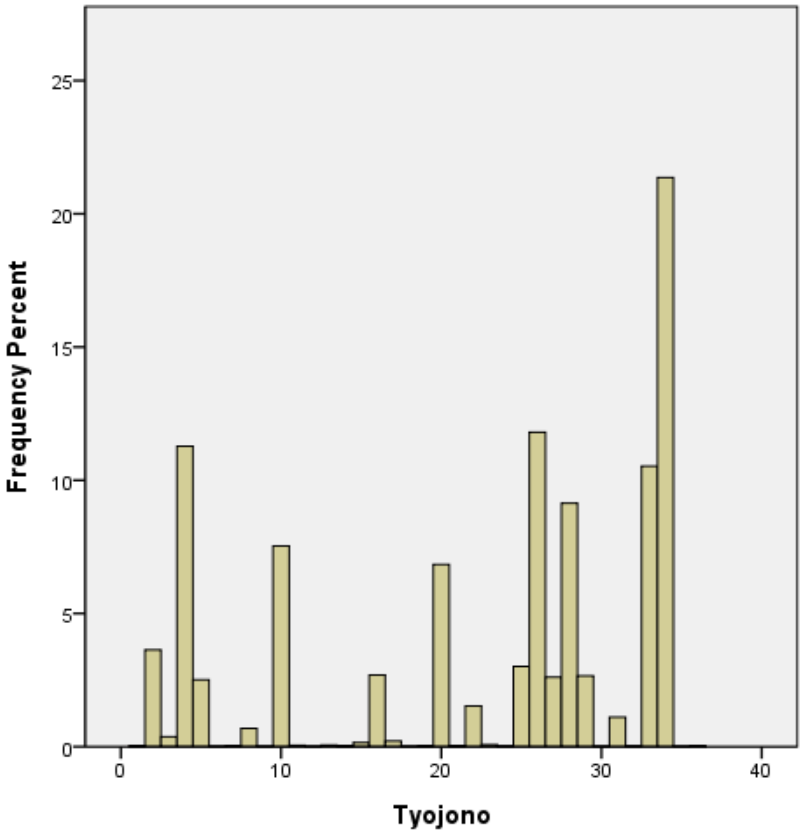
3.2 Häiriöilmoitushallinta

Häiriöilmoitushallintajärjestelmä on olennainen osa viankorjausprosessia. Järjestelmä ohjaa häiriöilmoitukset jatkokäsittelyyn viankorjausprosessiin tekniikoiden tai palveluiden mukaisesti. Häiriöilmoituksesta saadaan tietoa viankorjauksen etenemisestä ja tilanteesta. Hälytysviesteistä vain noin puoli prosenttia päätyy häiriöilmoitushallintajärjestelmään käsiteltäviksi. Häiriöilmoituksia mitataan, jotta saadaan raportoitua tilastoihin esimerkiksi vikamääriä, viankorjausaikoja ja operatiivisten ryhmien toimintaa.

3.2.1 Operatiiviset ryhmät ja häiriöilmoituskäsittely

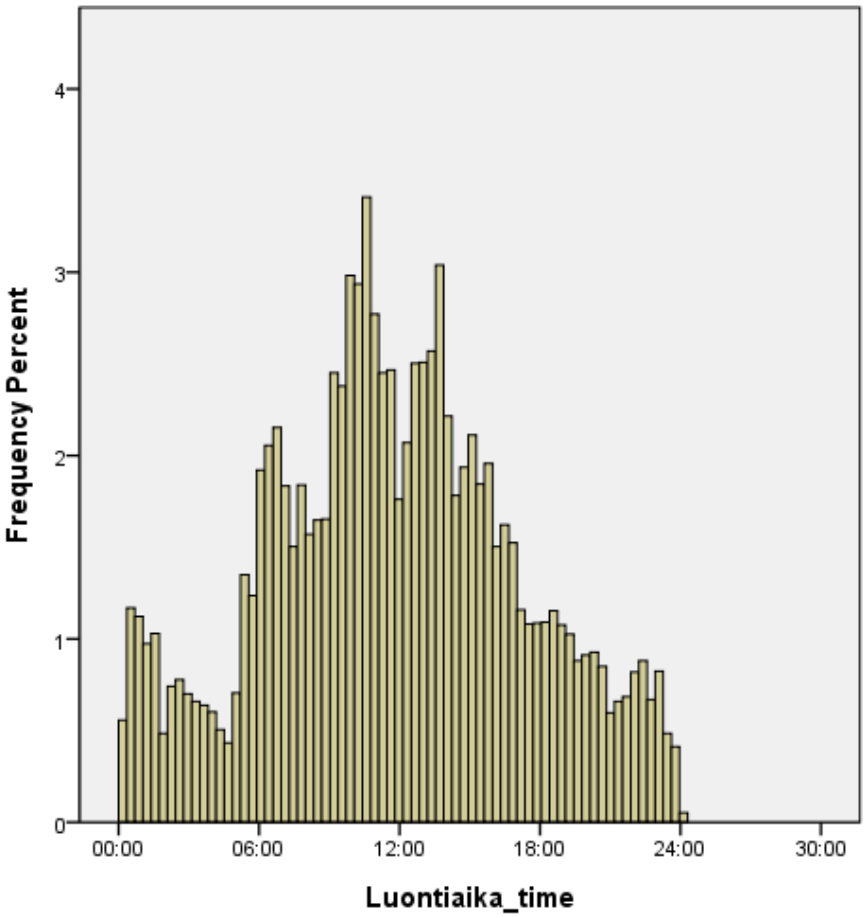
Häiriöhallinasta ja viankorjauksesta vastaavilla operatiivisilla ryhmillä on tärkeä osa suodatus- ja korrelointisääntöjen luomisessa ja optimoimisessa. Häiriöilmoituskäsittelyryhmien asiantuntijat päättävät, mitä hälytyksiä halutaan ottaa vastaan eri teknologioista ja millä ehdoilla niistä luodaan häiriöilmoituksia häiriöilmoitushallintajärjestelmän työjonoihin häiriöilmoituskäsittelyyn. Työjonot ovat tehty teknologioiden ja häiriöilmoituskäsittelyryhmien mukaisesti, jotta häiriöilmoituskäsittelijä löytää helposti oman vastuualueen häiriöilmoitukset. Tämä auttaa myös häiriöilmoituskäsittelyn työn seuraamista ja kehityssuuntien tunnistamista.

Häiriöilmoituskäsittelijä tulkitsee häiriöilmoituksen informaation ja suorittaa tarvittavat toimenpiteet viankorjausta varten. Informaation laadulla on suuri merkitys esimerkiksi juurisyyn löytämiseksi ja kenttäviankorjauksen lähettämiseksi oikeaan paikkaan. Olennainen informaatio muodostuu hälytyshallintajärjestelmässä, joko suoraan SNMP trap –viestistä tai hälytysviestin rikastusvaiheessa. Häiriöilmoituskäsittelyryhmät määrittelevät rikastettavan tiedon hälytyshallintajärjestelmälle.



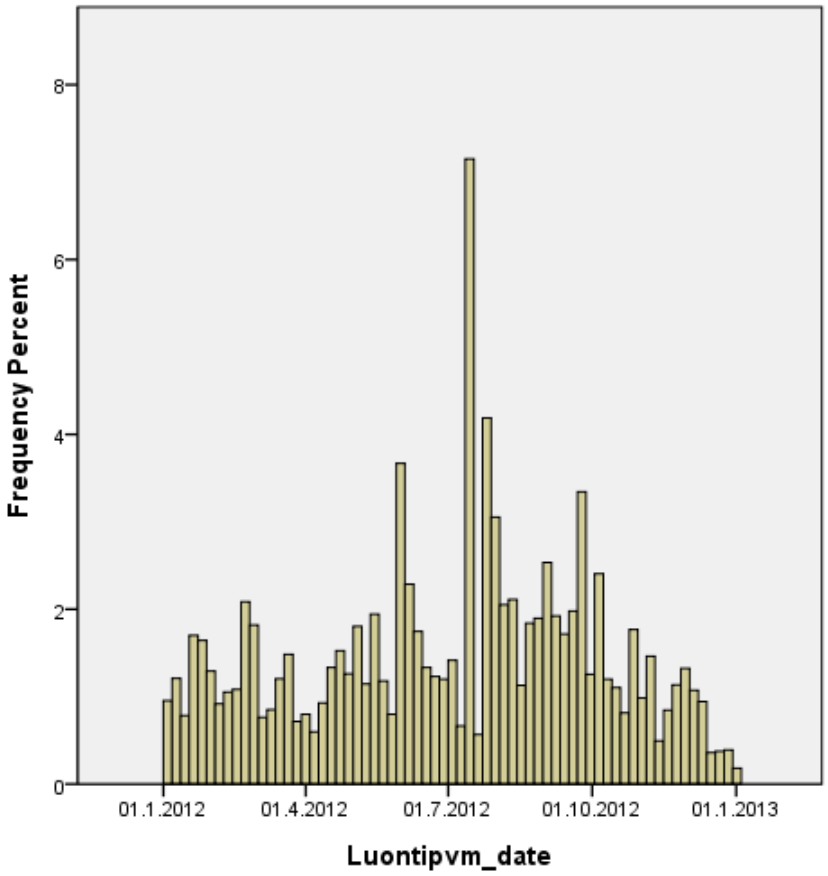
Kuvio 6. Vuoden 2012 merkittävimmät häiriöilmoituskäsittelyn työjonot, joihin häiriöilmoituksia muodostuu eniten (Muokattu häiriöilmoitusraportista 2012)

Häiriöilmoituskäsittelyn työjonojen kuormittavuus riippuu monesta eri asioista, joihin vaikuttaa mm. teknologian laajuus ja luonne sekä korrelaatiotekniikoiden tehokas hyödyntäminen. Voimme havaita merkittävimmät työjonot (Kuvio 6), joihin kannattaa panostaa korrelaatiotekniikoiden optimoinnissa. Merkittäviä työjonoja vuonna 2012 järjestelmässä on seitsemän: 4) Vaihdetekniikka #1 10) Vaihdetekniikka #2 20) Siirtoverkot 26) Mobiili ydin 28) Keskustekniikka 33) Puhealustat 34) Radioverkko. Merkittävää kuitenkin on häiriöilmoitusten määrän kehityssuunta kokonaisuudessaan, joka on lineaarisesti laskeva vuosittain.



Kuvio 7. Vuoden 2012 häiriöilmoitusten jakauma kellonaikoina (Muokattu häiriöilmoitusraportista 2012)

Häiriöilmoituskäsittelijöitä kannattaa resursoida hetkiin, jolloin häiriöilmoituksia muodostuu eniten. Päivä on selkeästi yötä kuormittavampi, mutta päiväaikaan häiriöilmoitukset tulevat selkeinä piikkeinä (Kuvio 7). Nämä piikit tapahtuvat aamulla 7-8, aamupäivällä 9-11 ja päivällä 13–15 välillä. Korkein piikki vuorokauden aikana on noin kello 11 ja tilastollisesti kiinnostava häiriöilmoitusten muodostumisen vähentyminen keskipäivällä. Häiriöilmoitusten luontiaikaa kannattaa jatkoanalyyseissa jakaa eri teknologioiden mukaan, jotta erityisominaisuudet tulevat esille.



Kuvio 8. Vuoden 2012 häiriöilmoitusten jakauma päivämäärinä (Muokattu häiriöilmoitusraportista 2012)

Häiriöilmoitusten muodostumisessa vuonna 2012 syntyi selkeitä piikkejä (Kuvio 8). Tämänkaltaiset piikit yleensä selittyvät, kun jokin iso kokonaisuus on mennyt hajalle ja tästä yhdestä viasta muodostuu monista kokonaisuuden laitteista omia häiriöilmoituksia. Tämän takia tilastot voivat vääristyä, koska häiriöilmoituksilla mitataan vikojen määrää. Tämän takia häiriöilmoituksia voidaan merkitä häiriöilmoitusjärjestelmässä peruutetuiksi, jolloin niitä ei lasketa vikamääriin. Tästä käsittelytavasta ohjeistetaan häiriöilmoituskäsittelyryhmiä, jonka avulla tilastot tulevat huomattavasti oikeaa tilannetta kuvaavimmaksi, kun laajemmasta vikatilanteesta mahdollisesti muodostuu monistuvia häiriöilmoituksia.

Laitepoistoissa ja päivityksissä on oltava selkeä käsittelyprosessi, jotta korrelointisäännöt pysyvät ajan tasalla. Riskinä on muutoin tiedon muuttuminen, mikä ei päivity hälytyshallintajärjestelmään, jolloin tuloksena on monistuvia, aiheettomia tai virheellisiä häiriöilmoituksia.

3.2.2 Eskalointi ja viankorjaus

Juurisyyanalyysin jälkeen häiriöilmoituskäsittelijä tekee tarvittavat toimet viankorjausta varten. Häiriöilmoituskäsittelijä analysoi häiriöilmoituksen juurisyyn ja tekee tarvittavat toimet vian korjaamiseksi. Tarpeen vaatiessa häiriöilmoituskäsittelijä eskaloi häiriöilmoituksen kenttäviankorjaukseen. Viankorjauksen jälkeen tai kentältä saadun viankorjauksen kuittauksen jälkeen häiriöilmoitus suljetaan.

3.2.3 Proaktiivinen viankorjaus

Proaktiivisella viankorjauksella tarkoitetaan tilannetta, jossa häiriöilmoitus ei ole vielä muodostanut häiriövaikutusta asiakkaalle. Täten voidaan estää häiriön eskaloituminen ja tehdä tarvittavat korjaustoimet ennen asiakkaan palvelun häiriintymistä. Proaktiivisia häiriöilmoituksia merkitään hälytyshallintajärjestelmässä hälytysviestin tietoihin, jolloin muodostuneet häiriöilmoitukset näkyvät vikaa ennakoivina viankorjausprosessissa ja raportoinnissa.

Proaktiivisia häiriöilmoituksia on melko hankala havaita ilman kunnollista hälytystiedonlouhintaa ja analysointia. Nykytilanteessa proaktiivisiksi häiriöilmoitukseksi on merkattu jo muodostuneita häiriöilmoituksia, koska hälytystietoa ei ole ollut saatavilla analysoitavaksi. Analyysin avulla pystytään tunnistamaan kehityssuuntia ja ilmiöitä, jotka ennakoivat mahdollista vikaa. Tämä vaatisi juurisyyanalyysista saadun tiedon tallentamista, jotta ennakoivia vikoja voisi ennustaa esimerkiksi elinkaarikäyrän ekstrapoloinnilla. Parhaaseen tulokseen päästään analysoimalla mahdollisimman useaa tietolähdettä, joita ovat esimerkiksi hälytyshallintajärjestelmä, häiriöilmoitushallintajärjestelmä, juurisyyanalyysi, palveluehtosopimus sekä suorituskykymittari. Informaation ja muuttujien suuren määrän takia, eri lähteistä kannattaa tehdä pääkomponenttianalyysi, jotta analysoitavan muuttujien määrää saadaan vähemmäksi.

3.2.4 Monistuvat häiriöilmoitukset

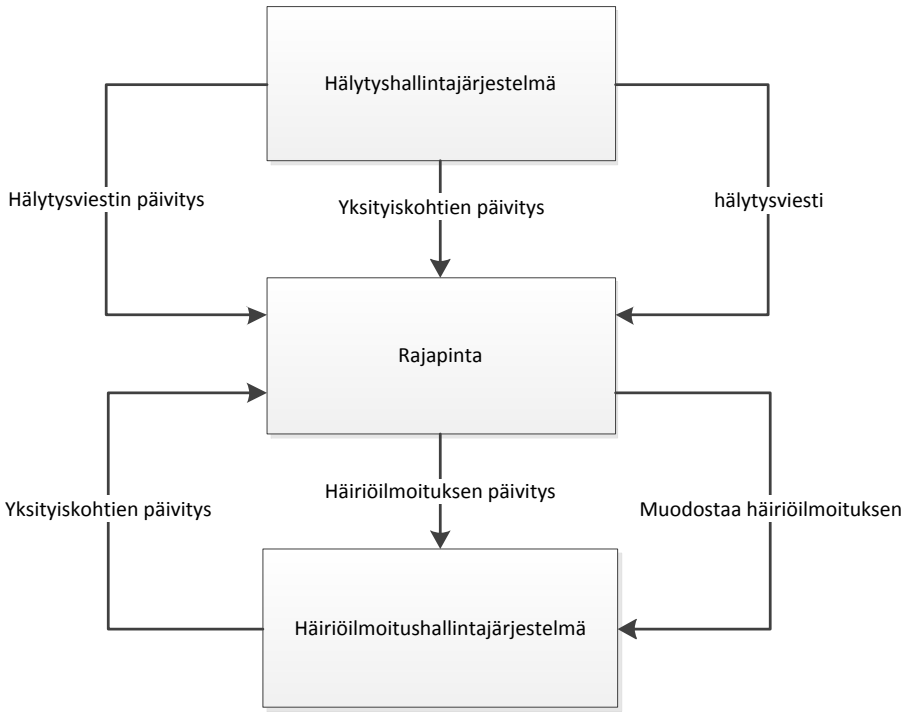
Monistuvilla häiriöilmoituksilla tarkoitetaan tilannetta, jossa yhdestä viasta muodostuu useita häiriöilmoituksia. Luvussa 3.1.2 esitelty monistuva hälytysviesti liittyy osaltaan tähän tilanteeseen. Jos häiriöinformaation pohjalta tehtyjä korrelointeja ei ole tehty, mahdollisesta hälytysmyrskystä aiheutuu runsaasti aiheettomia ja monistuvia häiriöilmoituksia. Monistuvat häiriöilmoitukset ovat tunnistettavissa analysoimalla häiriöilmoitusraporttia. Tutkimalla mistä palvelusta ja teknisistä paikoista häiriöilmoitukset muodostuvat lyhyessä aikaikkunassa, saadaan selville monistuvien häiriöilmoitusten määrä.

3.3 Automaattisen hälytys- ja häiriöilmoitushallintajärjestelmän integraatio

Häiriöilmoituksen muodostumisen ja käsittelyn jälkeen tietoa ei palaudu hälytyshallintajärjestelmän hälytysviestiin (Kuvio 4, Kuvio 5). Tämä on problemaattista useasta eri näkökulmasta. Kun luvussa 3.2.1 esitetty häiriöilmoituskäsittelijä sulkee häiriöilmoituksen, jää alkuperäinen hälytysviesti vielä aktiiviseksi. Hälytysviesti täytyy käydä erikseen sulkemassa, jotta vian korjaantuminen päivittyy myös palveluehtosopimustietoihin. Samalla tavalla häiriöilmoitus jää aktiiviseksi, vaikka hälytysviesti saisi automaattisen kuittauksen. Häiriöilmoituskäsittelijä joutuu tällöin tekemään turhaa manuaalista työtä häiriöilmoituksen avaamisessa, tutkimisessa, päivittämisessä ja sulkemisessa. Automaattisen hälytyshallinta- ja häiriöilmoitushallintajärjestelmän integroimisella edellisessä kappaleessa mainitut ongelmakohdat korjaantuisivat kahdensuuntaisten toimintojen avulla.

3.3.1 Kahdensuuntaiset toiminnot

Kahdensuuntaisilla toiminnoilla tarkoitetaan tilanteita, joissa hälytysviestin tilaa voidaan muokata muuttamalla häiriöilmoituksen tilaa. Vastavuoroisesti häiriöilmoituksen tilaa voidaan muokata muuttamalla hälytysviestin tilaa.



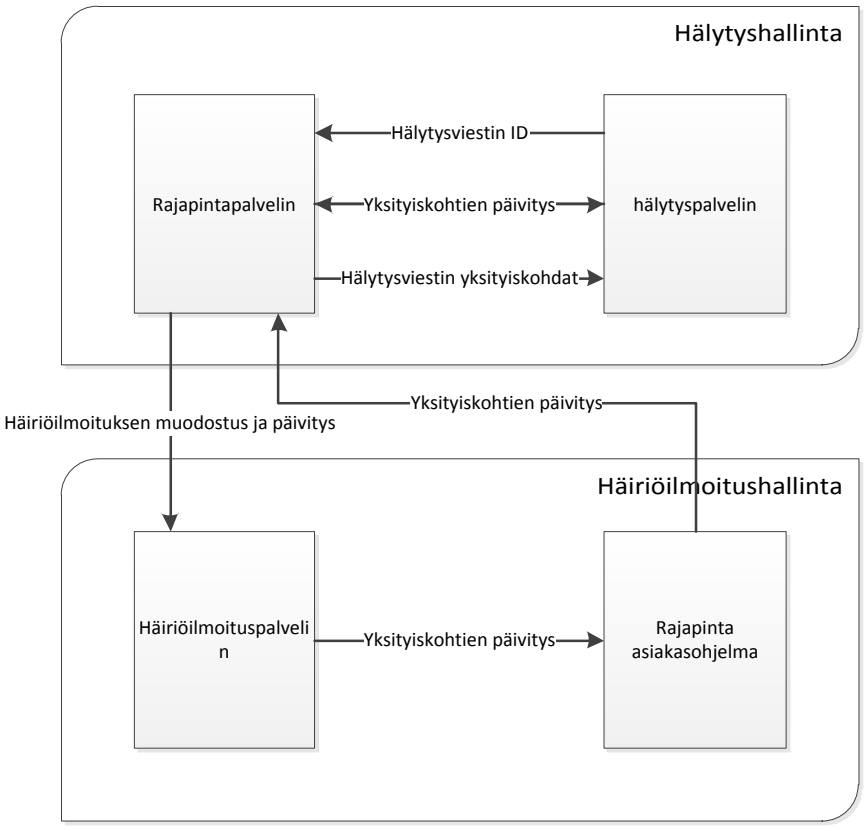
Kuvio 9. Yleiskuva hälytys- ja häiriöilmoitushallintajärjestelmien integraatiosta. (Muokattu kuviosta sisäinen dokumentti 2013).

Integraatiolla saavutetaan kahdensuuntaiset toiminnot (Kuvio 9), jotka tuo monia etuja sekä viankorjaukseen että tiedon laatuun. Tämän avulla vianhallinnan ei tarvitse päivittää tietoa kahteen eri järjestelmään ja vältytään päällekkäisen turhan työn tekemiseltä.

3.3.2 Kuittautuneet hälytykset

Automaattisen hälytyshallintajärjestelmän sisällä olevat hälytykset kuittautuvat, kun elpynyt laite antaa kuittausviestin. Jos hälytyksestä on jo muodostunut häiriöilmoitus häiriöilmoitushallintajärjestelmään, kuittautunut hälytys ei pääse kuittaamaan jo muodostunutta häiriöilmoitusta. Integraation avulla kuittautuneet hälytykset voivat muuttaa häiriöilmoituksen tilaa ja täten vältytään turhalta manuaaliselta työltä.

Kuittautuneista hälytyksistä muodostuneita häiriöilmoituksia tunnistetaan häiriöilmoitusraporteista tutkimalla häiriöilmoituskäsittelijän tuottamaa tietoa. Häiriöilmoituskäsittelijöillä on hieman erilaisia tapoja merkitä tämänkaltaisia hälytyksiä, joka tekee tutkimisesta hankalaa. Osa käyttää merkitsemiseen valmiita pudotusvalikoita ja osa kirjoittaa tiedon selväsanallisesti lisätietokenttään.



Kuvio 10. Hälytys- ja häiriöilmoitushallintajärjestelmän integraatio verkon ja palvelimen näkökulmasta. (Muokattu kuviosta sisäinen dokumentti 2013).

Verkon kannalta integraatio toimii lähes samalla tavalla, kuin luvussa 2.2 esitelty agentti, kuten kuviosta (Kuvio 10) voidaan havaita. Asiakasohjelma asennetaan häiriöilmoituspalvelimelle, jossa se pystyy hallintaoikeuksien avulla muuttamaan häiriöilmoitusten tilaa, kun hälytysviesti muuttuu. Samoin jos vianhallinnassa muutetaan häiriöilmoituksen tilaa, päivittyy muutos asiakasohjelman avulla hälytyshallintajärjestelmän hälytysviestiin.

3.3.3 Palveluehtosopimus

Palveluehtosopimuksia varten saadaan tietoon tarkennusta integraation avulla, koska aikaa ei kulu manuaaliseen työn odottamiseen automaattisissa hälytysten kuittauksissa. Palveluehtosopimuksien ajat otetaan suoraan automaattisesta hälytyshallintajärjestelmästä. Kun vianhallinta kuittaa häiriöilmoituksen käsitellyksi, muuttuu hälytysviestin tila hälytyshallintajärjestelmässä, josta tieto menee palveluehtosopimushallinnan monitorointiin.

4 Aineiston kerääminen ja esiprosessointi

Työn kanalta olennainen tieto saatiin analysoimalla häiriöilmoituksia ja hälytystietoa sekä haastattelemalla asiantuntijoita. Asiantuntijoilta sai tietoa myös vapaamuotoisten keskusteluiden kautta ja sähköpostikirjeenvaihdolla. Tietoa kerättiin myös osallistumalla palavereihin, tilaisuuksiin ja aiheeseen liittyviin projekteihin sekä tutkimalla verkkokansioihin tallennettuja tiedostoja eri järjestelmiin liittyen.

Automaattisista hälytyksistä muodostuneita häiriöilmoituksia raportoidaan. Raportin voi hakea mm. Excel-taulukkona halutulla aikaikkunalla. Raportissa on molempien rinnakkaisten automaattisen hälytyshallintajärjestelmän avaamat tiketit, josta voi tarpeen mukaan suodattaa toisen järjestelmän tiedot pois. Esimerkiksi ongelmanhallintaprosessi hyödyntää kyseistä lähdettä. Nämä raportit ovat hyödyllisiä myös operatiivisille ryhmille, mutta tätä mahdollisuutta ei täysin hyödynnetä asiantuntijoiden tai esimiesten toimesta.

Jäsennettävä hälytystieto löytyy ulkoistetun palvelimen web-käyttöliittymällä. Palvelimella jäsennetään hälytystieto SNMP trap -muotoon, jotta hälytyshallintajärjestelmä pystyy tiedon vastaanottamaan. Tämänkaltaista jäsennystä tehdään sellaisilla hälyttävillä laitteilla, jotka eivät osaa lähettää SNMP trap -paketteja. Esimerkiksi vanhemmat keskus- ja vaihdetekniikat ovat tämänkaltaisia.

4.1 Hälytysjärjestelmän tietokanta

Varsinaisista hälytysviesteistä ei luoda raportteja, vaan nämä tiedot täytyy hakea erikseen SQL-tietokannasta, johon taltioituu automaatin hälytyshistoria. Hälytyshistoriassa ei kuitenkaan ole kaikkea olennaista tietoa. Rikastettu hälytysviestitieto löytyy järjestelmästä, mutta tätä tietoa ei tallenneta tietokantaan palvelimen suorituskyvyn takia (Asiantuntijahaastattelu 2012). Rikastettua hälytysviestitietoa voi kuitenkin tutkia muutaman viikon puskurin päähän asiakasohjelmalla.

Informaatio haettiin CSV-tiedostona, jota muokattiin SPSS-ohjelmalla analysoitavaan muotoon. Esiprosessointi vei paljon aikaa, koska aineisto oli laaja ja muuttujien yksilöllisiä tietueita oli tuhansia. Suuri osa muuttujista täytyi ohjelmoida uudelleen, koska niiden tietueet olivat merkkijonoja. Merkkijonotietueilla analysoiminen saattaa vääristää tuloksia analyyseissa (Metsämuronen 2008, 28).

4.2 Asiantuntijahaastattelut

Asiantuntijahaastattelut tehtiin teemahaastattelun periaatteen mukaisesti Elisan Oyj:n tiloissa. Olennaisin tieto saatiin hälytyshallintajärjestelmän järjestelmäasiantuntijalta, jolla oli yksityiskohtainen tieto hälytyskeräilystä ja hälytysviestihallinnasta. Toisaalta eri näkökulmista asioita tarkastelevat asiantuntijat auttoivat saamaan laajan käsityksen verkonhallinnasta kokonaisuutena. Tämä auttoi löytämään luovia ratkaisuja tutkimusongelmiin. Tarkentavaa tietoa asiantuntijoilta saatiin myös sähköpostin välityksellä.

5 Pääkomponenttianalyysi

Pääkomponenttianalyysin (principal component analysis) avulla saadaan suuri joukko muuttujia tiivistettyä muutamiin tärkeimpiin. Menetelmää voi käyttää moniin erilaisiin aineistoihin ja tarkoituksena on löytää suuresta määrästä informaatiota jotain yhteistä muuttujien väliltä, joka yhdistää muuttujat toisiinsa teoriassa ja käytännössä. Pääkomponenttianalyysin tarkoitus on muodostaa lineaarisia yhdistelmiä korrelaatio- tai kovarianssimatriisin hajontaan. Menetelmän matemaattinen malli pyrkii löytämään sellaiset yhdistelmät, jotka parhaiten selittävät muuttujien välistä vaihtelua. (Metsämuronen 2008, 28).

Tutkittava aineisto soveltuu hyvin tähän menetelmään, koska aineistossa on 16 muuttujaa ja muuttujilla on aitoa korrelaatiota keskenään. Pääkomponenttianalyysin jälkeen aineistoa pystyy helpommin analysoimaan tulevissa tutkimuksissa.

Communalities

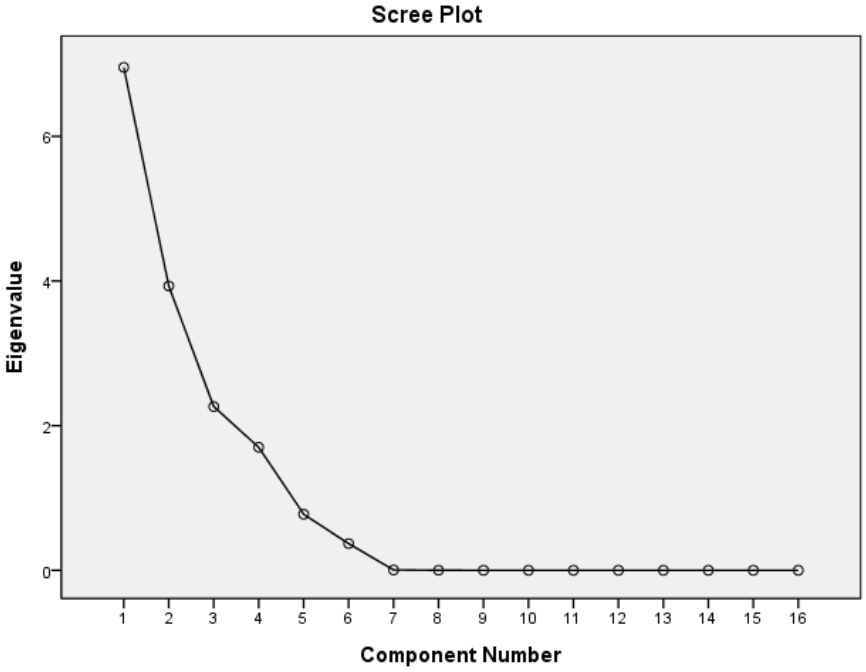
	Initial	Extraction
Luontiaika	1.000	.999
Vastaanottoaika	1.000	.999
Kuittausaika	1.000	.996
ViimVastaanottoaika	1.000	.999
Monistuva	1.000	.297
ViestinLahdeTyyppi	1.000	.976
Vakavuus	1.000	.992
ViestinLahdenimi	1.000	.991
Sovellus	1.000	.994
Viestiryhma	1.000	.966
Noodinimi	1.000	.992
Kohde	1.000	.674
Viestityyppi	1.000	.998
Palvelunimi	1.000	.987
Viestiavain	1.000	.996
NoodiRyhmanimi	1.000	.992

Extraction Method: Principal Component Analysis.

Taulukko 1. Muuttujien kommunaliteetit

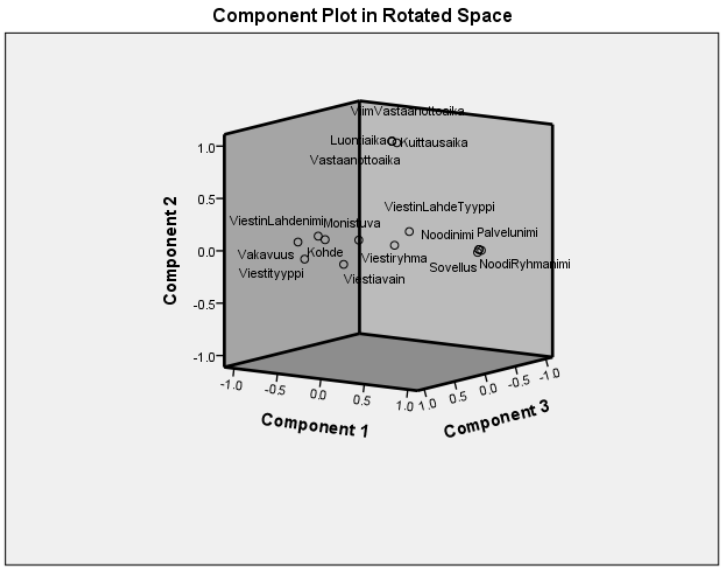
Muuttujien kommunaliteetit ovat korkeita (Taulukko 1). Tämä tarkoittaa sitä, että ne mittaavat luotettavasti pääkomponentteja. Kommunaliteetti mittaa muuttujan varianssin prosentuaalista osuutta pääkomponentista. (Verma 2012, 362).

Pääkomponenteiksi tulkitaan komponentit, joilla on ominaisarvo suurempi kuin 1.0. Tämä arvo määriteltiin SPSS-ohjelmassa raja-arvoksi, koska tätä käytetään yleisesti nyrkkisääntönä (Metsämuronen 2008, 31). Tätä raja-arvoa kutsutaan Kaiserin leikkauskohdaksi, joka tarkoittaa että vain kertoimet joissa ominaisarvo > 1, säilytetään analyysissa (Verma 2012, 363). Taulukosta (Liite 1) käy ilmi, että pääkomponentteja on neljä ja nämä neljä pääkomponenttia selittävät noin 93 % muuttujien varianssista.



Kuvio 11. Pääkomponentin ominaisarvot suuruusjärjestyksessä

Cattellin Scree-kuvassa (kuvio 11) on kuvattu pääkomponentin ominaisarvot suuruusjärjestyksessä. Kuvio havainnollistaa löytyykö ominaisarvoissa kriittistä kohtaa, jonka jälkeen ominaisarvoissa ei tapahdu suurta muutosta. Komponentin 4. ja 5. välillä tapahtuu selkeä lasku. Tämän jälkeen lisäinformaatiota komponenteissa ei juuri tule, joten 4 pääkomponenttia on sopiva määrä. Seitsemännen komponentin kohdalla tapahtuu Kaiserin leikkauskohta.



Kuvio 12. Pääkomponentit ja muuttujat

Pääkomponenttien graafisessa kuvassa (Kuvio 11) nähdään kuinka erillään pääkomponentti-analyysin muuttujat ovat toisistaan.

Rotated Component Matrix[a]

	Component			
	1	2	3	4
Luontiaika		.999		
Vastaanottoaika		.999		
Kuittausaika		.993		
ViimVastaanottoaika		.999		
Monistuva	-.369			-.399
ViestinLahdeTyyppi			-.450	.874
Vakavuus	-.970			
ViestinLahdenimi	-.962			
Sovellus	.988			
Viestiryhma				.919
Noodinimi	.970			
Kohde	-.811			
Viestityyppi	-.302		.947	
Palvelunimi	.990			
Viestiavain			.978	
NoodiRyhmanimi	.970			

Extraction Method: Principal Component Analysis.

Rotation Method: Varimax with Kaiser Normalization.

a. Rotation converged in 5 iterations.

Taulukko 2. Rotatoitu komponenttimatriisi

Rotatoidulla komponenttimatriisilla (Taulukko 2) pyritään löytämään selkeää tulkinnallista ratkaisua. Muuttujalla on sitä suurempi merkitys pääkomponentissa, mitä lähempänä se on arvoa 1. Analyysissa päätettiin jättää taulukosta pois arvot, jotka jäävät alle arvon 0.25, jotta taulukkoa on selkeämpi tulkita. Jatkoanalyyseissa muuttujan ”monistuva” voi jättää kokonaan pois, koska sillä ei ole selkeää merkitystä pääkomponenteissa.

Ensimmäisessä pääkomponentissa voimakkaan merkityksen omaavat muuttujat 1) Vakavuus 2) ViestinLahdenimi 3) Sovellus 4) Noodinimi 5) Kohde 6) Palvelunimi ja 7) NoodiRyhmanimi. Nämä muuttujat saivat arvot 1) -.970 2) -.962 3) .988 4) .970 5) -.811 6) .990 ja 7) .970. Toisessa pääkomponentissa merkittäviä muuttujia ovat 1) Luontiaika 2) Vastaanottoaika 3) Kuittausaika ja 4) ViimVastaanottoaika. Nämä muuttujat saivat arvot 1) .999 2) .999 3) .993 ja 4)

.999. Kolmannessa pääkomponentissa merkittäviä muuttujia ovat 1) Viestityyppi ja 2) Viestiavain. Nämä muuttujat saivat arvot 1) .947 ja 2) .978. Neljännessä ja viimeisessä pääkomponentissa merkittävät muuttujat ovat 1) ViestiLahdeTyyppi ja 2) Viestiryhma. Nämä muuttujat saivat arvot 1) .874 ja 2) .919. Tulkitsemalla lueteltujen muuttujien nimiä ja muuttujien informaatiota eri pääkomponenteilla, päätettiin pääkomponentit nimetä seuraavasti 1) Kohde 2) Aika 3) Viesti ja 4) Ryhmä.

6 Tutkimuksen tulokset ja pohdintaa

Tutkimuksen keskeiset tulokset olivat kehityshanke hälytys- ja häiriöilmoitushallintajärjestelmien integraatiosta sekä hälytyshallintajärjestelmän tietokannan pääkomponenttianalyysistä saadut pääkomponentit.

Ensimmäinen ja toinen hypoteesi todentui analyysissa ja hypoteesit korreloivat keskenään. Monistuvia häiriöilmoituksia vuonna 2012 oli noin 27 % kaikista häiriöilmoituksista (häiriöilmoitusraportti 2012). Tämänkaltaisia häiriöilmoituksia saadaan vähennettyä optimoimalla hälytyshallintajärjestelmän sääntöjä esimerkiksi aika ja määrä –korrelaatiotekniikalla sekä hälytysmyrskykorrelaatiotekniikalla.

Ensimmäiseen tutkimuskysymykseen saatiin vastaus Integroimalla hälytys- ja häiriöilmoitushallintajärjestelmä. Täten onnistuvat kahdensuuntaiset toiminnot näiden kahden eri järjestelmän välillä. Tämän seurauksena turhat häiriöilmoitukset, joiden alkuperäinen hälytys on kuittautunut, poistuvat ja turhan manuaalisen työn määrä vähenee viankorjauksessa (Asiantuntijahaastattelu 2013). Tämä tarkoittaisi noin 19 % vähennystä häiriöilmoituksissa ja noin 1,26 työkuukauden säästöä vuodessa (Häiriöilmoitusraportti 2012 & Asiantuntijahaastattelu 2013).

Myös toiseen tutkimuskysymykseen saatiin vastaus. Hälytyshallintajärjestelmän korrelaatio- ja suodatussääntöjen muodostamiseksi tarvitaan aineistoa tutkittavaksi, jotta tapahtumien ja häiriöiden kehityssuunta saadaan selville. Analysoimalla hälytyshallintajärjestelmän tietokannan tietoa löydettiin neljä pääkomponenttia pääkomponenttianalyysin avulla, jotka selittävät noin 93 % muuttujien varianssista. Nämä neljä pääkomponenttia nimettiin seuraavasti: kohde, aika, viesti ja ryhmä. Tämä auttaa lisäanalyysien suorittamisessa, kun tutkittavien muuttujien määrä vähenee.

6.1 Kehitysehdotukset

Tutkimuksen aikana ja tuloksia analysoidessa tuli eteen asioita jotka vaativat kehitystä tai jatkotutkimusta. Tällaiset asiat olivat joko järjestelmien toiminnallisuuksiin tai prosesseihin ja toimintatapoihin liittyviä asioita.

6.1.1 Hälytystiedon raportoinnin kehittäminen

Hälytyshallintajärjestelmä ei nykyisellään kerää rikastettua hälytystietoa tehokkaasti. Tiedosta on saatavilla vain noin kahden viikon puskurissa olevat hälytykset. Kahdessa viikossa ei saa luotettavaa analyysia kokonaistilanteesta, koska yksittäiset ilmiöt ylikorostuvat. Tämä puskuri on säädetty pieneksi suorituskyvyn puutteen takia. Hälytyshallintajärjestelmä kykenee kuitenkin käsittelemään koko aineistoa, mutta pullonkaulaksi muodostuu tietokannan suorituskyky.

Rikastamaton hälytystieto, joka tallentuu hälytyshallintajärjestelmän tietokantaan, ei pidä sisällään tietoa onko hälytyksestä muodostunut häiriöilmoitusta. Tämä toiminnallisuus on mahdollinen toteuttaa lisäämällä kyseinen ominaisuus raportointiin, jolloin tiedon louhinnasta saa aikaiseksi laadukkaampaa analyysia.

6.1.2 Korrelointisääntöjen tilauksen kehittäminen ja tuotteistaminen

Nykytilassa korrelointisääntöjen tilaamiseen ei ole luotuna selkeää prosessia ja eri häiriöilmoituskäsittelyryhmillä on omat tavat tehdä tilauksia. Tilaaminen tapahtuu pääsääntöisesti sähköpostilla tai kasvotusten. Joillakin ryhmillä on käytössä päivitettävä Excel-lista eri hälytysten korrelointisääntöjä varten. Tämän tiedon monimuotoisuuden ja saavutettavuuden vuoksi asiantuntijoiden ja esimiesten on vaikea seurata ja mitata kehitystä sekä tuloksia. Tieto tulee ohjata sähköposteista ja yksittäisistä Excel-tiedostoista yhteen tilausjärjestelmään. Tällä tavalla tiedon saavutettavuus paranee ja turhan työn tekeminen vähenee sekä korrelointisääntöjen laatu tehostuu.

Korrelointitekniikat voivat olla hyvin monimutkaisia ja mahdollisten korrelointitekniikoiden tuntemus on melko rajallista niitä tilaavilla. Täten on hyvä olla selkeät korrelointiominaisuudet tuotteina, joita häiriöilmoituskäsittelyryhmät voivat tilata ilman turhaa sähköpostivaihtoa.

6.1.3 Topologiaan perustuvan korreloinnin lisääminen

Hälytyshallintajärjestelmässä ei ole tällä hetkellä topologiaan perustuvaa korrelointia. Topologiaan perustuva korrelaatio parantaisi huomattavasti tapahtumahallintaa sekä viankorjausta. Topologiaan perustuva korrelaatio vähentäisi juurisyyanalyysiin kuluvaa aikaa, joka toisi säästöä viankorjauksen työmäärässä. Lisäksi palveluehtosopimusten aikoihin syntyvä tarkennus toisi säästöä.

6.1.4 Automaattisten toimintojen kehittäminen

Manuaalisesti luotujen häiriöilmoitusten määrää saadaan vähemmäksi siirtämällä niitä automaattisen hälytyshallintajärjestelmän piiriin. Tämä vähentää manuaalista työtä häiriöilmoituskäsittelyssä, nopeuttaa prosessin toimintaa ja lisää mahdollisuutta parempaan automaation hallintaan tulevaisuudessa.

Manuaalista viankorjausta saadaan vähennettyä merkittävästi integroimalla automaattiseen hälytyshallintajärjestelmään automaattisen viankorjauksen toimintoja. SNMP osaa yksinkertaisia viankorjauksia, kuten laitteen uudelleenkäynnistämisen, mutta yhä kehittyneempiä ja monimutkaisempia korjauskeinoja on syytä tutkia.

6.1.5 Automaattisten hälytyshallintajärjestelmien integraatio

Kahden rinnakkaisen hälytyshallintajärjestelmän integraatio lisää kykyä korreloida eri teknologioiden välillä. Myös järjestelmien erilaisten toiminnallisuuksien hyödyntäminen keskenään tuo etua esimerkiksi korrelaatiotekniikoiden kanssa.

6.1.6 Tiedonlouhinnan ja analyysin kehittäminen

Korrelointisääntöjen optimoiminen vie paljon resursseja asiantuntijoilta, jotta hälytyskeräily toimii mahdollisimman optimoidusti. Mahdollisuutta reaaliaikaiseen automaattiseen tiedonlouhintaa ja analysointiin kannattaa täten tutkia. Tämä mahdollistaa proaktiivisen viankorjauksen aloittamisen automaattisesti. Tällä tavalla voidaan puuttua ongelmiin ja korjata ne ennen asiakasvaikutusta ja täten saavuttaa merkittäviä säästöjä sekä kilpailuetua. Lisäksi automaattisesti luodut korrelointisäännöt tiedonlouhinnan kautta vähentää asiantuntijoiden työtaakkaa huomattavasti.

Lähteet

Elisa Oyj. 2012. Elisa Oyj. Viitattu 15.12.2012. http://corporate.elisa.fi/elisa-oyj/

Elisa Oyj. 2012. Tilinpäätös. Viitattu 2.6.2013. http://corporate.elisa.fi/attachment/content/130206TILINPAATOS%202012B.pdf

Kuvio 1. 2012. Elisa Oyj. Tulostettu 15.12.2012. http://corporate.elisa.fi/elisa-oyj/elisa-oyj/organisaatio/

Elisa Oyj. 2012. Organisaatio. Viitattu 15.12.2012. http://corporate.elisa.fi/elisa-oyj/elisa-oyj/organisaatio/

Kuvio 2. 2012. Elisa Oyj. Tulostettu 15.12.2012. http://corporate.elisa.fi/elisa-oyj/elisa-oyj/strategia/

Mäkelä, T. 2012. Tietoliikenneoperaattorin automaattisen häiriöiden käsittelyn kehittäminen. Aalto Yliopisto. Sähkötekniikan korkeakoulu. Espoo. Opinnäytetyö

Douglas, M. & Schmidt, K. 2008. Essential SNMP. 2. painos. Sebastopol: O'Reilly Media, Inc.

Hakala, M. & Vainio, M. 2005. Tietoverkon rakentaminen. Porvoo: WS Bookwell.

Chuvakin, A. Schmidt, K. & Phillips, C. 2012. Logging and Log Management : The Authoritative Guide to Understanding the Concepts Surrounding Logging and Log Management. Waltham: Elsevier Science.

Beaulieu, A. 2009. Learning SQL. Sebastopol: O'Reilly Media, Inc.

Andersen, B. & Fagerhaug, T. 2006. Root Cause Analysis: Simplified Tools And Techniques. 2. painos. Milwaukee: ASQ.

Wilson, P. Dell, L. & Anderson, G. 1993. Root Cause Analysis: A Tool for Total Quality Management. Milwaukee: ASQ.

Comprehensive report. 2003. Operations Support Systems: Solution and Strategies for the Emerging Network. Chicago: International Engineering Consortium.

Taylor, A. 2010. SQL For Dummies. 7. painos. Indianapolis: Wiley Publishing, Inc.

Farrel, A. 2011. Network Management Know It All. Burlington: Elsevier Science.

Abby, R. 2007. Effective IT Service Management: To ITIL and Beyond!. Berliini: Springer.

Thejendra, B.S. 2008. Practical IT Service Management: A Concise Guide for Busy Executives. IT Governance Publishing.

Computer Associates. 2007. Service Management Process Maps: Your Route to Service Excellence. Zaltbommel: Van Haren Publishing

Metsämuronen, J. 2008. Monimuuttujamenetelmien perusteet. 2. painos. Jyväskylä: Gummerrus kirjapaino Oy.

Verma, J.P. 2012. Data Analysis in Management with SPSS Software. Springer.

Julkaisemattomat lähteet

Häiriöilmoitusraportti. 2012. Elisa Oyj.

Tietokanta-aineisto. 2012 – 2013. Elisa Oyj.

Sisäinen dokumentti. 2012 – 2013. Elisa Oyj.

Asiantuntijahaastattelu 2012 – 2013. Elisa Oyj.

Kuviot

Taulukot

Liitteet

Liite 1 Taulukko pääkomponenttien ominaisarvoista ja selityksistä 1/2

Total Variance Explained

Component	Initial Eigenvalues			Extraction Sums of Squared Loadings	
	Total	% of Variance	Cumulative %	Total	% of Variance
1	6.954	43.463	43.463	6.954	43.463
2	3.932	24.576	68.039	3.932	24.576
3	2.264	14.148	82.187	2.264	14.148
4	1.701	10.631	92.818	1.701	10.631
5	.775	4.844	97.662		
6	.369	2.306	99.968		
7	.005	.029	99.997		
8	.000	.003	100.000		
9	2.427E-5	.000	100.000		
10	6.947E-6	4.342E-5	100.000		
11	2.642E-8	1.651E-7	100.000		
12	3.230E-12	2.019E-11	100.000		
13	1.905E-14	1.191E-13	100.000		
14	2.086E-15	1.304E-14	100.000		
15	3.970E-17	2.482E-16	100.000		
16	-9.464E-15	-5.915E-14	100.000		

Extraction Method: Principal Component Analysis.

Liite 1 Taulukko pääkomponenttien ominaisarvoista ja selityksistä 2/2

Total Variance Explained

Component	Extraction Sums of Squared Loadings	Rotation Sums of Squared Loadings		
	Cumulative %	Total	% of Variance	Cumulative %
1	43.463	6.695	41.843	41.843
2	68.039	4.000	24.999	66.842
3	82.187	2.227	13.920	80.762
4	92.818	1.929	12.056	92.818
5				
6				
7				
8				
9				
10				
11				
12				
13				
14				
15				
16				

Extraction Method: Principal Component Analysis.