LAUREA AMMATTIKORKEAKOULU Uuden edellä

Turvallisuus- ja pelastusviranomaisten ICT-järjestelmien kehittäminen ja integraatio

Hult, Taina

2012 Leppävaara

Laurea-ammattikorkeakoulu
Laurea Leppävaara

Turvallisuus- ja pelastusviranomaisten ICT-järjestelmien kehittäminen ja integraatio

Taina Hult
Tietojenkäsittelyn koulutusohjelma
Opinnäytetyö
Kesäkuu, 2012

Laurea-ammattikorkeakoulu **Tiivistelmä**
Laurea Leppävaara
Tietojenkäsittelyn koulutusohjelma
Tietojärjestelmät ja tietoliikenne

Hult Taina

Turvallisuus- ja pelastusviranomaisten ICT-järjestelmien kehittäminen ja integraatio

Vuosi 2012 Sivumäärä 69

Väestön turvaamisen ja pelastustoiminnan tärkeimpiä työvälineitä ovat hälytysajoneuvot. Näihin asennettujen teknisten järjestelmien ja laitteiston määrä on kasvanut huomattavasti tuoden mukanaan erilaisia toiminnallisuusongelmia esimerkiksi ajoneuvojen turvajärjestelmissä. Myös sähkön tarve on lisääntynyt, mikä aiheuttaa erinäisiä ongelmia sekä paineita alentaa virrankulutusta. Käytössä olevien ratkaisujen dokumentointi on vaihtelevaa, eikä alalla ole tapahtunut kaivattua standardisoitumista.

Syksyllä 2010 käynnistyi kolmivuotinen Tekesin rahoittama ja Laurea-ammattikorkeakoulun koordinoima MOBI (Mobile Object Bus Interaction) –hanke, jossa kehitetään hälytysajoneuvoihin yhteinen ICT-laitteiden ja -sovellusten infrastruktuuri. Hankkeen tavoitteena on viedä Euroopan laajuisille markkinoille suunniteltu toimiva tuote liiketoimintamalleineen. Hankkeen päätavoite on luoda standardisoitumista, joka mahdollistaisi markkinoille vietävät kaupalliset tuotteet. Hanke koostuu kahdesta yrityshankkeesta sekä Laurea-ammattikorkeakoulun johtamasta tutkimusprojektista. Tutkimusprojekti tuottaa ja dokumentoi aiheeseen liittyvää tutkimustietoa, jonka pohjalta tullaan toteuttamaan tietojärjestelmäarkkitehtuurilla ja järjestelmien integraatiolla varustettu demoajoneuvo.

Tämä opinnäytetyö on osa MOBI-tutkimusprojektia ja työssä kuvataan pelastus- ja turvallisuusviranomaisten asettamia vaatimuksia ja tarpeita kenttähenkilöstön ja komentokeskuksien välillä kulkevalle kriittiselle tietoliikenteelle. Viranomaisilla tulee olla jatkuvat yhteydet kriittisiin järjestelmiin, joista saadaan tehtävien hoitamisen kannalta tärkeää tietoa. Työssä esitellään monikanavareiritykseen perustuva tietoliikenneratkaisu sekä järjestelmien välistä yhteentoimivuutta tehostava ohjelmistoarkkitehtuurin ajatusmalli.

Tutkimuksessassa hyödynnettiin Jay Nunamakerin luomaa monimenetelmällistä suunnittelututkimusta. Monimenetelmällisessä suunnittelututkimuksessa esitetään kuinka teorian kehittäminen, tutkimusmenetelmät, kokeellisuus ja järjestelmäkehitys muodostavat yhtenäisen tutkimusprosessin.

DSiP-järjestelmän avulla mahdollistetaan useamman erilaisen tiedonsiirtomenetelmän (3G, UMTS, HSDPA, GRPS, Tetra, WiFi jne.) hyödyntämisen rinnakkain niin, että se näkyy loppukäyttäjälle yhtenä vakaana ja turvallisena “multipoint-to-multipoint” yhteytenä. Palvelupohjaisella ohjelmistoarkkitehtuurilla voidaan parantaa turvallisuus- ja pelastusviranomaisten tietojärjestelmäkokonaisuuden yhteentoimivuutta, jolloin eri-ikäiset ja eri tekniikalla toteutetut Web-sovelluspalvelut voitaisiin määrittää käyttäjäryhmäkohtaisesti eri hälytysajoneuvotyyppeihin (poliisiautoon, ambulanssiin tai paloautoon). Molemmilla tutkituilla ratkaisuilla voitaisiin saavuttaa MOBI-hankkeen asettamia tavoitteita, joten niitä voitaisiin soveltaa lopullisen tuotteen implementointiin.

Avainsanat: kriittinen tietoliikenne, järjestelmäintegraatio, monikanavareititys, ohjelmistoarkkitehtuuri, palvelupohjainen ohjelmistoarkkitehtuuri, SOA, DSiP

Laurea University of Applied Sciences **Abstract**
Laurea Leppävaara
Information Technology programme
Information Systems and Data Communication

Hult, Taina

Public Protection and Disaster Relief services ICT-systems developing and integration

Year 2012 Pages 69

In field operations of Public Protection and Disaster Relief (PPDR) services, vehicles are the most important tools. The number of technical devices and applications in vehicles has increased considerably, which has generated different technical problems e.g. in vehicles security systems. Power consumption has also increased, which generates new problems and pressure to reduce power consumption. Documentation of the solutions applied is varied and there has been no standardization in the field.

MOBI (Mobile Object Bus Interaction), a three-year project led by Laurea University of Applied Sciences and funded by Tekes, started in September 2010. The purpose of this project is to create a common ICT hardware and software infrastructure for all emergency vehicles. The aim of the project is to develop product concepts which have potential in both domestic and export markets. The main objective of this project is to create standardization in this field which enables exporting a commercial product including commercializing plans to be offered in the European market. The programme consists of two industrial projects and a research project led by Laurea University of Applied Science. The research project generates relevant research data for the industrial project. From the results of the research a demo vehicle with workable ICT-systems integration will be made.

This thesis is part of the research project and it describes needs and requirements of PPDR mission critical communication in surveillance situations on land, at sea and in the air. It will present one traffic engineering solution for secure communication and one software architecture paradigm which enables system integration.

This research work followed the multimethodological approach created by Jay Nunamaker for information system research. In the multimethodological approach theory building, observation, experimentation and systems developing phases are integrated during the research process. The conclusive research report consists of four international publications published in 2011. The publications cover PPDR's mission critical communication, multichannel routing communication and service oriented computing based software architecture paradigm for system integration.

DSiP communication system enables routing data over any kind of connection (IP and non-IP) and works in multi-operator environments applying satellites, 3G, GRPS, UMTS, HDSPA, IP-network, TETRA, serial connections and radio modems. Customers can use multiple communication channels in parallel in such a way, that ending peers "think" they are using one channel. SOA paradigm enhances fire and rescue departments ICT systems usability, performance, scalability, reliability, availability, extensibility, maintainability, manageability and so on. With these two presented solution we could achieve objectives of MOBILE project.

Keywords: mission critical communication, system integration, multichannel routing, software engineer, Service-Oriented Architecture, SOA, DSiP

Sisällys

Lista julkaisuista

Julkaisu 1) Hult, T. & Rajamäki, J. 2011. ICT Integration of Public Protection and Disaster Relief (PPDR): Mobile Object Bus Interaction (MOBI) Research and Development Project, 10. WSEAS kansainvälinen konferenssi. Applied Electromagnetics, Wireless and Optical Communications (ELECTROSCIENCE '11). Meloneras, Kanariansaaret Espanja, 24.-26.3.2011. Sivut 143-148

Julkaisu 2) Rajamäki, J., Hult, T. & Ofem, P. 2011. ICT integration of public protection and disaster relief: services for fire and rescue personnel International Journal Of Communications. Volume 5, 2011. Sivut 119-132.

Julkaisu 3) Holmstrom, J. Rajamäki, J. & Hult,T. 2011. DSiP Distributed Systems intercommunication Protocol - A Traffic Engineering Solution for Secure Multichannel Communication in Proc. 9th WSEAS International Conference on Applied Electromagnetics, Wireless and Optical Communications (ELECTROSCIENCE '11), Meloneras, Kanariansaaret, Espanja 24.-26.2011 Sivut 57-60.

Julkaisu 4) Holmstrom, J. Rajamäki, J. & Hult,T. 2011. The future solutions and technologies of public safety communications - DSiP traffic engineering solution for secure multichannel communication. International Journal Of Communications. Issue 3, Volume 5, 2011. Sivut 115-122.

1 Johdanto

Väestön turvaamiseen ja katastrofiavun toimijoiden, kuten tullin, rajavartiolaitoksen, poliisin, pelastuslaitoksen, ensihoidon ja puolustusvoimien kenttätyöskentelyn tärkeimpiä työvälineitä ovat ajoneuvot sekä niihin asennetut laitteet ja järjestelmät. Sisäasiainministeriön teettämässä pelastustoimen strategiaa 2025 -julkaisussa todetaan, että viranomaisten toiminta perustuu yhä enenevissä määrin tietojohtoiseen ohjausmalliin. Keräämällä sekä analysoimalla eri lähteistä saatavaa tietoa, pystytään kohdentamaan resursseja ja hoitamaan tehtäviä entistä tehokkaammin (Pelastustoimen strategia 2025, 8.) Tärkeimmät pelastustehtävät suoritetaan kentällä. Viranomaistahojen kenttätyöskentelyssä hyödynnettävien järjestelmien ja laitteiden tulee toimia moitteettomasti paikasta riippumatta haasteellisissakin olosuhteissa. Niiden tulee olla ominaisuuksiltaan vakaita, turvallisia, luottamuksellisia, eheitä ja saavutettavia.

Viranomaisten ammattikäyttöön suunniteltu VIRVE (viranomaisradioverkko) perustuu TETRA-standardiin, minkä avulla kriittinen viestintä mahdollistetaan. VIRVE on yksityinen radioverkko kriittisten toimintojen suorittamiseksi (Aronsson 2012, 14). Pelastuslaitoksen vuonna 2011 teettämässä tutkimuksessa kuvataan VIRVEä ja siihen liittyviä langattoman tiedonsiirron rajoitteita ja tulevaisuuden haasteita pelastustoimessa. VIRVE soveltuu puhepalveluihin ja kapeakaistaiseen datasiirtoon, mutta leveäkaistaiset laajakaistaiset palvelut pitää hoitaa jollain muulla tavalla. VIRVEn heikko kohta onkin vaatimaton tiedonsiirtonopeus ja sen avulla voidaan välittää lyhyitä tila- ja paikannusviestejä, joita kutsutaan lyhytsanomiksi. Isompien tiedostojen kuten kuvien, videon ja multimedian siirtoon se ei sovellu sen hitauden vuoksi. Vaikka lyhytsanomaviestit kuormittavat VIRVEä keskimäärin vähän, niin paikallisia ja ajoittaisia kuormitushuippuja on havaittu esimerkiksi viime vuosina tapahtuneissa ampumistapauksissa Jokelassa ja Kauhajoella sekä Espoon Sellon kauppakeskuksessa. VIRVEn datasiirron rajoittuneisuus on johtanut erinäisiin kokeiluihin, joissa on hyödynnetty kaupallisten verkkojen (esimerkiksi 2G/3G ja @450) palveluita. Näin on voitu siirtää myös isoimpia tiedostoja. Suurin ongelma kaupallisten dataverkkopalveluiden hyödyntämisessä on se, että niitä ei ole suunniteltu kriittisen tietoliikenteen vaatimuksia vastaamaan. Esimerkiksi katastrofitilanteen sattuessa nämä palvelut saattavat ylikuormittua suuren tiedonsiirron tarpeen vuoksi, jolloin tärkeät palvelut eivät ole saatavissa (Rantama & Junttila 2011, 37-39).

Laurea-ammattikorkeakoulu käynnisti kolmivuotisen MOBI (Mobile Object Bus Interaction)hankkeen syksyllä 2010 ja toimii tämän opinnäytetyön toimeksiantajana. Hankkeen suurin rahoittaja on TEKES. Hanke koostuu kahdesta yritysprojektista sekä Laurea-ammattikorkeakoulun johtamasta tutkimusprojektista. Rajamäki ja Villemson (2009) kuvaavat tutkimusongelmaa ja kertovat viranomaisten kenttätyöskentelyssä käytössä olevien järjestelmien ja laitteiston määrän kasvaneen runsaasti. Laitevalmistajien määrä on kirjava

eivätkä kaikki sovelletut ratkaisut vastaavat vaatimuksia, joita tulevaisuuden kriittiselle tietoliikenteelle asetetaan. Laitteden määrän kasvun seurauksena onraportoitu erilaisista toiminnallisuusongelmista esimerkiksi ajoneuvojen turvajärjestelmissä. Myös sähkön tarve on lisääntynyt, mikä aiheuttaa erinäisiä ongelmia sekä paineita alentaa virrankulutusta. Rajamäki ja Villemson (2009) täsmentävät, että sovellettujen ratkaisujen dokumentointi on vaihtelevaa, eikä alalla ole tapahtunut kaivattua standardisoitumista. ICT-integraatioon liittyy päätöksiin liittyviä haasteita, kuten se, että mitä protokollia laitteiden tulisi tukea (Rajamäki & Villemson 2009, 1-6). MOBI-hankkeessa tutkitaan ja dokumentoidaan käyttäjän tarpeita ja vaatimuksia, määritellään nykyiset järjestelmät, tutkitaan ajoneuvojen sähkön kulutusta ja tarvetta. Hankkeen tavoitteena on kehittää viranomaisten kriittistä tietoliikennettä ja järjestelmien välistä yhteentoimivuutta. Tutkimustuloksien perusteella tullaan rakentamaan demoajoneuvo toimivalla tietojärjestelmäarkkitehtuurilla, järjestelmien integraatiolla ja kriittisillä tietoliikenneyhteyksillä.

MOBI-tutkimusprojektin tavoitteena on luoda pohja vientiin tähtäävälle viranomais- ja hälytysajoneuvokonseptille, johon partnereiksi haetaan ajoneuvoteollisuutta ja sen kanssa yhteistyössä olevia sovellusintegraattoreita. Tarkoitus on saada alkuun alan standardoitumiskehitys like-minded-maiden ja mahdollisesti EUROPOL:n kanssa. Tutkimusprojektin rinnalla käynnistyy kolme yrityshanketta, jotka hyödyntävät tämän tutkimusprojektin tuloksia (MOBI projektisuunnitelma 2010, 5).

Tämä tutkimus on osa MOBI-hankkeen tutkimusprojektia ja sisältää neljä kansainvälistä vuonna 2011 julkaistua julkaisua, jotka käsittelevät PPDR-viranomaisten kriittiselle tietoliikenteelle asettamia tarpeita ja vaatimuksia sekä kriittisten järjestelmien välistä yhteentoimivuutta.
Ensimmäinen julkaisu käsittelee MOBI-hankkeen suunnittelua ja toteuttamista. Toisessa julkaisussa käsitellään viranomaisten kriittisen viestinnän vaatimuksia sekä esitellään palveluarkkitehtuuri-ajatusmalli järjestelmäintegraation toteuttamiseksi. Kolmannessa ja neljännessä julkaisuissa käsitellään monikanavareititykseen perustuvaa tietoliikennejärjestelmää. Työn lopussa arvioidaan tutkimustuloksissa esitettyjen ratkaisujen soveltamista lopulliseen markkinoille vietävän tuotteen toteuttamiseen.

2 Tavoite, menetelmät ja rajaus

Tutkimus liittyy toimeksiantajan koordinoimaan MOBI-tutkimusprojektiin ja tavoitteena on tutkia erilaisia ratkaisuja, joilla voitaisiin parantaa viranomaistahojen yhteistyöstä kriittisen tietoliikenteen ja järjestelmien välisen yhteentoimivuuden osalta. Tutkimuksessa pyritään vastaamaan seuraaviin kysymyksiin:

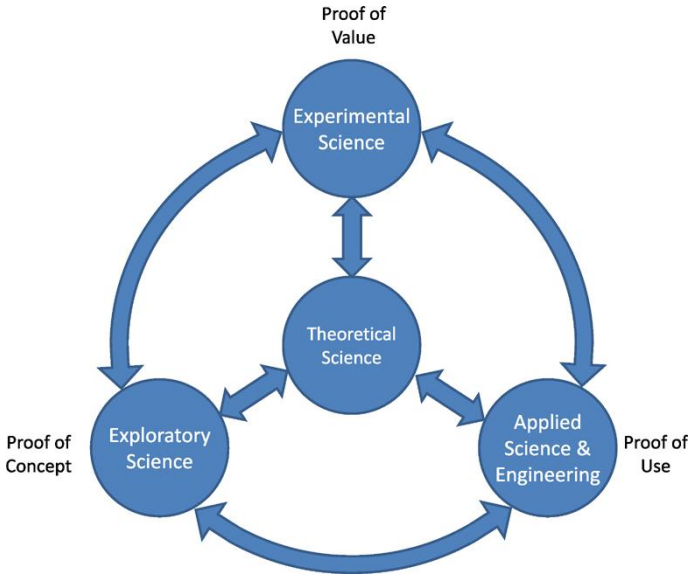
- Kuinka PPDR-viranomaisten kriittisiä tietoliikenneyhteyksiä ja järjestelmien välistä yhteentoimivuutta voitaisiin kehittää niin, että saavutetaan vakaa ja turvallinen integroitu yhteentoimiva tietojärjestelmä kenttätehtävien suorittamiseen?
- Kannattaako tutkittavia ratkaisuja hyödyntää?

2.1 Monimenetelmällinen suunnittelututkimus

Mikään tietojenkäsittelytiede yksistään jollain teknisellä ratkaisullaan ei pysty vastaamaan nykypäivän turvallisuuteen liittyviin ongelmiin riittävän yhtenäisellä tasolla. Jos käynnistetään innovatiivisista artefakteista toimintaa ja analysoidaan, kuinka niitä voidaan käyttää ja hyödyntää, nähdään sellaisia asioita, joita ei pelkässä laboratorioympäristössä pysty näkemään.

Kansainvälisesti tunnetun tutkijan, opettajan ja tietojärjestelmien johtavan asiantuntijan Jay Nunamakerin mukaan tietojärjestelmien hallinnointiin tarvitaan kolmea ensisijaista resurssia: ihmistä, teknologiaa ja tietoa. MOBI-hankkeessa seurataan tätä tavanomaista tietojärjestelmän monimenetelmällisen tutkimuksenn periaatetta (kuvio 1), jonka Nunamaker kehitti 1991 (Nunamaker 2010).

Käsite kehitystutkimus (Development Research, DR) on jatkumoa tieteellisille menetelmille käyttäen jokaista tietojärjestelmien suunnitteluun (Design Science Research, DSR) liittyviä näkökohtia, joita March ja Smith, VanAken yms. kuvaavat teoksissaan aiheina tietojärjestelmien tutkiminen ja suunnittelu. Näitä näkökohtia käytetään esittämään tietojärjestelmien suunnitteluun liittyviä valintoja sekä käyttämään erilaista järjestelmätekniikkaa havainnollistamaan tiedettä. Design Science Research on lähestymistapa, joka voidaan yhdistää muihin sosiaalisen tieteen menetelmiin, kuten strategiaan ja analyysimenetelmään (grounded theory) tai toiminnalliseen toimintatutkimukseen (action research) kuten myös tapaustutkimukseen (case study). (March, Smith 1995; VanAken 2004 ; Henver, March, Park & Ram 2004).



Kuvio 1: Monimenetelmällinen suunnittelutkimus (Nunamaker 2010)

Kuvio 1 kuvaa MOBI-hankkeen tutkimusmenetelmiä, jotka sisältävät teoreettisen tietopohjan soveltamisen laboratorio- ja kenttäympäristössä. Nunamakerin mukainen motto ”going to the last mile” toimii tämän tutkimuksen lähtökohtana, sillä kyseessä on todelliset ongelmat todellisille ihmisille. Tutkimusprosessi sisältää kolme vaihetta:

- ”Proof of Concept ” (POC)
- ”Proof of Value” (POV)
- ”Proof of Use” (POU)

Suunniteltuja artefakteja ei voida ymmärtää eikä voida oikeastaan arvioida ennen kuin ne toteutetaan oikeasti. POC- ja POV-vaiheen lisäksi pitää pyrkiä myös POU-vaiheeseen, sillä loppukäyttäjillä on keskeinen rooli tässä hankkeessa:

- He ovat törmänneet näihin todellisiin ongelmiin, joihin MOBI-hanke pyrkii löytämään ratkaisua
- Vain heidän avullaan voidaan toteuttaa POU-vaihe

Tämä tutkimus liittyy MOBI-hankkeen tutkimusprosessin ytimeen eli teoriasouuteen ja se toteutetaan laadullisena tutkimuksena. Tutkimuksen tarkoituksena on kehittää teoriaa edelleen. Tutkimustuloksia voidaan mitata käytännön tasolla MOBI-hankkeen muissa tutkimusprosessin vaiheissa, jolloin hankkeen monimenetelmällisyys tulee esiin.

2.2 Rajaus

Väestön turvaamisen ja katastrofiaputoimintaan kuuluu useita viranomaistoimijoita ja tämä tutkimus rajataan poliisi- ja pelastusviranomaisten näkökulmaan. Tutkimustuloksissa viitataan myös terveydenhuollonviranomaisiin, jotka ovat hyödyntäneet yhtä tässä tutkimuksessa esitettyä ratkaisua. Järjestelmäintegraation toteuttamiseen on kehitetty monia malleja ja tässä tutkimuksessa perehdytään palvelupohjaiseen arkkitehtuurimalliin.

Tutkimuksessa hyödynnetään aiempaa koulutukseni kautta saatua tietojärjestelmiin, tietoturvaan ja tietoliikenteeseen liittyviä tietoja ja taitoja. Tutkimustulokset esitellään työn liitteenä olevassa neljässä kansainvälisessä julkaisussa. Työ sisältää myös suomenkieliset lyhennelmät näistä julkaisuista.

- Julkaisu 1: ICT Integration of Public Protection and Disaster Relief (PPDR): Mobile Object Bus Interaction (MOBI) Research and Development Project. Taina Hult & Jyri Rajamäki.

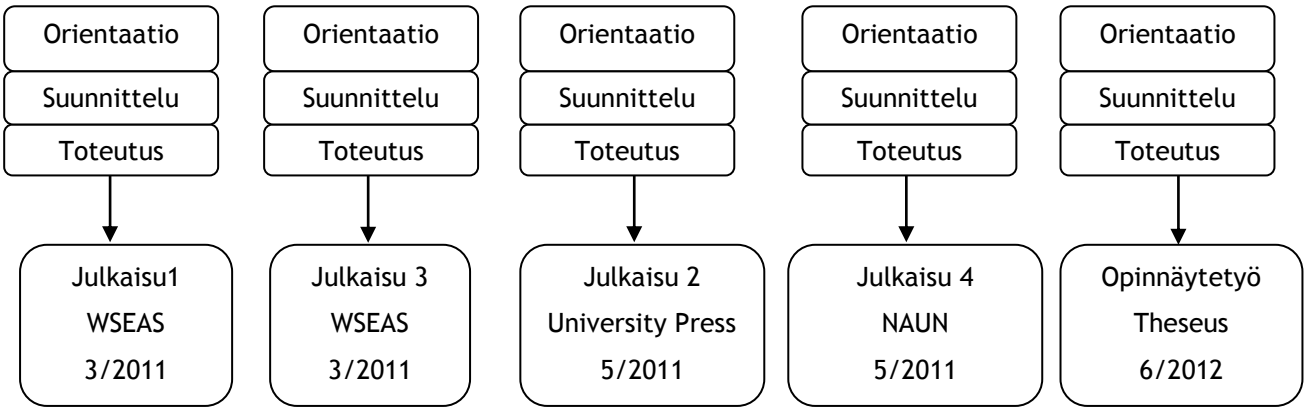
- Julkaisu 2: ICT Integration of Public Protection and Disaster Relief: Services for Fire and Rescue Personnel. Jyri Rajamäki, Taina Hult ja Paulinus Ofem

- Julkaisu 3: DSiP Distributed Systems intercommunication Protocol - A Traffic Engineering Solution for Secure Multichannel Communication. Laajannettu versio julkaisusta nro 1. John Holmstrom, Jyri Rajamäki, Taina Hult

- Julkaisu 4: The Future Solutions and Technologies of Public Safety Communications - DSiP Traffic Engineering Solution for Secure Multichannel Communication. Laajannettu versio julkaisusta nro 3. John Holmström, Jyri Rajamäki ja Taina Hult

Kuvio 2 esittää opinnäytetyön tutkimusprosessia:

- Perehtyminen tutkimusongelmaan (orientaatiovaihe)
- Suunnitelman tekeminen (suunnittelmauvaihe)
- Tuotokset kansainvälisten julkaisujen muodossa (toteutusvaihe)
- Tuloksien arviointi (julkaisuvaihe)



Kuvio 2: Tutkimusprosessi

3 Käsitteet

DSiP (Distributed Systems intercommunication Protocol): on Ajeco Oy:n kehittämä protokolla, joka mahdollistaa laitteille ja ohjelmistolle keskeytymättömän tietoliikenneyhteyden. Ratkaisu perustuu useampaan rinnakkain toimivaan yhteyteen ja monikanavareititykseen. Se on täysin riippumaton yksittäisistä operaattoreista. Loppukäyttäjille DSiP-järjestelmä näkyy kuin yhtenä vakaana tietoliikenneyhteytenä (Ajeco Oy 2009.)

Kriittinen tietoliikenne (mission critical communication): Ammattikäyttäjien, kuten väestön turvaamisen ja pelastustoiminnan viranomaisten välistä tietoliikenneyhteyksien kautta kulkevaa viestintää, joka mahdolistaa yhteyksien kautta kulkevan tiedon turvallisuuden ja saatavuuden. Sitä hyödynnetään puheen ja sovellusten kanssa kriittisissä toiminnoissa ja se on toteutettu jollain langattomalla tietokoliikenneyhteyden avulla (TCCA 2012, 14.)

Public Protection Disaster Relief (PPDR): Termillä tarkoitetaan väestön ja omaisuuden turvaamiseen liittyviä palveluita kuten esimerkiksi lainvalvonta, palontorjunta, ensiapu ja katastrofiapu (Baldini 2010, 8.)

SOA (Service-oriented architecture): Palvelupohjainen ohjelmistoarkkitehtuurin ajatusmalli. Se sisältää joukon erilaisia määrityksiä ja menetelmiä, joita voidaan hyödyntää ohjelmistojen suunnittelussa ja kehittämisessä. Sen avulla voidaan määritellä, miten integroidaan erilaisia sovelluksia WEB-pohjaiseen ympäristöön alustasta riippumatta (Bell 2008.)

SOAP (Simple Object Access Protocol): Pääasiassa Microsoftin kehittämä ja W3C:n ylläpitämä XML-protokollaan perustuva tietoliikenneprotokollastandardi mahdollistamaan proseduurien etäkutsut (W3C 2000.)

Standardi: Hyväksytty ja monistettavissa oleva menetelmä tehdä ja toteuttaa jokin asia. Standardista on julkaistu dokumentti, joka sisältää esimerkiksi tekniset määritelmät ja kriiterit. Standardin sääntöjen, suosituksien ja määritelmien avulla mahdollistetaan palveluiden helppo toteuttaminen luotettavasti ja tehokkaasti (BSi, 2012.)

URI (Uniform Resource Identifier): Merkkijonosta koostuva kokonaisuus, mikä tunnistaa abstraktit ja fyysiset resurssit. URI:n erikoistapausta eli URL:ää (Uniform Resource Locator) käytetään osoittamaan WEB-sivuja (T. Berners-Lee 1998.)

Web-sovelluspalvelu (Web-service): Tarjoaa palveluita sovellusten käytettäväksi. Palvelut on toteutettu standardoitujen Internet-yhteyskäytäntöjen avulla esimerkiksi SOAP-protokollan avulla, mikä hyödyntää XML-kieltä. Se mahdollistaa sovelluksen hyödyntämisen millä tahansa alustalla. W3C osallistuu aktiivisesti web-sovelluspalveluiden kehittämiseen. (Tietotekniikan termitalkoot 2012 ; W3Ca 2012a.)

W3C (World Wide Web Consortium): 1994 kansainvälinen yritysten ja yhteisöjen yhteenliittymä, joka ylläpitää ja kehittää WWW:n standardeja tai suosituksia. Yhteisöä johtaa WWW:n kehittäjä Tim Berners-Lee (W3C 2012b.)

XML (Extensible Markup Language): W3C:n kehittämä standardi ja merkintäkieli, jonka avulla tiedon merkitys voidaan kuvata tiedon sekaan. Se on yleinen formaatti järjestelmien väliseen tiedonsiirtoon ja dokumenttien tallentamiseen, joka auttaa jäsentämään laajoja tietomassoja (W3C 2012c.)

4 Toimintaympäristö ja tutkimuksen lähtökohta

Eur-Lex listaa väestön turvaamisen ja katastrofiaputoiminnan julkisten turvallisuuspalvelun toimijoiksi seuraavat viranomaistahot: poliisi, palolaitos, ambulanssit, puolustusvoimat, etsintäpartiot jne. Myös Euroopan unioni kannattaa jäsenvaltioiden välistä tehokasta koordinointimekanismia, jonka avulla voitaisiin tehostaa hätäaputoimia ja vähentää toimien päällekkäisyyksiä. Komissio totesi jo vuonna 2003 Maailman radioviestintäkonferenssissa seuraavanlaisesti: ”Vaikka taajuuksia on yhdenmukaistettu yhteisössä jonkin verran, laitteiden yhteentoimivuuden puute on alalla ilmeistä, ja siihen on puututtava asteittain siten, että turvallisuuspalvelujen toiminnalliset vaatimukset asetetaan etusijalle.” Tavoitteena olisi taata tietoliikennelaitteiden yhteentoimivuus myös kustannustehokkuus- ja toiminnallisuussyistä. Eur-Lex kuvaa, että tällä hetkellä viranomaistoiminnan yhteentoimivuuteen liittyy rajoittavia tekijöitä jopa maiden sisällä, mikä johtuu siitä, että erilaisilla turvallisuuspalveluilla on omat hankintapolitiikkansa. Viestintälaitteiden elinkaari on pitkä, jolloin valmistuserätkään eivät ole suuria. Maalla tapahtuvissa kriisitilanteissa on

vaikeaa sallia ulkomaisten apujoukkojen käyttää omia viestintälaitteitaan tai, vaikka ne sallittaisiinkin, laitteiden erojen takia niiden on vaikea viestiä keskenään (Eur-Lex 2003).

4.1 Kansainvälisen poliisiyhteistyön toimijat

Keskusrikospoliisi (KRP) vastaa vakavimmasta ja luonteeltaan järjestäytyneestä ja ammattimaisesta rikollisuuden torjunnasta. Tämän lisäksi KRP tuottaa asiantuntijapalveluita liittyen rikostorjuntaan koko poliisikunnalle ja muille lainvalvontaviranomaisten käyttöön (Poliisi 2012.)

Europol (European law enforcement agency) on Euroopan Union jäsenmaiden poliisiorganisaatioiden yhteenliittymä, joka tukee jäsenien lainvalvontatoimia. Pääasiallinen tehtävä on kerätä ja välittää rikostiedustelutietoja, minkä päämääränä on parantaa rikostutkinnan ja ennaltaehkäisevän työn tehokkuutta (Europol 2012.)

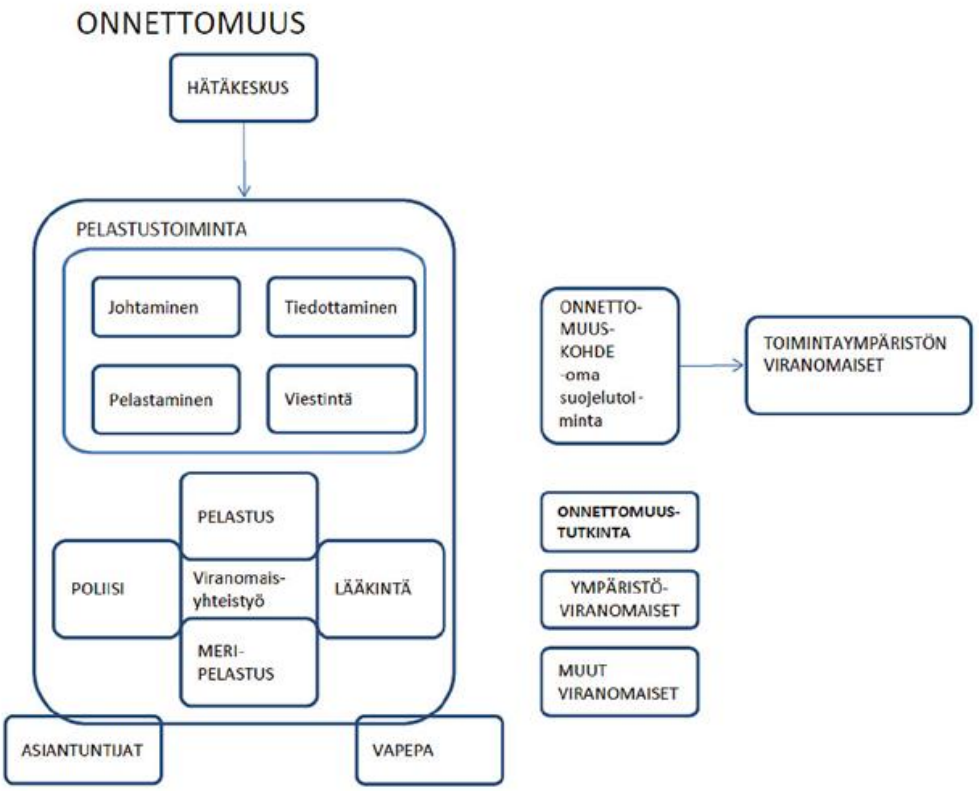
Eurojust (Euroopan unionin oikeudellisen yhteistyön yksikkö) on Euroopan unionin elin, joka edistää EU:n jäsenmaiden toimivaltaisten oikeusviranomaisten yhteistyötä, kun käsitellään rajat ylittävää, vakavaa ja järjestäytynyttä rikollisuutta (Euroopan unioni 2012.)

Interpol (International Criminal Police Organization) on maailman suurin kansainvälinen rikospoliisijärjestö, joka kehittää jäsenmaidensa rikospoliisien yhteistyötä (Interpol 2012.)

Euroopan rikosoikeudellinen verkosto (EJN) parantaa Euroopan unionin jäsenvaltioiden keskinäistä oikeudellista ja käytännön avunantoa vakavan rikollisuuden torjumiseksi (EJN 2012.)

4.2 Viranomaistahojen yhteistyö suuronnettomuuspaikalla

Cosafen teettämässä oppaassa (2011) kuvataan suuronnettomuuksiin varautumista, tässä tapauksessa harvaanasutuilla alueilla. Usein tapahtumaketju saa alkunsa yhteydenotolla hätäkeskukseen, jota johtaa joko pelastustoimi maalla tai merivartiosto merellä. Hätäkeskus ja ensimmäiset paikalle ehtivät viranomaiset ovat avainasemassa tunnistettaessa suuronnettomuutta. Myös lääkintähenkilöstö ja poliisi saapuvat paikalle usein. Toimintaan kuuluu itse pelastustehtävän lisäksi johtamista, tiedottamista niin paikallisille kuin kansainvälisille tiedotusvälineille sekä viestintää pelastustahojen kesken. Kuviossa 3 esitetään viranomaistahojen yhteistyötoimintaa pelastustehtävässä (Cosafe 2012).



Kuvio 3: Viranomaistahojen yhteistyö onnettomuudessa (Cosafe 2012, 6)

5 Lyhennelmät julkaisuista

Tämä luku vastaa opinnäytetyön alussa esitettyihin tutkimuskysymyksiin. Tutkimuskymyksiin liittyvät ratkaisut esistetään neljän tieteellisen artikkelin muodossa ja näistä julkaisuista on koostettu tähän opinnäytetyöhön lyhennelmät omiksi alaluvuikseen:

1) **Väestön turvaamisen ja katastrofiaputoiminnan ICT-integraatio: Mobile Object Bus Interaction (MOBI) tutkimus- ja kehityshanke.** Kyseessä on konferenssipaperi, joka esitettiin WSEAS-järjestön järjestemässä 10. konferenssissa, jonka aiheena oli “Communications, electrial & computer engineering”. Koneferenssi järjestettiin 3/2011 Espanjassa.

2) **Väestönsuojelun ja katastrofiavun ICT-järjestelmien integraatio: Palo- ja pelastushenkilöstön palvelut.** Laajempi versio ensimmäisestä konferenssipaperista, mikä julkaistiin 5/2011

3) **DSiP Distributed Systems intercommunication Protocol – tietoliikenneratkaisu vakaaseen ja turvattuun monikanavaviestintään.** Kyseessä on konferenssipaperi, joka esitettiin WSEAS-järjestön järjestemässä 10. konferenssissa, jonka aiheena oli

"Communications, electrial & computer engineering". Koneferenssi järjestettiin 3/2011 Espanjassa

4) **Tulevaisuuden monikanavareititykseen perustuvat turvalliset teknologiaratkaisut.** Laajempi versio kolmannesta konferenssipaperista, mikä julkaistiin 5/2011.

Nämä neljä tieteellistä artikkelia täydentävät MOBI-hankkeeseen liittyvää esitutkimusta. Opinnäytetyössä käsiteltävät aihealueet liittyvät MOBI-hankkeen seuraaviin tiiviisti toisiinsa liittyvään työpakettiin:

- Työpaketti 4 tietoliikenne
- Työpaketti 5 järjestelmäintegraatio

5.1 Väestön turvaamisen ja katastrofiaputoiminnan ICT-integraatio: Mobile Object Bus Interaction (MOBI)-tutkimus- ja kehityshanke

Väestön turvaamiseen ja katastrofiapuun liittyviä palveluita harjoittavia toimijoita ovat esimerkiksi poliisi, palo-, pelastus-, ensihoito- ja sairaankuljetuslaitokset. Nämä palvelut tuottavat lisäarvoa yhteiskunnalle luomalla vakaan ja turvallisen ympäristön. Työtehtävät käsittävät kansalaisten sekä ympäristön turvaamisen, ja tehtävät voivat olla ihmisen tai luonnon aiheuttamia. Tärkeimmät pelastustehtävät suoritetaan vaihtelevissa olosuhteissa maalla, merellä ja ilmassa. Tehtävien suorittamiseen tarvittavien välineiden tulee vastata tarpeita ja vaatimuksia. Ajoneuvot ja niihin asennetut laitteet sekä järjestelmät ovat avainasemassa, mutta myös työturvallisuuteen, tehokkuuteen ja ergonomiaan tulee kiinnittää erityishuomiota. Ajoneuvojen ja niihin asennettujen laitteiden tulee olla vakaita ja turvallisia.

Ajoneuvoissa olevien laitteiden, sovellusten ja tärkeiden tietoliikenneyhteyksien määrä on kasvanut viime vuosikymmeninä. Tämä on lisännyt erilaisten käyttöliittymien lukumäärää, jota aiheuttaa ongelmia tilankäytön suhteen. Esimerkiksi ajoneuvojen turvatyynyillä on vähemmän tilaa täyttyä. Myös erinäisistä teknisistä ongelmista liittyen virrankulutukseen ja kaapelointiin on raportoitu.

Toinen ongelma on sovellettujen ratkaisujen olematon dokumentointi hyödynnetyistä ja tämä johtuu siitä, että alalla ei ole tapahtunut standardisoitumista. Standardisoitumiseen liittyvät puutteet johtuvat siitä, että markkinoilla on niin monen eri laitevalmistajan tuotteita. Kirjava laitevalmistajien joukko lisää myös haastetta järjestelmäintegraation toteuttamiselle sekä standardisoitumiselle. Alalle kaivataan myös uusia toimintamalleja, jotta standardisoituminen olisi helpompaa ja myös uusille liiketoimintamalleille on kysyntää (Rajamäki ja Villemson 2009).

Sovelluksien ja laitteiston määrän lisääntyminen on johtanut tiedonsiirron räjähdysmäiseen kasvuun. Langattomalla tiedonsiirrolla tuetaan kenttätyöskentelyn liikkuvuutta tarjoamalla jatkuva tietoliikenneyhteys operaatioon liittyvien toimijoiden kesken. Kentällä suoritettavan tehtävän suorittamiseen tulee olla saatavilla:

- Ääniyhteys, jotta voidaan koordinoida avustustoimia ja kriisinratkaisua
- Onnettomuus- ja tilannekuvaksen luominen ja jakaminen kaikille tehtävää suorittaville vastuuviranomaisille
- Erilaisista antureista saadun tiedon kerääminen ja jakaminen
- Tehtävään suorittamiseen liittyvä tiedonhaku järjestelmien tietokannoista

Euroopassa on useita yleensä TETRA-/TETRAPOL-pohjaisia suojattuja yksityisiä radioverkkoja, jotka ovat ominaisuuksiltaan kapeakaistaisia. Baldini (2010) kuvaa, että pelastus- ja turvallisuusviranomaisten käytössä olevien sovelluksien langattomien laajakaistayhteyksien puutteellisuudet aiheuttavat todellisia ongelmia. Monet nykypäivänä kehitetyt sovellukset vaativat laajakaistaisia yhteyksiä toimiakseen ja näitä yhteyksiä tarjoavat useimmiten vain kaupalliset operaattorit. Alalla olisi kysynytää vakaalle monikanavaisuuteen perustuvalle tietoliikennejärjestelmä-konseptille, joka näkyisi loppukäyttäjälle kuin yhtenä tietoliikenneyhteytenä, mutta olisi toteutettu erillisinä rinnakkaisina tietoliikenneyhteyksinä. Ratkaisulta vaaditaan riippumatomuutta yksittäisistä operaattoreista (Rajamäki, Holmström & Knuuttila 2010). On tieteellisesti todistettu, että standardisoituminen vaikuttaa vahvasti sellaiseen liiketoimintaan, joka kehittää ja myy teknologiaa sekä teknologia-pohjaisia tuotteita ja palveluita – standardit ovat yksi tärkein mahdollistaja nopealle kasvulle (TEKES 2012).

5.1.1 Väestön turvaamisen ja katastrofiavun palveluiden ICT-järjestelmät

Turvallisuus- ja pelastusviranomaisten toiminta on lähes riippuvaista erilaisista ICT-järjestelmistä. Ajoneuvoihin asennetut langattomat tietoliikenneyhteydet ovat kriittisessä roolissa. Tieto ja palvelut tulee olla aina saatavilla joko yhden tai useamman langattoman arkkitehtuurin avulla.

5.1.2 Loppukäyttäjän näkökulma

Kuten on jo todettu, niin poliisi- ja pelastusviranomaisten toiminta on riippuvaista erilaisista tietojärjestelmistä. Varsinkin langattomat tietoliikenneyhteydet ovat avainasemassa ja niiden tulee olla turvallista ja luotettavaa.

Tietojärjestelmien kehittämisen yhtenä päämääränä on luoda standardisoitumista. Käytettävyys on yksi vaatimuksissa huomioon otettava kriteeri, sillä monet sovelletut ratkaisut ovat epäergonomisia, eikä edes helposti mukautettavia.

5.1.3 MOBI-hanke

Suomalaisen tutkimus-, kehitys-, ja innovaatiohjelma ”Mobile Object Bus Interaction” eli MOBI-ohjelman tavoitteena on etsiä ratkaisut aiemmin esitettyihin ongelmiin ja kehittää hälytysajoneuvoihin yhteinen ICT-laitteiden ja sovellusten infrastruktuuri. Infrastruktuuriin sisältyy ratkaisut esimerkiksi puhe- ja dataliikenteen laitteistoon, tietokoneisiin, näyttöihin, tulostimiin, antenneihin, kaapelointiin ja lisäksi ratkaisuissa esitetään kytkennät sekä rajapinnat tehtaalla varustettaviin hälytysajoneuvoihin.

Hanke koostuu kahdesta yritysprojektista sekä tutkimusprojektista, jonka tarkoituksena on kerätä, tuottaa ja dokumentoida tietoa yrityspojektien käyttöön. Tutkismusprojektissa selvitetään ja dokumentoidaan esimeriksi loppukäyttäjän asettamia vaatimuksia ja tarpeita sekä tähän asti sovellettuja ratkaisuja.

Cassidian Finnland Oy:n johtama projekti keskittyy kehittämään turvallisuus- ja pelastusviranomaisille kehitettävää ammattikäyttöön soveltuvaa ajoneuvoihin integroitavaa radioverkko-konseptia. Insta DefSec Oy:n projekti kehittää kansallisen turvallisuuden sovellusratkaisuja. Molemmissa yritysprojektissa hyödynnetään tutkimusprojektin tuloksia ja yhteisenä päämääränä on kehittää tuotekonsepti, jolla olisi potentiaalia sekä kotimaan että ulkomaan markinoilla. (TEKES 2012).

Tutkimus, kehitys- ja innovaatioprojekti on aloitettu Suomessa koska:

- Suomi on todistetusti menestynyt langattomien tietoliikenneratkaisujen kehittämistyössä (1G [NMt], 2G [GSM], 3G [UMTS])
- Ensimmäinen maailmassa rakennettu maanlaajuinen TETRA-standardiin perustuva VIRVE (viranomaisradio)-verkko on yleisessä viranomaiskäytössä Suomessa ja sitä hyödyntävät pelastus-, poliisi-, puolustus-, rajavartio-, terveys-, meripelastus ja valtion muut viranomaiset. VIRVE mahdollistaa maanlaajuisen yhteistoiminnan edellä mainittujen toimijoiden kesken.
- Suomessa on laajalti kokemusta erilaisista kenttäjohtojärjestelmistä, kuten poliisin toiminnassa käytetystä POKEsta ja pelastus toiminnassa käytetystä PEKEstä. Molemmat kenttäjohtojärjestelmät ovat olleet toiminnassa vuodesta 2006 lähtien (Vilppunen 2006 ; Nurhonen 2008). POKE-järjestelmä on toiminut pohjana pelastusviranomaiskäytössä olevan PEKE-järjestelmän kehittämistyössä.

- Suomessa on toimiva ja hyvin organistoitu yhteistyö eritasoisten viranomaisten välillä (esimerkiksi poliisi- sekä tulli- ja rajavartiolaitosviranomaisten kesken (Niemenkari 2010).
- Suomessa vallitsee innovatiivisuuteen kannustava ilmapiiri, sillä suomalaiset yritykset tekevät tiivistä tutkimus- ja kehitystyötä sekä korkeakoulujen että kilpailijoidensa kanssa. ”Suomi on pikemminkin klubi kuin maa” -slogan muistuttaa edellä mainituista faktoista (Ilmavirta 2010).

5.1.4 MOBI-tutkimusprojekti

Tutkimusprojekti kerää ja dokumentoi tietoa yritysprojekteille sovelletuista ratkaisuista. Myös SOA- ja Web-sovelluspalvelu pohjaisten palveluiden hyödyntämistä tutkitaan. Tutkimustulosten perusteella rakennetaan demo-hälytysajoneuvo, johon tehdään toimiva ICT-integraatio. Projekti tähtää lopullisella tuotteellaan Euroopan laajuisille like-minded maiden markkinoille.

5.1.5 Konsortio ja perustajajäsenet

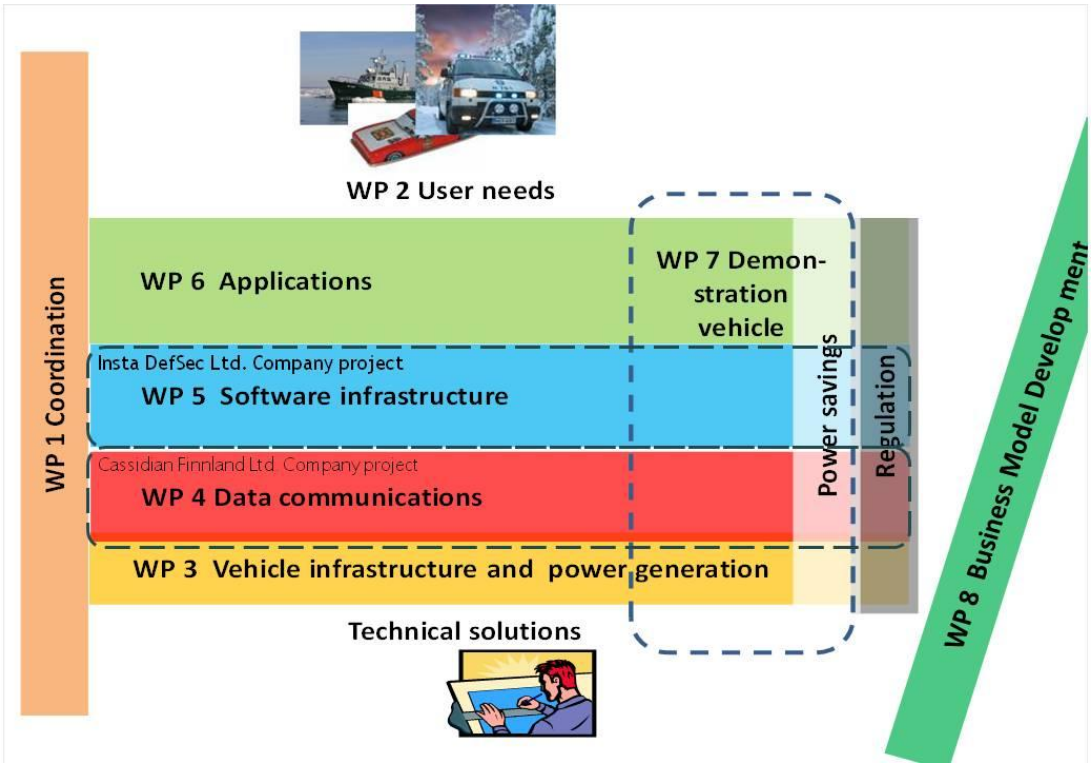
Konsortiota johtaa Laurea-ammattikorkeakoulu ja se koostuu kolmesta tutkimuslaitoksesta, kahdesta yrityskumppanista, kolmesta pienestä- ja keskisuuresta yrityksestä sekä useasta loppukäyttäjäorganisaatiosta. Toimintaa rahoittaa myös Tekes. MOBI-hankkeen budjetti on 800 000. Taulukossa 1 esitetään projektiin osallistujat ja niiden rahoitusosuus:

Rahoittajat	**€**	**%**
Tekes	480 000	60
Tutkimuslaitokset	108 000	13
Yrityskumppanit	110 000	14
PK-Yritykset	63 000	8
Loppukäyttäjät	39 000	5
Yhteensä	800 000	100

Taulukko 1: MOBI-hankkeen rahoittajat

5.1.6 Työpaketit

Kuvassa 1 esietään MOBI-ohjelman työpaketit ja yritysprojektien yhteenliittymät.



Kuva 1: MOBI-ohjelman työpaketit ja yritysprojektit (MOBI projektisuunnitelma 2010, 6)

TP1: Koordinointi

Työpaketti sisältää projektinhallintaan liittyviä tehtäviä ja tärkeimpänä tehtävänä on varmistaa, että MOBI-tutkimushanke tuottaa tutkimustietoa rinnakkaisille yrityshankkeille. Työpakettiin kuuluu myös yhteistyöhön ja tietojen vaihtamiseen liittyviä toimia muiden relevanttien projektien kanssa (mm. MOBIn rinnakkaiset yrityshankkeet, Jyväskylän yliopiston SCOPE-hanke, VTT Oulun ITEA2 -hanke ja Laurean muut hankkeet).

Työpaketissa hyödynnetään Wise Guys -paneeleita, jotka toimivat myös eri työpaketeille yhteisenä tilaisuuksina, joissa käydään läpi aikaansaannokset sekä jatkotoimenpiteet. Wise Guys -paneeleihin tuodaan työpakettien tuloksia tarkasteltavaksi. Wise Guys -paneelit rytmitetään kaikkien työpakettien mukaan siten, että ne ehditään järjestää ennen muiden työpakettien deadlineja. Työpakettiin osallistuvat tutkimusprojektin kaikki osapuolet (MOBI projektisuunnitelma 2010, 7-8).

TP 2: Käyttäjävaatimukset

Työpaketissa kartoitetaan viranomaisajoneuvojen nykyiset sähkö-, elektroniikka- ja ICT-järjestelmät (esimerkiksi poliisin tapauksessa sähköntuotannon teknologiat, radiolaitteet, videolaitteet, tutkat, keskinopeuden mittaus -laitteistot, hälytyslaitteet, IT-työasemat, tulostimet, vaa'at, biometriikkalaitteet, rekisterikilpien tunnistus, paikannus, tarkkuusalkometri, digitaalisen ajopiirturin lukulaite) sekä selvitetään näiden käyttäjä- ja viranomaisvaatimukset. Työpaketissa hyödynnetään aiempia tutkimuksia (esimerkiksi pelastustoimen osalta PELTI - Pelastustoimen langattoman tiedonsiirron tarpeet, KEJO, VITJA ja TOTI1/TOTI2 –hankkeita).

Työpaketissa yksilöidään hallinnolliset ja operatiiviset järjestelmät sekä määritetään näiden prioriteetti ja ylläpidettävyysvaatimukset. Lisäksi selvitetään mitä viranomaishyväksyntöjä (e-hyväksyntä, RTTE-, EMC-direktiivi) eri järjestelmät vaativat. Työpaketti toimittaa ajantasaisen kuvauksen suomalaisen hälytysajoneuvon IT-ratkaisuista, jossa vaatimukset ovat jäsenneltynä projektissa mukana olevien yritysten käyttöön (MOBI projektisuunnitelma 2010, 8-9).

TP 3: Ajoneuvojen infrastruktuuri ja virrankulutus

Tehon kulutus on yksi hälytysajoneuvojen ja niiden ICT-järjestelmien suurimmista haasteista. Tässä työpaketissa mm. selvitetään tarvittavien fyysisten ja virtuaalisten tietokoneiden lukumäärä sekä tutkitaan muiden tehoa kuluttavien laitteiden virrankulutusta eri toimintamoodeissa. Lisäksi selvitetään erilaisia energiantuotantovaihtoehtoja, kuten polttokennoratkaisut sekä ulkoisen energian käyttö (MOBI projektisuunnitelma 2010, 10).

TP 4: Tietoliikenne

Viranomais- ja hälytysajoneuvoissa tarvittavat yhteydet voidaan jakaa pitkän matkan yhteyksiin (esimerkiksi TETRA, @450, 2G, 3G, 4G, FM, GPS, WiMAX), lähiverkkoyhteyksiin (CAN, LAN, ja WLAN sekä ad-hoc –yhteydet ajoneuvojen välille) ja lisälaiteyhteyksiin, näissä kategorioissa vielä skaalaus pienestä isoon (esimerkiksi mahdolliset yhteydet miehittämättömiin lennokkeihin). Tietoliikenneratkaisun on oltava varmatoiminen sekä helposti asennettava. Tietoturvallisuuteen on kiinnitettävä erityistä huomiota. Eri järjestelmien erilaiset salaustekniikat asettavat projektille ja tietoturvallisuusratkaisulle omat haasteensa. Lisäksi eri toimijoilla on omat vaatimuksensa tietoturvallisuuden järjestämiselle ajoneuvojensa järjestelmissä.

Tässä työpaketissa tutkitaan dataväylälle asetettavia vaatimuksia ja suunnitellaan on-line -järjestelmien perus- ja varayhteydet sekä off-line -järjestelmien synkronoinneissa käytettävät

yhteydet. Lisäksi tutkitaan erilaisia antenniratkaisuja ja näiden kaapelointeja huomioiden sijoittelun ja alttiuden häiriöille sekä mahdollisuuden yhteiseen kaapelointiin.

Tämän työpaketin tavoitteena on kuvata hälytysajoneuvon tietoliikennearkkitehtuuri sekä tehdään rajapintamäärittelyjä. Tietoliikennearkkitehtuurin kuvauksesta on tavoitteena käydä ilmi, mistä komponenteista ajoneuvon sisäinen (LAN/CAN + lisälaiteyhteydet) ja ulkoinen tietoliikennejärjestelmä koostuvat. Rajapintamäärittelyssä kuvataan sitä, miten tietojärjestelmä ja sovellutukset pystyy hyödyntämään tietoliikennekerrosta. Myös yrityshankkeena toteutettava prototyyppitoteutus on mahdollinen työpaketin tuotos (MOBI projektisuunnitelma 2010, 11).

TP 5: Järjestelmäintegraatio

Työpaketissa suunnitellaan hälytysajoneuvon IT-integraatio ja luodaan tyyppiajoneuvon tietojärjestelmäarkkitehtuurin kokonaiskuva sekä on- että off-line-tilanteissa. Tässä on huomioitava datan turvallisuus lokaalivarastoinnissa ja kiinnitettävä huomiota replikoitaviin turvaluokiteltaviin tietoihin. Ajoneuvon suunnittelussa on huomioitava myös turvallisuus (ajoneuvon turvalaitteiden toiminta), joka on yksi integraation tuomista tärkeistä parannuksista. Lähtötietoina käytetään TP2:n tuloksena saatuja järjestelmävaatimuksia, joista johdetaan arkkitehtuurin suunnittelu ja käyttöliittymäratkaisuiden (HMI) suunnitteluratkaisuiden tekeminen.

Työpaketin tavoitteena on arkkitehtuurin kuvaus, jossa on kuvattu sovellusarkkitehtuuri, tietoarkkitehtuuri, tekninen arkkitehtuuri ja sijoittelukaavio -tasoilla, mistä komponenteista järjestelmä koostuu ja miten se sijoitellaan sekä rajapintamäärittely, jossa on kuvattu sovellusten liitettävyys järjestelmään. Lisäksi selvitetään markkinoilla olevia valo-ohjausjärjestelmiä (MOBI projektisuunnitelma 2010, 12-13).

TP 6: Sovellukset

Työpaketissa tutkitaan erilaisia sovellutustarpeita, joita eri käyttäjäryhmillä on ja valitaan kunkin käyttäjäryhmän kannalta keskeisimmät sovellutukset työn alle (esimerkiksi poliisilta video ja tutka; pelastustoimesta savusukellus ja säiliön vesimäärän mittari; rajavartiolaitokselta rajatarkastus jne.) Työpaketin tavoitteena on viranomaisajoneuvojen keskeisimpien sovellusten toiminnallisuuden määrittely sekä suunnitelma näiden keskeisimpien sovellusten teknisestä suunnittelusta (MOBI projektisuunnitelma 2010, 14).

TP 7: Demo-ajoneuvon varustelu

Projektissa mukana olevat yritykset sekä loppukäyttäjäorganisaatiot pääsevät testaamaan valittuja ratkaisuja tutkimusympäristössä. Projektissa mukana olevien yritysten rakentama kokeiluajoneuvo toimii kokeiluympäristönä loppukäyttäjäorganisaatioiden edustajille. Eri toimijoiden yhteistyön tuotoksena tullaan toteuttamaan varusteltu demo-ajoneuvo. Lähtökohtana on yhden ajoneuvotyypin demoajoneuvon toteutus, ajoneuvoon ei tulisi sekoittaa poliisi- ja paloautoa keskenään muuten kuin niiltä osin kun eri ajoneuvotyyppeihin sisältyy yhteisiä vaatimuksia. Ajoneuvosta tehdään siis yhdelle viranomaiselle suunnattu.

Demo-ajoneuvolle pyritään suorittamaan kenttätestaus joko PoAMK:ssa tai Pelastusopistolla (MOBI projektisuunnitelma 2010, 15).

TP 8: Liiketoimintamallit

ICT-konseptin kehittäminen on huomattavan kallista, joten pääsy kansainvälisille markkinoille on suotavaa. Suomessa on hyvät mahdollisuudet kehittää ko. alaa, koska viranomaisten keskinäinen yhteistyö on kehittynyttä ja tehokasta. Yllä mainitut ongelmat ovat samanlaisia kaikissa maissa: mm. viranomaisajoneuvoihin joudutaan lisäämään IT -laitteita. Välttämätöntä standardoitumista alalla ei ole tapahtunut. Tarkoituksena on luoda alalle kansainvälinen standardi (alan de facto- ja/tai de jure), joka tehostaa ja helpottaa viranomaisten yhteistoimintaa. Tavoitteena on saada lopullinen tulos soveltumaan myös muiden toimijoiden kuin viranomaisten käyttöön. Esimerkiksi teollisuuden yrityksillä, yksityisellä turva-alalla ja fleet management -palveluissa saattaa olla tarvetta liikkuvan toimiston kaltaiselle ajoneuvoratkaisulle. Tällaiset tarpeet otetaan MOBI-projektissa myös huomioon erityisesti kaupallisia ratkaisuita kehitettäessä.

Liiketoimintamalleja käsittelevässä työpaketissa haetaan ratkaisua kysymykseen siitä, miten kehitettyä kokonaisratkaisua tai sen osaa voidaan markkinoida yhteensopivana kokonaisuutena. Työpaketissa selvitetään alan markkinoita ja volyymeja, kansainvälisen ja kansallisen sekä Public-Private-partnershipien sääntelyn suhdetta eri maissa. Yksi keskeisistä tehtävistä on seurata EU:n piirissä tapahtuvaa markkinoiden kehitystä alalla. Liiketoimintamalleista pyritään luomaan skenaarioita selvittämään, kenen kannattaa vastaa integrointityöstä ja edelleen laitehankinnoista ja ylläpidosta. Työpaketissa kehitetään ja dokumentoidaan suomalaista mallia pohjaksi RFQ-dokumenttien luomiselle. Työpaketissa seurataan myös EU:n piirissä tapahtuvaa kehitystä (mm. EUROSUR) ja markkinoiden sekä sääntelyn (mm. EU:n parlamentin käsittelyssä olevan ulkorajojen exit-entry-järjestelmän, joka luo henkilöiden identifikaatiolle uusia haasteita) kehitystä. Tässä mielessä seurataan

Center for Identification Research´in (CITeR) piirissä tapahtuvaa kehitystä, johon Laurea on liittynyt jäseneksi Arizonan yliopiston partnerina.

Työpaketti tuottaa käytettäväksi uusia liiketoimintamalleja turva-alalle, uusia konsepteja, liiketoimintasuunnitelman ja mahdollisesti FP7-hakemuksen. Käyttäjätarvemäärittely tehdään Suomessa ja markkinatutkimukset kansainvälisellä tasolla (MOBI projektisuunnitelma 2010, 16-17).

5.1.7 Vaatimusmäärittely

Vaatimusmäärittely sisältää dokumentin, jossa kuvataan mitä poliisi- ja pelastustyön käytössä olevilta ICT-järjestelmiltä odotetaan ja vaaditaan. Vaatimukset tullaan kartoittamaan ja tulokset esitetään vaatimusmäärittely-dokumentissa. Tämän dokumentin tarkoituksena on tunnistaa vaatimukset ja tehdä ICT-järjestelmän toiminallinen kuvaus. Vaatimukset jaetaan kahteen ryhmään: toiminnalliset ja ei-toiminnalliset vaatimukset. Vaatimukset kuvaavat järjestelmän toiminnot, tehtävät ja rajoitteet.

Toiminnalliset vaatimukset määrittävät turvallisuusviranomaisten asettamat odotukset järjestelmän toiminnoista ja käytöksestä. Siinä kuvataan kuinka se tulee toimimaan, kuinka se on yhteydessä muihin relevantteihin järjestelmiin, mitkä toimijat voivat järjestelmää hyödyntää sekä kuinka toimijat käyttävät sitä. Yleisesti toiminnalliset vaatimukset määrittävät mitä toimintoja järjestelmän tulee tukea.

Ei-toiminnalliset vaatimukset, ja mitkä tunnetaan myös laadullisina vaatimuksina määrittävät järjestelmän ominaisuudet sekä rajoitteet. Näitä laadullisia ominaisuuksia ovat järjestelmän käytettävyys, luotettavuus, tehokkuus ja tuettavuus. Tämän dokumentin tarkoituksena on taata, että projektin lopputulos vastaa käyttäjien odotuksia (Pohjonen 2002 ; Kruchten 2004 ; Haikala & Märijärvi 2004).

5.1.8 Keskustelu

Meneillään olevan Euroopan ulkorajojen valvontajärjestelmän suunnittelutyö ja Lisboan sopimuksen EU:n sisäisen turvallisuuden tehostaminen vauhdittaa tulevaa standardisointia (EUROSUR). Suomessa on valtakunnallinen TETRA-verkko, jota hyödyntävät useat viranomaisorganisaatiot, joten Suomessa vallitsee kokonaisvaltainen viranomaistahojen välinen toiminnan yhteentoimivuus. Suomi on todistetusti ollut mukana langattoman tietoliikennestandardien kehittämistyössä ja osoittan hyvin toimivaa sekä organisoitua yhteistyötä useamman viranomaistahon kesken.

MOBI-hankkeessaa kehitettävän prototyyppisen ympäristön tarkoituksena on aloittaa standardointiin liittyvä kehitystyö, jolla mahdollistettaisiin poliisi- ja pelastusviranomaisten käyttöön suunnattujen järjestelmien tehokas yhteentoimivuus siten, että tietoa voidaan jakaa erilaisten sovelluksien avulla sekä valtioiden sisällä että eri valtioiden kesken. Demoajoneuvon toteuttamisen tarkoituksena on tarjota esimerkiksi tutkijoille, järjestelmäsuunnittelijoille, tietoliikenneyhteyksistä vastaaville turvallisuuden toimijoille fokus tulevaa kehitystyötä ja standardisoitumista varten.

5.2 Väestön turvaamisen ja katastrofiavun ICT-järjestelmien integraatio: Palo- ja pelastushenkilöstön palvelut

Tämä luku esittelee 5.1-luvussa esitetyn konferenssipaperin pohjalta kirjoitetun lehtiartikkelin, joka on julkaistu 5/2011 tieteellisessä lehdessä nimeltään ”Journal Of Communications”.

Yleisen turvallisuuden ja hätäavun palvelut, kuten lainvalvonta, palotorjunta, lääketieteen hätäapu ja hätätilanteesta parantamisen palvelut tuovat arvoa yhteiskunnalle luomalla vakaan ja turvallisen ympäristön. Pelastushenkilöstön vastuulla oleva pelastus- ja suojelutyö ulottuu ihmisiin, ympäristöön ja omaisuuteen. Se käsittelee suuria määriä luonnon ja ihmisten aiheuttamia uhkia. Yksi tärkeimmistä tehtävistä on hoitaa hätätapauksia ja valvoa tilannetta maalla, merellä ja ilmassa. Tärkein työ tehdään kentällä, joten kaikki työkalut tulee vastata tarpeita. Kenttätyöskentelyssä ajoneuvot ja niiden erilaiset laitteet, järjestelmät ja palvelut ovat tärkeässä roolissa, joten työturvallisuus, tehokkuus ja ergonomia on otettava huomioon. Käytössä olevien ajoneuvojen sekä niihin asennetun laitteiston tulee olla vakaita ja turvallisia. Niiden tulee sopeutua vaihteleviin ja vaativiinkin olosuhteisiin (Hult, Rajamäki & Holmström 2011, 143-148).

Jyri Rajamäki ja Timo Villemson kuvaavat ongelman muodostumista, että ajoneuvoihin asennettujen laitteiden, sovelluksien ja niiden tarjoamien palveluiden määrä on kasvanut viime vuosikymmenien aikana. Kehitys on kasvattanut myös erilaisten käyttöliittymien määrää, joka taas aiheuttaa uusia ongelmia esimerkiksi sen suhteen, että ajoneuvojen turvatyynyillä on vähemmän tilaa täyttyä. Myös erilaisista teknisistä ongelmista liittyen kaapelointiin ja virrankulutukseen on raportoitu. Yksi ongelma on sovellettujen ratkaisujen kehno dokumentointi, koska alalla ei ole tapahtunut standardisoitumista. Tämä johtuu laitteiden toimittajien ja valmistajien monimuotoisuudesta. Laitetoimittajien monimuotoisuus lisäävät ongelmia järjestelmäintegraation tekemisessä ja laitteiden yhteentoimivuudessa kenttätyöskentelyssä eri yksiköiden, kuten hätä- ja komentokeskuksen välillä. Näiden ongelmien myötä on tarvetta uusille liiketoimintamalleille (Rajamäki & Villemson 2009, 44-53 ; Rajamäki & Villemson 2009, 83-90).

Varsinkin Turvallisuus- ja pelastusviranomaisten käytössä olevien sovellusten määrän kasvaminen on johtanut myös siihen, että tärkeää tietoa välitetään erilaisten tietoliikenneyhteyksien välityksellä yhä useammin. Langaton tiedonsiirto on erittäin tärkeässä roolissa ja se tukee viranomaisten kenttätyöskentelyä. Langattomalla tietoliikenneyhteydellä tarjotaan jatkuva yhteys kentän ja johtokeskuksen välille. Tilannekuvat ja toimintasuunnitelmat tulee jakaa kaikille operaatioon osallistuville viranomaisille (Baldini 2010).

Euroopassa on rakennettu ja otettu käyttöön omia erityisiä ja suojattuja verkkoja viranomaisten kriittisen viestintää varalle, että taataan pelastustehtävän suorittaminen tilanteesta riippumatta. Toiminnassa olevat verkot perustuvat useimmiten TETRA/TETRAPOL-standardiin. Suomessa poliisin- ja pelastusviranomaisten kriittiseen viestintää varten on rakennettu oma viranomaisverkko VIRVE, jonka kautta merkittävässä roolissa oleva puheviestintä mahdollistetaan. Näihin liitetyt tiedonsiirto kanavat ovat kuitenkin luonteeltaan kapeakaistaisia ja eivät vastaa tiedonsiirtoyhteydelle asetettuja vaatimuksia. Nykyäänkin sekä etenkin tulevaisuudessa nämä kapeakaistaiset langattomat yhteydet väestön turvaamisen ja katastrofiavun palveluiden tukemisessa on todellinen ongelma (Baldini 2010). Monet uusimmat applikaatiot vaativat laajakaistaisia yhteyksiä, joita tarjoavat useimmiten kaupalliset operaattorit. Tämän vuoksi, yksittäisiä erillisiä tietoliikennekanavia tarvitaan. Vakaa monikanavaisuuteen perustuva tietoliikennejärjestelmä, joka on riippumaton yksittäisestä operaattorista, esitetään työn kolmannessa julkaisun suomenkielisessä lyhennelmässä. Neljännessä julkaisun suomenkielisessä lyhennelmässä esitellään protokolla, joka mahdollistaa tämän järjestelmän.

EUROPOL ja FRONTEX ovat kiinnittäneet huomiota väestön turvaamisen ja katastrofiavun viranomaisten välisen yhteistoiminnallisuuteen liittyvät puutteet oikeassa toiminnassa. On tieteellisesti todistettu, että standardisoitumisella on vahva vaikutus sellaiseen liiketoimintaan, joka kehittää ja myy teknologiaa tai teknologia-pohjaisia tuotteita tai palveluita: standardit ovat yksi tärkein mahdollistaja nopealle kasvulle (Kivimäki 2007).

Tämän luvun toisessa kappaleessa esitellään kenttäympäristöä, varisinkin loppukäyttäjän näkökulmasta. Kolmannessa luvussa esitellään tutkimus-, kehitys- ja innovaatiohanke Mobile Object Bus Interaction (MOBI), joka koostuu kahdesta yritysprojektista sekä tutkimusprojektista. Neljännessä luvussa esitellään tutkimusprojekti yksityiskohtaisemmin. Julkaisun viidennessä luvussa SOAn soveltuvuutta ratkaisemaan integraation liittyvät asiat ja kuudennessa luvussa esitellään tulevan tutkimuksenn tarpeita.

5.2.1 Väestön turvaamisen ja katastrofiavun palveluiden ICT-järjestelmät

Järjestelmäintegraatiot ovat vallitseva trendi kaikenlaisessa liiketoiminnassa ja organisaatioissa (Litan & Mocanu, 2011, 250-256). Työskentelytapojen trendi menee kohti enemmän liikkuvuutta ja Internet on suuremmassa roolissa, kun hankitaan liiketoimintaan liittyvää tietoa, applikaatioita ja palveluita liikkuville käyttäjille. Palvelutason vaatimukset ovat tärkeässä roolissa. Siitä huolimatta palvelutason vaatimuksia on vaikea määrittää. Seuraavia toiminnallisia rajoitteita voidaan käyttää lähtökohtina: 1) käytettävyys, 2) tehokkuus, 3) skaalautuvuus 4) luotettavuus, 5) saatavuus, 6) laajennettavuus, 7) huollettavuus, 8) hallittavuus, 9) rehellisyys ja turvallisuus. Nämä ominaisuudet voidaan määritellä vasta todellisen käyttöönoton jälkeen. Jotta tarkoituksenmukaiset vaatimukset saavutetaan, järjestelmää tulee muuttaa ja virittää; ja jos se ei ole mahdollista, palvelutason vaatimukset tulee muodostaa uudelleen toimintaympäristön mukaisesti. Kaikkien olemassa olevien web-järjestelmien tarkoituksena on tukea liiketoimintaa ja organisaation tarpeita (Tumin & Encheva 2011).

5.2.2 Loppukäyttäjän näkökulma

Väestön turvaamisen ja katastrofiavun toiminta on yhä enenevissä määrin riippuvaisempi ICT-järjestelmistä ja etenkin niiden langattomista tietoliikenneyhteyksistä. Tiedonsiirto on kriittisessä asemassa ja useamman tai yhden langattoman tietoliikenneyhteyden kautta kulkeva tiedonsiirto tulee olla turvallista ja luotettavaa.

Poliisi- ja pelastusviranomaisten tietojärjestelmien kehittämisen yhtenä päämääränä on standardisoida tietoliikennejärjestelmien liitettävien sovellusten arkkitehtuuri ja infrastruktuuri. Käytettävyys on yksi tärkein kriteeri, sillä monet ratkaisut ovat epäergonomisia tai ei helposti mukautettavissa nykyisiin ajoneuvojen infrastruktuuriin. Seuraavia Baldinin esittämiä vaatimukset tulisi huomioida:

- Inter-System Interface (ISI) on avoimen rajapinnan standardi mitä käytetään yhdistämään kaksi TETRA-verkkoa yhteen. Yhteinen kehitystyö pitäisi aloittaa.
- Yhdenmukaiset tietoliikennepalvelut PPDR-viranomaisille tulisi selvittää ja tunnistaa.
- TETRA Enhanded Data Servicestä (TEDS) pitäisi toteutettavuustutkimus, jotta voitaisiin vahvistaa vastaavatko ne Euroopan PPDR-viranomaisten vaatimuksia.
- PPDR-viranomaisten käytössä olevat tietoverkkojen laajakaistapalvelut tulee standardisoida ja yhdenmukaistaa (Baldini 2010).

5.2.3 Suomen väestön turvaamisen ja katastrofiavun viranomaiset

Suomen poliisiorganisaatio koostuu 24 alueellisesta poliisilaitoksesta mukaan lukien KRP sekä liikkuvan poliisin yksikkö. Nykyaikaiset hälytysajoneuvot sisältävät enemmän tietoliikennejärjestelmiä kuin koskaan. Hälytysajoneuvoista on tehty liikkuvia toimistoja, joissa suoritetaan erilaisia asiakaskontakteihin liittyviä tehtäviä ja yleisen järjestyksen valvontaa. Hälytysajoneuvoihin on kytketty erilaisten järjestelmien lisäksi tehtävien suorittamista varten tarvittava alaitteistoa.

Suomi on jaettu 22 alueelliseen pelastusyksikköön, joista jokainen alue on vastuussa alueensa turvallisuudesta ja pelastuspalveluista. Suurimmissa kaupungeissa ja kunnissa pelastusammattilaiset kantavat vastuun palo- ja pelastustehtävissä, kun taas pienimmillä paikkakunnilla palo-ja pelastustoimen tehtäviä hoitaa vapaaehtoinen palokunta. Pelastustehtävien hallintaa varten tarvittavien tietojärjestelmien määrä on kasvanut ja kenttätehtävien hoitamista varten on olemassa useita erilaisia järjestelmiä.

Suomen hälytystehtäväpalvelut (Emergency Medical Services) on ulkoistettu yksityisille yrityksille 200 kunnassa. Tehtävään liittyvä potilaan tutkimus, hoito ja elintoimintojen ylläpitäminen aloitetaan jo kentällä käsin, jotta potilaan kunto ei heikkenisi kuljetuksen aikana. Potilaan hoidon aloittaminen jo kentällä asettaa omat vaatimuksensa EMS-ajoneuvoihin. Tietotekniikka korvaa perinteisen paperityön ja näin ollen teknologian hyödyntämistä on lisätty myös muissa prosesseissa.

5.2.4 Palvelut palo- ja pelastushenkilöstölle

Seuraavissa luvuissa tehdään alustavaa esitutkimusta pelastusajoneuvojen ohjelmistoarkkitehtuurin muuttamisesta palvelupohjaiseen arkkitehtuuriin (Service Oriented Architecture, SOA) ja Web-sovelluspalveluihin. Ajatuksena on kartoittaa voidaanko SOA:lla ja Web-sovelluspalveluiden avulla tukea hälytysajoneuvojen tieto- ja viestintärjestelmien integraatiota, yhteentoimivuutta ja uudelleenkäytettävyyttä. Tutkimuksessa saatujen tietojen avulla pyritään tekemään ratkaisu tukeeko SOA-ajatusmalli hälytysajoneuvojen ohjelmistosovelluksien toimintaan liittyviä vaatimuksia täydentävästi.

5.2.5 Palo- ja pelastustyön palvelut sekä tieto- ja viestintäjärjestelmät

Hälytysajoneuvojen, kuten esimerkiksi ambulanssien, palo- ja pelastusautojen palvelut edustavat hajautettua järjestelmää. Tämä siksi, että Suomen hätäpalvelut hallinnoidaan ja säännöstellään alueittain ja paikallisesti. Hätätilanteen sattuessa hälytysajoneuvojen tieto- ja viestintäjärjestelmät ovat ratkaisevassa roolissa. Kentällä olevat ajoneuvoissa tulee olla

tietoliikenneyhteydet päällä, että voidaan olla yhteydessä esimerkiksi komentokeskukseen katkoksitta. Mykkäsen, Korpelan ja Ripatin mukaan ohjelmistokehityksen paradigmat eivät anna riittävää tukea standardisoinnille, integroinnille ja hajautettujen järjestelmien yhteentoimivuudelle. Hätätilanteen sattuessa reaaliaikainen tieto, joka kulkee keskenään vuorovaikutuksissa olevien järjestelmien välillä, on kriittisessä roolissa ja SOAn on ajateltu olevan ratkaiseva tekijä tähän (Mykkänen, Korpela & Ripatti 2007, 470-475).

Harkittaessa siirtymistä kohti SOA-ratkaisua, tulee nykyiset palo- ja pelastushenkilöstön palvelut ja toiminnalliset vaatimukset kartoittaa, sillä SOAn avulla pyritään yhdenmukaistamaan liiketoimintaa teknologian avulla. Edessä on kuitenkin suuria ja olennaisia kysymyksiä, jotka antavat suuntaa tutkimukselle. Koska tutkimustyö on vasta esitutkimusvaiheessa, niin joihinkin kysymyksiin vastataan vasta myöhemmässä vaiheessa tulevien tutkimuksien omissa julkaisuissa. Kysymyksiä tällä hetkellä ovat:

- Voidaanko SOA-ajatusmalli ottaa käyttöön, kun kehitetään pelastus- ja turvallisuuviranomaisten ICT-järjestelmiä tai mitä tahansa kohtaa heidän järjestelmässä?
- Jos kyllä, niin missä määrin tämä arkkitehtuuri tukee standardisointia, integrointia, yhteentoimivuutta, uudelleenkäytettävyyttä ja laajennettavuutta tulevaisuuden palveluita ajatellen? Kuinka SOA antaa tukea Web-sovelluspalveluiden välityksellä ja tarjoaa palveluita hälytysajoneuvoille ja henkilöstölle?
- Jos ei, niin minkälaista ratkaisua voisimme hallita?

Erään pelastuslaitoksen työntekijän mukaan pelastustehtävän ketju alkaa hätäkeskukseen soitetusta puhelusta. Tässä kuvatussa tilanteessa esitetyt asiat pitävät paikkansa kyseisessä pelastuslaitoksessa, sillä esimerkiksi kenttäjohtojärjestelmät (PeKe tai Merlot) ovat erilaisia eri pelastuslaitoksissa. Hätäkeskus vastaanottaa puhelun, käsittelee sen ja välittää tiedon eteenpäin jollekin pelastusyksikölle. Yksikkö voi olla palolaitoksen yksikkö, ambulanssi tai ensihoidon yksikkö tai poliisiyksikkö. Puhelut priorisoidaan tilanteen vakavuuden mukaisesti. Hätäkeskus tekee useimmiten päätöksen, kuinka monta yksikköä lähetetään onnettomuuspaikalle. Koska tehtävä on toimitettu eteenpäin jollekin yksikölle tai osastolle, niin pelastustehtävän ketju ei hajoa. Liikkeellä olevat yksiköt ja hätäkeskus on yhteydessä toisiinsa. Yksiköt voivat siis siirtyä tehtäväpaikalle ja vastaanottaa samanaikaisesti tietoa tästä tehtävästä. On mahdollista, että pelastustehtävä vaatii palo- ja pelastuslaitoksen palveluiden lisäksi paikalle myös ensihoidon palveluita eli ambulanssin. Tämä tarkoittaa sitä, että kaikki pelastustehtävään liittyvät yksiköt raportoivat komentokeskukseen ja jakavat tilannetietoa tapahtumista.

Edellä mainitut asiat määrittelevät prosessin ja tiedonkulun, kun hätäkeskus vastaanottaa hätäpuhelun. Hätäkeskus voi vastaanottaa uutta tietoa ilmoittajalta ja välittää nämä tiedot

eteenpäin yksiköille, jotka ovat liikenteessä. Aiemmat tiedot päivitetään ajantasalle aina tuoreilla tiedoilla. Samanaikaisesti pelastusyksiköt voivat seurata tilannetta usean käyttöliittymän kautta ajoneuvoihin asennettujen tietokoneiden kautta. Näiden laitteiden avulla saadaan ärkeää tietoa, jota tarvitaan tehtävän suorittamista varten.

Jokaiselle hätäkeskukseen tehdylle ilmoitukselle annetaan koodi, joka kertoo tapauksen vakavuudesta ja luonteesta. Tämän ilmoituskoodin vastaanottaa ensimmäinen vastuussa oleva johtoyksikkö. Hän pystyy arvioimaan, kuinka monta pelastusyksikköä tullaan ottamaan käyttöön. Ajoneuvoihin asennettuihin tietokoneisiin on asennettu sovellus nimeltään ”Merlot Mobile 4.1”, joka on Logican tarjoama tuote. Tämän sovelluksen avulla kenttähenkilöstö vastaanottaa ajantasaista tietoa tapahtumapaikalta. Ambulanssien ja pelastushelikopterien käytössä on laajennettu versio tästä, mikä sisältää pääsyn myös mahdollisen potilaan henkilötietoihin ja sairaushistoriaan. Tähän järjestelmään pääsy on rajoitettu vain lääkärille tai ennalta nimetyille henkilöille.
Ajoittain tehtävän luonne tai laatu muuttuu kesken, jolloin kenttäjohtaja joutuu tekemään muutoksia suunnitelmiin ja järjestelmän avulla tiedot päivitetään kaikille ajantasalle. Komentokeskuksella on mahdollisuus seurata kentällä tapahtuvaa reaaliaikaisesti. Kun palotorjunnan yksikkö saapuu onnettomuuspaikalle, kenttäyksikön tulee ensimmäiseksi selata läpi piirustukset rakennuksista ja tapahtuma-alueesta. Yksi ongelmista onkin piirustuksien laatu, sillä ne ovat paperisena versiona ja jotkut ovat kärsineet kulumista repeämistä ajan myötä. Näillä pienillä yksityiskohdilla on suuri merkitys siihen, kuinka nopeasti tulipalo saadaan sammutettua. Tämä manuaalinen prosessi on yksi asia, johon tarvittaisiin parannusta.

Pelastushenkilöstöllä on käytössään VIRVE-laitteet, jota he voivat hyödyntää laaja-alaisissakin operaatioissa. VIRVE-viranomaisradioverkko on armeijan, poliisin, palo- ja pelastuslaitoksen, pelastushelikoptereiden ja muiden yleistä turvallisuutta harjoittavien toimijoiden ammattikäyttöön rakennettu yksityinen radioverkko. Se sisältää myös toiminnon, joka ilmoittaa varoitusviestillä hätäkeskukselle, jos se havaitsee tulta tai savua.

5.2.6 Palo-, pelastus- ja hätäpalveluihin liittyvät ICT-haasteet

Kuten onkin jo kerrottu, niin pelastus- ja turvallisuuspalveluita tarjoavat eri alan viranomaiset, kuten poliisi, palo- ja pelastusyksikkö, ensihoito jne. Se myös tiedetään, että jokaisella viranomaisella on käytössään omat tieto- ja viestintäjärjestelmät, jotka mahdollistavat heidän toimintansa kentällä. Hätätilanteessa kenttähenkilöstö hyödyntää ajoneuvoihin asennettuja järjestelmiä sekä laitteistoa ja ratkaisee tehtävät yhteistyössä muiden viranomaistahojen kanssa. Tietojärjestelmien integroinnilla tehostetaan reaaliaikaisesti tapahtuvaa tietojen vaihtamista sekä jakamista ja tarjoataan yhteinen alusta

Web-sovelluspalveluiden jakamiseen. Näitä palveluita voi hyödyntää kaikki tehtävään osallistuvat viranomaistahot.

Palo- ja pelastustoimen palvelut toimivat muun muassa Merlot tuoteperheeseen kuuluvan Merlot Mobile-kenttäjohtojärjestelmän avulla. Tämä kenttäjohtojärjestelmä mahdollistaa tehokkaan tilanneseurannan. Yksi tärkeä elementti, jota tämä järjestelmä ei tue on digitaalisessa muodossa saatavat blueprintit eli piirustukset rakennuksista. Tämä puuttellisuus konkretisoituu, kun kenttähenkilöstö joutuu kartoittamaan onnettomuuspaikan rakennukset vasta paikanpäällä selailemalla blueprint-käsikirjoja. Jos nämä rakennuspiirustukset löytyisivät suoraan ajoneuvoihin asennetun järjestelmän avulla, niin onnettomuuspaikka voitaisiin kartoittaa jo ennen paikalle saapumista suoraan ajoneuvosta käsin.

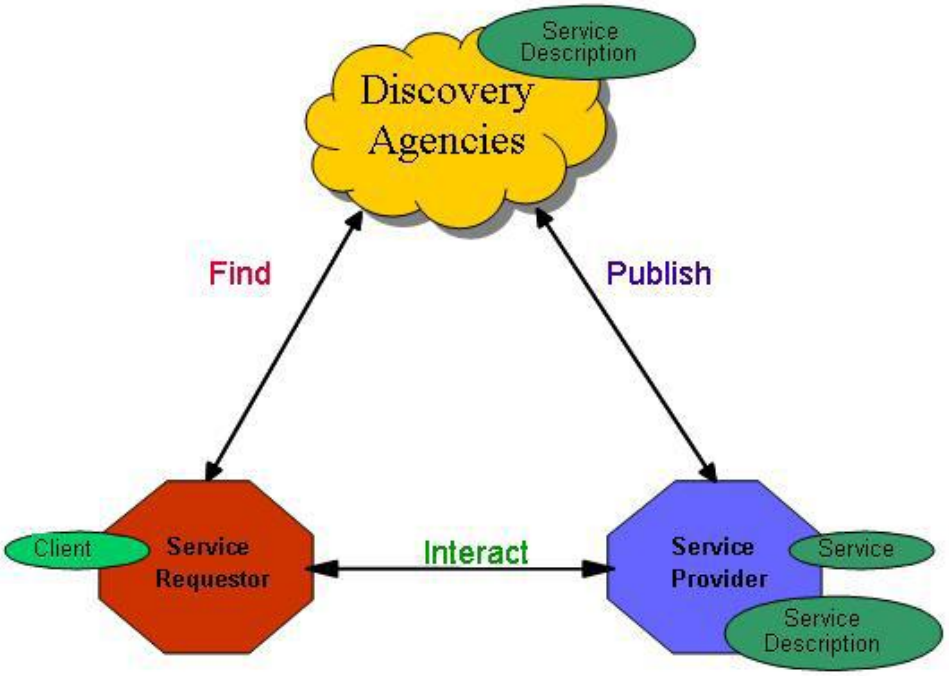
Pelastus- ja turvallisuuspalvelut, kuten ensihoidon palvelut ovat kallistumassa kohti SOA-ratkaisun omaksumista, minkä avulla mahdollistetaan tälläkin hetjekkä esimerkiksi terveyspalveluiden laadukas ja tehokas toiminta. Suomen hallitus onkin omaksunut SOA:n jo osaksi valtakunnallista terveydenhuoltoa ja suunnittelee sen ottamista käyttöön myös muissa terveydenhuollon aloilla. Potentiaalia olisi myös rakentaa yksityinen tai julkinen palvelurekisteri erilaisten Web-sovelluspalveluiden jakamiseen kaikkien pelastus- ja turvallisuustoimijoiden keskuudessa. Yhtenäiset Web-sovelluspalvelut kriisitilanteiden ratkaisemiseen on mahdollista monistaa myös muihin EU-maihin, jotka haluavat harjoittaa pelastus- ja turvallisuustoimintaa samanlaisella mallilla.

5.2.7 SOA:n ja WEB-sovelluspalveuiden rooli palo- ja pelastustoiminnassa?

Jotta voimme vastata luvun otsikossa esitettyyn kysymykseen, tulee meidän aluksi esitellä palvelupohjainen arkkitehtuuri ja Web-sovelluspalvelut.

SOA on arkkitehtuuritason paradigma, jolle ominaisinta on edistää kytkentöjen joustavuutta, kun suunnitellaan ja toteutetaan tietojärjestelmiä. World Wide Web Consortiumin (W3C) mukaan SOA on joukko erilaisia komponentteja, jotka mahdollistavat sovellustoiminnallisuuksien tarjoamisen ja pyytämisen joukkona jaettuja liiketoimintalähtöisiä sovelluspalveluita. SOA paradigma tarjoaa ympäristön joustavalle kytkennälle, yhteentoimivuudelle ja standardeihin perustuvaan tietojenkäsittelyyn. SOA on myös tapa suunnitella uusia sovelluksia, jotka sisältävät jo olemassa olevien järjestelmien vanhoja palveluita. Se tarjoaa valmiin ratkaisun voittaa haasteita, mitä sellaiset organisaatiot kohtaavat, joiden pyrkimyksenä on saavuttaa tehokas ja suorituskykyinen vuorovaikutus. Kytkentöjen joustavuus on SOAn keskeinen ominaisuus ja se mahdollistaa yhteentoimivan ja tehokkaan tietojärjestelmien suunnittelu- ja hallitsemistavan. Kuvassa 2 esitetään näiden kolmen tärkeän komponentin välinen yhteistyö (Neubaue 2007, 101-107; Guidi, Lucchi &

Mazzara 2007, 55-70; Ardissono, Petrone & Segnan 2004 , 693-709; Bieberstein, Bose & Fiammante 2006, 215).



Kuva 2: Palvelupohjainen arkkitehtuuri

Web-sovelluspalvelut ovat täysin riippumattomia mistään ohjelmointikielestä, laitteistosta tai käyttöjärjestelmästä ja siten mahdollistetaan palvelujen löyhä kytkös. Web-sovelluspalvelun malli on yksinkertainen: palveluntarjoaja tarjoaa palvelun, jota kuluttaja etsii ja pyytää. Web-sovelluspalveluita kuvataan yleensä perheenä, joka sisältää määritelmät, protokollat ja standardit. Näiden avulla sovellukset voivat olla vuorovaikutuksessa, tehdä yhteistyötä ja vaihtaa tietoja keskenään turvatusti, luotettavasti ja yhteentoimivasti. SOAP ja REST ovat tällä hetkellä vallitsevat ajatusmallit, joita käytetään useimmiten Web-sovelluspalveluiden toteuttamiseen.

W3C:n (Ferris & Newcomer 2002) mukaan ”Web-sovelluspalvelu on URIn yksilöimä ohjelmistosovellus, jonka rajapinnat on mahdollista määritellä, kuvata ja löytää. Web-sovelluspalvelu tukee suoraa vuorovaikutusta muiden sovelluksien kanssa, käyttämällä XML-pohjaista viestinnän vaihtoa muiden Internet-protokollien välityksellä”. Web-sovelluspalveluiden kuvataan perheenä erilaisia teknologioita, jotka sisältävät vaatimukset, protokollat ja teollisuus-pohjaiset standardit, joita voi heterogeeniset sovellukset hyödyntää vuorovaikuuttakseen, tehdäkseen työsä yhdessä ja jakaakseen informaatiota turvallisella, luotettavalla ja yhteentoimivalla tavalla(Ferris & Newcomer 2002). SOAP ja REST ovat tämänhetkiset vallitsevat ajatusmallit, joita voidaan hyödyntää Web-sovelluspalveluiden toteuttamiseen.

Web-sovelluspalveluiden teknologia perustuu avoimen lähdekoodin teknologioihin, mitkä sisältävät: eXtensible Markup Language (XML), Simple Object Access Protocol (SOAP), REST, Universal Description, Discovery ja Integration (UDDI) sekä Web Services Description Language (WSL). Kuten aiemmin jo mainittiin, niin avoimen lähdekoodin standardit mahdollistavat useamman eri valmistajien sovelluksien yhteentoimivuuden. Suurin SOA:ssa on integroinnin ja muutoksiin mukautumisen helppous. Tässä tutkimuksessa käsiteltyjen SOA:n ja web-sovelluspalveluiden yleiskuvaus vahvistaa, että siitä voi olla merkityksellistä hyötyä.

5.2.8 SOA-standardit

Palvelupohjaisen arkkitehtuuriin menestyksen takana on kahdeksan suunnitteluperiaatetta, jotka ratkaisevat monta standardisoitumiseen, integraatioon ja toiminnallisuuteen liittyviä kysymyksiä. Seuraavaksi esitellään nämä kahdeksan suunnitteluperiaatetta, jotka ovat Erlin (2009) mukaan seuraavat:

1) Standardisoidun palvelusopimuksen periaate

Tässä periaatteessa selvitetään noudattaako palvelun yleiskuvaus suunnittelustandardeja. Niiden osapuolien tulee ymmärtää yleiskuvaus palvelun valmiuksista, mitkä tulevat käyttämään palvelua. Näiden palveluiden ominaisuudet tulee noudattaa palvelusopimuksia, jotka tässä tapauksessa ovat suunnittelustandardeja. Palvelusopimus useimmiten kuljettaa informaatiota, jota voidaan käyttää määritellessä minkä tahansa palvelun sanallinen kuvaus, UL, nimi jne. Sillä on tämän lisäksi myös toiminnallisia ominaisuuksia, kuten I/O parametrit, vuorovaikutusmalli, mutta lisäksi ei toiminnallisia ominaisuuksia, jotka sisältävät QoS, palvelun sijainnin ja turvallisuusrajoitukset.

Standardisoinnin säännöstely mahdollistaa palveluiden yhteentoimivuuden, joka lisää palvelun käyttäytymisen ennustettavuutta. Palvelun käyttäytymisen ennustaminen on tärkeä mekanismi, jonka avulla saavutetaan skaalatutuvuus mikä johtuu siitä, että se tekee tilaa tärkeiden laskentaresurssien arvioinnille, jota tarvitaan todentamaan kohdennettuja palvelua. Tämä keskeinen mekanismi helpottaa älykkään resurssien provisionnin, ehkäisemään ohjelmistoresurssien väheneminen.

2) Löyhän kytkennän periaate

Tämän periaatteen mukaan käyttöliittymän palvelun tulisi asettaa alhainen kytkennän kulutus. Kaynen mukaan (2003) löyhän kytkennän tarkoituksena on vähentää palvelurajapintojen välinen riippumattomuus ja näin saavutetaan järjestelmien välinen

joustavuus ja yhteentoimivuus. Tämä periaate mahdollistaa löyhä kytkennäisten sovelluksien kehittämisen, jotka ovat uudelleenkäytettäviä ja sopeutuvat paremmin muuttuviin vaatimuksiin. Tiiviisti kytketyt järjestelmät eivät ole ominaisuuksiltaan yhtä skaalattavia kuin löyhästi kytketyt (Eugster, 2002). Tila-pohjaisten järjestelmien on todistettu olevan myös skaalattavampia kuin tiukasti kytkettyjen järjestelmien (Krummenacher 2007).

3) Palvelun abstrahoinnin periaate:

Tämä periaate piilottaa olioparadigman tavoin mahdollisimman paljon taustalla olevia tarkkoja ohjelmiston yksityiskohtia. Jotkut kirjoittavat kutsuvat tätä ”black boxing”-periaatteeksi joka on synonyymi vanhalle ”black boxing” ohjelmistotuotanto-konseptille. Tämä periaate edistää vaihdettavuutta.

4) Uudelleenkäytettävyyden periaate

Tämä periaate on vahva osa palvelupohjaisuutta tarkoituksenaan ei-omisteinen toiminnallinen uudelleenkäytettävyys. Palveluteknologia mahdollistaa SOA infrastruktuurin ja sillä on kyky luoda valtavia toimiala-riippumattomia erilaisia palveluita sisältäviä kirjastoja.

5) Itsehallinnan periaate

Tämä periaate konkretisoi sitä, että palveluihin liitetyt prosessit tulee suorittaa siten, että ne ovat riippumattomia kaikista ulkopuolisista vaikutteista, jotta ne voisivat toteuttaa kyvykkyytensä tasaisesti ja luotettavasti.

6) Tilattomuuden periaate

Tämä periaate määrittelee sen miten palveluiden tulisi minimoida resurssien kulutuksen tilan suhteen.

7) Löydettävyyden periaate

Tämä periaate, joka liittyy läheisesti standardisoituun palvelusopimukseen, esittää sen, että palveluiden metatiedot tulee merkitä. Näin ollen kaikki osapuolet, jotka voisivat olla niistä kiinnostuneita, löytäisivät nämä palvelut. Hälytysajoneuvot ja ohjauskeskukset pystyvät löytämään nämä palvelut ja käyttämään niitä vuorokauden ympäri, koska niitä tarjotaan verkossa.

8) Koostettavuuden periaate

Tämä periaate määrittelee sen, että palvelut tulee olla hyvin koostettavia, sillä kasvavat ja kehittyvät SOA-toteutukset vaativat yhä kompleksisempaa palvelukoosteiden muodostumista.

5.2.9 Web-sovelluspalveluiden standardit

Tässä osiossa keskitytään kahteen vallitsevaan web-sovelluspalveluiden toteuttamiseen tarkoitettuun standardiin(SOAP ja REST). Myös muita standardeja olisi tarpeen tutkia, mitkä mahdollistaisivat SOA:n toteuttamisen. Nämä kaksi standardia ovat kuitenkin vallitsevia standardeja ja ovat herättäneet paljon keskustelua siitä, että kumpi niistä tulisi valita.

1) SOAP

SOAP on Web-sovelluspalvelu-standardi, joka tukee kahden Web-sovelluspalvelun välistä vuorovaikutusta. SOAPin on kehittänyt Microsoft, mitä sen jälkeen edelleen kehitettiin yhdessä UserLandin, Lotuksen, IBM:n ja Developmentorin kesken. SOAP on tyypillinen XML-pohjainen määritelmä, jota voidaan käyttää viestintään ja proseduurien etäkutsuun. SOAPia käytetään olemassa olevien siirtoprotokollien, kuten HTTP:n, SMTP:n ja MQSeriesin yli.

SOAP-standardi määrittelee viestintämallin, joka vahvistaa kuinka viestien vastaanottajien tulee käsitellä SOAPin kautta lähetetty viesti. Määritelmä määrää toimijat, jotka saavat käsitellä sanomaa.

Curberan, Duftlerin & Khalafin (2002) mukaan WWW on luonteeltaan jaettu ja heterogeeninen, sovellukset tulee olla alustasta riippumattomia, kansainvälisiä, turvattuja ja niin kevyitä kuin mahdollista. Jotta nämä asiat voidaan saavuttaa, niin esiin astuu XML. XML on koneellisesti luettavaa merkintäkieltä, joka tukee tietojen koodausta sellaisella tavalla, joka osoittaa järjestelmille itsenäisyyttä. He täsmentävät, että XML:ään perustuvat tiedonsiirtoprotokollat ovat pääosin vastaus web-sovelluspalveluiden toteuttamiseen. XML tarjoaa yhtenäisen representaation tiedolle, joka mahdollistaa tiedon vaihtamisen erilaisien järjestelmien välillä. XML-pohjainen SOAP-protokolla toimii HTTP:n välityksellä js pitää lupaukset liittyen web-sovelluspalveluiden toteuttamiseen.

2) REST

REST tulee sanoista Representational State Transfer. Kalifornian yliopistosta Roy Fielding loi tämän akronyymin ja esitteli RESTin vuonna 2000 väitöskirjassaan. Vaikka REST ei

konseptina alkuun ottanut tuulta purjeisiinsa, niin nykypäivänä se on saavuttanut valtavasti hyväksyntää kaikkialla verkkomaailmassa. Muutaman viime vuoden aikana REST on saanut maailmanlaajuista hyväksyntää ja on käynnistänyt jatkuvaa keskustelua näistä kahdesta johtavasta SOAn toteutuksiin käytettävistä ajattelutavoista. Jotkin tämän tutkimuksen näkökulmat voitaisiin saada käynnissä olevaan keskustelun avulla sekä erilaisten alan asiantuntijoille esitettujen kyselyiden ja haastatteluiden perustella. Saadun palautteen avulla voitaisiin helpottaa raportointia päättäjille siitä, kumpi paradigma kannattaisi valita siirryttäessä SOA infrastruktuuriin.

RESTin päämääränä on:

- Komponenttien tai resurssien vuorovaikutuksen skaalattavuus
- Yhdenmukaisten rajapintojen saavuttaminen
- Riippumattomuus resurssien kohdentamiseen
- Komponenttien välisen vuorovaikutuksen viiveen vähentäminen, turvallisuuden parantaminen sekä vanhojen järjestelmien kapselointi.

Seuraavaksi käydään läpi, kuinka nämä päämäärät saavutetaan Fieldingin (2000) mukaan. Seuraavat keskeiset rajoitteet ja arkkitehtuuriset periaatteet muodostavat REST-ajatusmallin ja mahdollistavat edellä mainittujen tavoitteiden saavuttamisen (Fielding 2000).

a) REST-palveluiden tilattomuus

Fielding (2009) on sitä mieltä, että tässä periaatteessa yksittäiset pyynnöt, jotka kantautuvat mistä tahansa asiakassovelluksesta mihin tahansa ennalta määritettyyn palvelimeen tulee sisältää kaikki elintärkeä tieto, mikä on tarpeellista ymmärtääkseen asiakkaan tarpeen. Pyyntö ei saa kuitenkaan riippua mistään sellaisesta tiedosta, joka sijaitsee tai on tallennettu palvelimelle. Asiakkailla tulee olla mahdollisuus suorittaa pyynnöt onnistuneesti riippumattomasti palvelimen tilasta, joka on tallennettu palvelimelle.

Koska tämä periaate ei edellytä Web-sovelluspalvelua asiakasta hyödyntämään tilaa, joka olisi tallennettu palvelimelle suoriutuakseen pyynnöstä, joten asiakkaalta odotetaan kaiken tiedon toimittaminen (kuten tila, parametrit ja muita sellaista dataa), mitä palvelimet tarvitsevat tuottaakseen ja vastatakseen kysymykseen. Tämä tärkeä informaatio tulee sijoittaa asiakkaan pyynnön HTTP:n ylätunnisteeseen ja ohjelmakoodiin. Tämä periaate on tunnustettu olevan hyvin hyödyllinen, koska se lisää Web-sovelluspalveluiden tehokkuutta. Sen lisäksi palvelimella sijaitsevien komponentit on suunniteltu ja toteutettu yksinkertaiseksi, koska se asia tiedostetaan, että palvelimen tilan olemassa olemattomuus tarkoittaa, että istunnon tietoja ei tarvitse synkronoida sovelluksien ulkopuolella.

b) REST-palveluiden yhtenäinen rajapinta

Tämä periaate edellyttää, että REST-palvelun on nimenomaisesti mahdollista käyttää HTTP-toimintoja, jotka määritellään RFC:n 2616-protokollassa. Nämä HTTP-toiminnot tai menetelmät, joka sisältävät ”GET”, ”POST”, ”PUT” ja ”DELETE” tulee olla ainoat menetelmät, jotka mahdollistetaan HTTP-protokollassa. Niitä tulee käyttää juuri niin tarkasti kuin ne on alun perin tarkoitettu käytettävän.

Tämä periaate tulee jäljessä, sillä samoja HTTP-menetelmiä on törkeästi käytetty myös tapauksissa, mihin niitä ei ole alun perin tarkoitettu. Esimerkiksi ”GET”-menetelmä on erityisesti tarpeen silloin, kun asiakkaat hakevat tietoa palvelimelta, mutta sitä on myös väärinkäytetty kehittäjien toimesta suorittaakseen kyselyitä ja kauko proseduurikutsuja. Tämä kuitenkin tuo esiin suunnittelupuutteita, jotka rajoittavat yhdenmukaisten rajapintojen saavuttamisen kaikille REST-palveluiden asiakkaille. On hyödyllistä sisällyttää tämä suunnitteluperiaate mihin tahansa REST-palveluiden toteuttamiseen. (Fielding 2000)

c) Resurssit ja niiden tunnistaminen

Fieldingin mukaan, tiedot resursseista ovat REST-ajatusmallissa tärkeimmässä roolissa. Hän täsmentää, että tietyt tiedot, jotka voidaan nimetä, voisivat edustaa resursseja. Resurssi voi siksi olla dokumentti, kuva, kokoelma resursseja ja muita asioita, joita voidaan verrata resursseiksi. Tämä pitää sisällään sen, että koko REST-arkkitetehtuuri pyörii resurssikonseptin ympärillä. Seuraava huomioitava konsepti on URI. Mikä tahansa resurssi, joka voidaan nimetä, tulee sisältää oman URIn, mikä yksilöllisesti tunnistaa sen. Tämä on toinen RESTin keskenäisistä rooleista. (Fielding 2000)

Kuten Rodriquez (2008) kuvaa, REST-palvelun asiakassovellukset käyttävät resurssejja URIn kautta. URI helpottaa Web-sovelluspalveluiden intuitiivisuutta, kun ne ovat hyvin määriteltyjä. REST-palveluiden käyttämät URIt pitäisi pystyä osoittamaan tiettyihin resursseihin ilman epäselvyyksiä. Tämän mukaan Rodriquez rohkaisee käytettävyyteen, joka saavutetaan paremmin altistamalla URI sellaiseen hakemistorakennemuotoon, joka on luettavampi ja ymmärrettävämpi.

d) Resurssien edustamisen vaihtaminen

Tietoa pidetään resurssina. Tämä esitysmuoto voi jäljitellä tilan yhteydessä olevia resurssia ja kaikkia sen ominaisuuksia silloin kun asiakassovellus lähettää pyyntöjä palvelimelle. Komponentit, jotka muodostavat REST-palvelun ovat toiminnassa heti dataa vaihdettaessa mukana olevien resurssien avulla. Yksi saa esitysmuodokseen järjestää tietueet tietokantaan.

Tällä esitysmuodolla olisi suora yhteys tietokenttien ja XML-tagien väliseen esitykseen. Toisin kuin SOAP-arkkitehtuuriin perustuvassa viestinnässä, niin ”REST-pohjainen arkkitehtuuri vuorovaikuttaa ensisijaisesti tiedonsiirrossa mukana olevien edustavien resurssien kanssa”. M. D. Hansenin mukaan RPC-kutsu (Remote Procedure Call) pääasiallisesti pyrkii piilottamaan etäpalvelimen resurssien hyödyntämisen (Hansen 2007).

Jotta saavutettaisiin tehokas esitysmuotojen vaihtaminen, REST-palveluita kannustetaan noudattamaan tiedon tarkoituksenmukaista formaattia, jota asiakassovellus ja Web-sovelluspalvelu vaihtavat pyynnön ja vastauksen hyötykuormituksessa, jopa HTTP:n bodyn sisällä. RESTin päämääränä on saavuttaa komponenttien interaktion skaalattavuuden parantamista, sillä WWW:n eksponentiaalinen kasvu ei ole johtanut suorituskyvyn heikentymiseen. Yksi ilmentymä on asiakasohjelmistosovelluksien moninaisuus, jotka on tehty saatavaksi muille sovelluksille ja niihin pääsee käsiksi myös muut sovellukset. Kiinnostusta lisää tavoite yhtenäiset rajapinnat, mikä puhuttaa sekä RESTin että SOAPin puolestapuhujia. RESTin puolestapuhujat uskovat REST-ajatusmallin olevan parempi kuin SOAP-ajatusmalli, koska HTTP asiakassovellukset voivat vuorovaikuttaa HTTP etäpalvelimen kanssa ilman, että vaaditaan uudestaan konfigurointia. SOAP taasen vaatii tietoa menetelmistä kutsuakseen ja on kehysprotokolla kun taas HTTP on sovellusprotokolla.

Käynnissä on keskustelua RESTin ja SOAPin ominaisuukista. Eräät alan asiantuntijat tutkimuksissaan ovaat tuonut esille sen, että joissain olosuhteissa RESTIÄ ei voida käyttää web-sovelluspalveluiden suunnittelussa ja toteuttamisessa. Tässä keskustelussa asiantuntijat myöntävät, että RESTin avulla voidaan suunnitella ja toteuttaa Web-sovelluspalveluita, jotka ovat riippumattomia väliohjelmistoista kuten Oracle Application Server ja vastaavanlaiset palvelimet. Tämä kuitenkin poikkeaa SOAP-WSDL perustuvista Web-sovelluspalveluiden toteutuksista. REST on oikea esitysmuoto WWW:lle, sillä sen periaatteet rohkaisevat noudattamaan tiukasti alkuperäisiä WWW, URI- ja HTTP-standardeja. Richardsonin ja Rubyn (Richardson & Ruby 2007) mukaan Web-sovelluspalveluiden toteuttaminen RESTillä tekee mahdolliseksi saavuttaa integraation vaatimukset, jotka ovat tarpeen rakennettaessa yritysjärjestelmiä. Yritysjärjestelmien resurssit voidaan altistaa läpi REST-palveluiden, jotka voivat tarjota eri asiakkaille sovellusten tietoja, jotka on muotoiltu standardien mukaisesti.

5.2.10 SOAP vai REST

SOAP ja REST ovat tämän hetkiset kaksi vallitsevaa standardia web-sovelluspalveluiden toteuttamiseen. Järjestelmien kehittäjien ongelma ei johdu ymmärryksen puutteesta tai näistä toteutuksista vaan päätöksestä valita kumpaa toteutustapaa hyödynnettäisiin. Kuten Hansen (2007) tunnustaa SOAP ja REST ovat vain kaksi mallia WEB-rajapintojen toteuttamiseen web-sovelluspalveluille. Molemmat ovat toimivia ja niissä on omat hyvät ja

huonot puolensa. Kehittäjillä on loppuviimein velvollisuus valita parempi lähestymistapa käyttöönsä. Päätöksentekoprosessi on ehkä juuri se mikä aiheuttaa keskustelua ja tuo tarpeen tarkastella näiden kahden lähestymistapojen etuja. SOAPia on hyödynnetty laajasti Enterprise Application Integration (EAI)-ratkaisuissa edustaakseen erilaisia web-pohjaisia sovelluksia, jotka on yhdistetty ”legacy” eli uusien ja vanhojen järjestelmien integroimiseen. Yksi tunnettu SOAP-ajatusmallia toteuttamiseen käyttänyt organisaatio on Google. Toisaalta taas REST tarjoaa ensisijaisesti standardisointia URIlle, jota käytetään resurssien esitysmuotoihin. HTTP-toimintoja, kuten ”GET” jne. on hyödynnetty manipuloimaan näitä resursseja. SOAP on kehitetty ennen RESiä, REST on kuitenkin todistanut itse olevansa suositumpi ajatusmalli. Tällä hetkellä Web-sovelluspalvelut, jotka ovat saatavavilla verkossa hyödyntävät RESTiä. Nämä Web-sovelluspalveluita tarjoaa Yahoo, Flickr, pubsub, Bloglines, del.icio.us, Twitter usean muun joukossa. Amazon ja eBay tarjoavat Web-sovelluspalveluita jotka hyödyntävät sekä SOAPia että RESTiä. Seuraavaksi keskitytään kysymyksiin, jotka liittyvät tmän keskustelun otsikoihin.

a) Turvallisuus

Turvallisuus on yksi merkittävät näkökohta ”SOAP vai REST” välisessä keskustelussa. RPC-kutsujen edelleen lähettäminen HTTP-standardiporttien yli on pidetty parempana tapana tukea web-sovelluspalveluita pitkin ja pokin organisaation rajojen. RESTin kannattajat uskovat, että se vaarantaa verkon turvallisuutta. Koska RESTin RPC-kutsut toteutetaan HTTP:n yli, palomuurilla on mahdollisuus estää asiakkaan viestien motiivin suodattamalla HTTP-pyyntö, jota käytetään asiakkaan pyynnössä. Koska REST on tiukka HTTP-toiminnoille, se mahdollistaa sen, että GET-komento ei voi tehdä kyselyä palvelimelle tiedonhakua varten. Tämä ei päde SOAPiin, joka ei ole tiukka HTTP-komennoille ja mikä esimerkiksi käyttää POST-komentoa palvellakseen asiakkaan pyyntöjä.

b) Tietotyyppien käsittely

SOAP tukee joukkoa erilaisia kiinteitä tietotyyppejä ja tarjoaa tiukempaa tyypitystä kuin REST. Tämän etuna on se että, arvo joka palautetaan millä tahansa alustalla, on tehty saatavaksi vastaavan natiivissa muodossa.

c) Välimuistiin säilöminen

SOAP-asiakas pyytää hyödyntämään ”POST HTTP”-operaatiota, mikä usein vaatii kehittynyttä XML-pyynnön muodostamista, täten vastaukset säilötään asiakkaan välimuistiin. Asiakkaat voivat helposti käyttää REST APIa GET-operaatiolla, joka helpottaa välipalvelimia säilömään vastauksia välimuistiin. SOAP-viestejä ei siten voi helposti säilöä välimuistiin.

d) Server-side /Client Side toiminnallisuus

Yleisellä tasolla ollaan sitä mieltä, että REST on helppokäyttöisempi kuin SOAP. SOAP kuitenkin tekee helpommaksi altistaa työmenetelmille kuin REST. On selvää, että asiakkaan näkökulmasta on paljon helpompaa tehdä palvelupyyntöjä HTTP APIn kuin suorittaa vastaava SOAP APIn kautta. SOAP API vaatii useimmiten asiakaskirjastoa, stub-puhelua ja paljon taitoja ymmärtääkseen sitä, kun taas REST on valmiiksi paikallinen eri ohjelmointikielille ja on siksi helpompaa muodostaa HTTP asiakas kutsu. Koska REST-resursseja on useimmiten helppo kutsua suoraan asiakkaan käyttöliittymästä, niin se tekee REST-ajatusmallista hyödyllisemmän kuin SOAPista, joka taas on vahvoilla palvelin-puolelta katsoen.

e) Rajallinen kaistanleveys

REST on arkkitehtuuriltaan kevyempi, joten se pienentää vasteaikoja ja soveltuu siten paremmin web-käyttöön. SOAP tarvitsee XML-merkintäkieltä pakkaamaan asiakkaan pyynnöt ja vastaukset. SOAP kannattajat ovat sitä mieltä, SOAPin tarjoama vahva tiedon tyypitys tekee palvelun asiakkaan ja sen tarjoajan tietoisemmaksi siitä, mitä tyyppejä on osallisina ja näin ollen tekee siitä erittäin hyödyllisen. Tämä kysymys esitetään RESTin puolestapuhujille. On väitetty sekä REST että SOAP tarvitsevat dokumentin, joka määrittelee sisään- ja ulosparametrit. RESTin puolestapuhujien mielestä RESTin ollessa joustava, kehittäjät pystyvät tuottamaan WSDL-tiedostoja Web-sovelluspalveluille, mitkä tarvitsisivat erityisiä ilmoituksia parametreistä. Tämä olisi ”On demand”-tyyppinen ratkaisu.

Kun ottaa huomioon tämän keskustelun pohjalta esille tulleet mielipiteet, niin tämän tutkimuksen perusteella kumpikaan ajatusmalleista ei voi korvata toista. Tutkimuksessa ollaan samaa mieltä molempien puolestapuhujien kanssa SOAPin monimutkaisuudesta client side–kannalta sekä RESTin monimutkaisuudesta server side –kannalta. Molemmista ajatusmalleista on esitetty hyviä ja huonoja puolia ja on olemassa, että kyseessä oleva ala määrittää parhaiten sen, että kumpaa ajatusmalleista SOAP vai REST hyödyttää eniten kyseisen alan sovellusta.

5.2.11 SOA-ratkaisusta koituvat edut

Tässä osiossa arvioidaan SOA-ratkaisun lupaamia etuja ja kuinka se voisi mahdollistaa pelastus- ja turvallisuusviranomaisten käytössä olevien tietojärjestelmien integroinnin sekä yhteentoimivuuden. Yrityksien tietohallintojohtajat ja IT-osaston avainhenkilöt ovat kohdanneet ristiriitaisia haasteita siinä, että kustannuksia tulisi pienentää kun samalla pitäisi maksimoida käytössä olevien teknologioiden hyöty, parempien asiakaskokemuksien saavuttaminen, paremman kilpailuedun saavuttaminen ja ennakoivampi sekä reagoivampi

liiketoiminnan tavoitteiden toteuttaminen. Endrein, Angin ja Arsanjanin (2004) mukaan heterogeenisuus sekä muutokset ovat niitä taustatekijöitä, jotka ovat aiheuttaneet nämä haasteet. Eri valmistajien tuotteista koostetuvien järjestelmien integroiminen on edelleen painajainen organisaatioille. Teknologien kehittyminen on kiihtynyt viime aikoina ja organisaatioiden tulee muuttua ja sopeutua nopeasti uudistuksiin, jos he haluavat saavuttaa kilpailuetua ja vastata asiakkaiden muuttuviin vaatimuksiin sekä vähentää palveluista aiheutuvia kustannuksia. Yllä mainitut haasteet ovat johtaneet SOA-ratkaisun valintaan ja Endrein, Angin sekä Arsanjanin (2004) ovat määritelleet muun muassa seuraavat SOA-ratkaisusta koituvat edut:

1) Organisaation nykyisten voimavarojen hyödyntäminen

SOA on luonteeltaan palvelu- ja liiketoimintakeskeinen ja tekee organisaatioille mahdolliseksi hyödyntää tehokkaasti IT-investointejaan. Tehokkuus saavutetaan pakkaamalla yhteen olemassa olevat infrastuktuurit kuten palvelut. Tässä kohtaa SOA yhdistää liiketoimintatavoitteet teknologiaan ja myös ilman IT-infrastruktuurien uudelleenrakentamista, yritykset voivat silti saavutta liikevoittoa hyödyntämällä heidän nykyisiä ratkaisujaan. Ennalta määritetyt palvelut sisältävät omat rajapintansa. SOAn tunnustetaan olevan enemmän liiketoimintaprosessikeskeinen kuin teknologiakeskeinen, jos sitä verrataan muihin arkkitehtuureihin. Näin ollen palvelu yhdistetään tiettyyn ennaltamääritettyyn liiketoimintatehtävään. Seurattaessa SOAn suunnitteluperiaatteita, palveluiden rajapinnat ovat usein karkeita ja tilattomia. Ne perustuvat myös viestien ja dokumenttien vaihtamiseen. Oliopohjainen ajatusmalli on erilainen, koska se ei tue palvelualttiuden näkökulmaa. Sen sijaan se käsittelee yksittäisiä kohteita ja niiden ominaisuuksia tiiviisti kytketyllä tavalla.

2) Integrointi, yhteentoimivuus ja monimutkaisuuden hallinta

SOAn avulla mahdollistetaan integroinnin helppous ja kompleksisuuden hallinta. Tämä puolestaan tuo avoimuutta itse toteutukselle, joka täten vähentää vaikutuksia, jotka syntyvät IT-infrasruktuuien muutoksissa ja toteutuksissa. Palveluiden vaatimusmäärittely sitoo yhteen olemassa olevat infrastruktuurit, tekee integroinnista helpomman. SOAN avulla voidaan suunnitella ja toteuttaa yhteentoimivia ja standardeihin perustuvia järjestelmäkokonaisuuksia. Palvelut ovat SOA-ratkaisussa avaintekijänä ja niiden yhteentoimivuus tuetaan erilaisten rajapintojen avulla. Wrigthin ja Reynoldsin mukaan (2005) SOA-arkkitehtuurin johdonmukaisuuden sekä standardien avulla voidaan saavuttaa heterogeenisten järjestelmien yhteentoimivuus. Valitsemalla SOA-ratkaisu helpotetaan kehitystyötä. Web-sovelluspalveluita kehitetään useimmiten yhteistyössä jonkin merkittävän standarditoimijan, kuten esimerkiksi OASIS-järjestön (Organization for the Advancement of

Structured Information Standards) kanssa. Toimijoiden kehittämät standardit mahdollistavat yhteentoimivuuden eri laitevalmistajien kanssa. Erl (2009) on sitä mieltä, että SOA tarjoaa natiivin yhteentoimivuuden palveluiden kesken tarkoituksenaan vähentää integraatioastetta.

3) Kustannukset ja uudelleenkäytettävyys

SOAn kautta toteutetulla palvelukeskeisellä arkkitehtuurilla on tarkoitus tukea loogisen ratkaisun luomista, mikä ei ole sidottu mihinkään tiettyyn teknologiaan. Nämä ratkaisut ovat siksi luonnostaan tilattomia ja uudelleenkäytettäviä. Suuriin liiketoimintapalveluiden kokonaisuuksiin SOA-ratkaisu mahdollistaa löyhän kytkennän toisin kuin muissa arkkitehtuurin ajatusmalleissa. Tämä johtaa palveluiden saatavuuteen ja niitä voidaan yhdistellä täysin liiketoiminnan tarpeiden mukaisesti. Ohjelmistoresurssien päällekkäisyyttä on vähennetty, koska resursseja voidaan uudelleen käyttää pienimmillä kustannuksilla. SOA-ratkaisun avulla pienennetään kustannuksia ja kasvatetaan tuottavuutta.

4) Liiketoiminnan ja teknologian yhdenmukaistaminen sekä nopeampi markkinoille pääsy

SOAn avulla voidaan yhdenmukaistaa organisaation liiketoiminta ja teknologia. Organisaatiot, jotka pyrkivät olemaan muutosvalmiita ja haluavat vastata vaativiin liiketoimintatarpeisiin hyötyisivät SOA-ratkaisusta, joka mahdollistaa uusien palveluiden lanseeraamisesta nykyisten palveluiden avulla. SOA-ajatusmallin avulla voidaan hyödyntää organisaation nykyisiä palveluita, jolloin voidaan vähentää ohjelmistoprojektiin käytettävä aika, joka olisi suurempi täysin alusta aloitettavassa ohjelmistokehitystyössä ja edellyttäisi kaikkien ohjelmistosuunnittelun vaiheiden läpikäymisen. Kun ohjelmistokehitystyötä kierretään SOAn avulla, saadaan aikaan uusien palveluiden nopeampi kehittäminen ja annetaan organisaatioille mahdollisuus reagoida nopeasti alati muuttuviin tilanteisiin. Näin ollen markkinoille pääsee nopeammin.

5) Nopea mukautumiskyky ja monipuolisemmat vaihtoehdot laitevalmistajista

SOAn avulla organisaatiolla on paremmat valmiudet vastata muutoksiin. Organisaatioiden liiketoimintaprosessit koostuvat erilaisista palveluista ja SOAn avulla uusia palveluita voidaan luoda helposti lisää ja tarpeen tullen muuttaa vastaamaan tarpeita uudestaan. SOA tarjoaa joustavuutta sekä reagointikykyä, mitä tarvitaan yrityksien elinvoimaisuuden säilyttämiseen. Vaikka yleisesti sanotaan, että organisaatioilla ei ole tarvetta monipuoliseen IT-alustojen laitevalmistajien kirjoon, mutta monipuolisuus on kuitenkin etu. SOA-ratkaisu mahdollistaa ja varmistaa sen, että erilaisiin palveluiden totettamiseen hyödynnettävät teknologiat ovat täysin riippumattomia laitevalmistajista. Näin organisaatiot voivat helposti muuttaa tai laajentaa omia IT-alustojansa. SOA tarjoaa riippumattomuutta laitevalmistajista. Tämä

osaltaan tukee ja vahvistaa yrityksiä tekemään muutoksia IT-alustoihinsa, koska fyysiset palvelusopimukset on standardisoitu.

Tiivistettynä luvussa esiteltiin SOAn ja web-sovelluspalveluiden taustat. Olemme osoittaneet, että SOA ja Web-sovelluspalvelut ovat avainasemassa, kun halutaan saavuttaa järjestelmien standardointia, integrointia ja yhteentoimivuutta. Esitutkimuksen jälkeen voidaan siirtyä seuraavaan vaiheeseen eli tutkia miten SOA-ratkaisua voidaan soveltaa pelastus- ja turvallisuusviranomaisten ICT-järjestelmien taroamien palveluiden kehittämiseen. Tulevissa julkaisuissa tullaan esittelemään erilaisia toimintasuunnitelmia ja lisää tutkimustuloksia.

5.2.12 Keskustelu

Tavoitteena on aloittaa turvallisuus- ja pelastusviranomaisten tietojärjestelmien palveluihin liittyvää standardisointi ja toteuttaa eri järjestelmien välinen integrointi, jonka avulla parannetaan yhteentoimivuutta. SOA ja siihen liittyvät web-sovelluspalvelut olisivat kiinnostava ja mielekäs ratkaisu toteuttaa pelastus- ja turvallisuusviranomaisten kenttätyöskentelyn palvelut ja niiden jakaminen tehokkaasti. Kuvasimme aiemmin julkaisussa alan toimintaympäristöä, joka yli koostuu yli 20 alueellisista yksiköistä ja laitoksesta. Kaikki viranomaiset sijainnista riippumatta voisivat hyötyä SOA-ratkaisun käyttöönottamisessa, koska sen avulla mahdollistetaan yhtenäinen ja yhteinen web-sovelluspalveluiden hallinnointi ja informaation jakaminen tietoliikenneyhteyksien välillä. Tämä helpottaisi ratkaisemaan hallinnollisiin liittyviä kysymyksiä. Tulevassa tutkimustyössä on tältä osin tarkoitus tehdä hyödyllisiä suosituksia todennäköisimmästä ohjelmistoarkkitehtuurista, joka vastaisi parhaiten viranomaispalveluiden tarpeita.

5.3 DSiP Distributed Systems intercommunication Protocol – tietoliikenneratkaisu vakaaseen ja turvattuun monikanavaviestintään

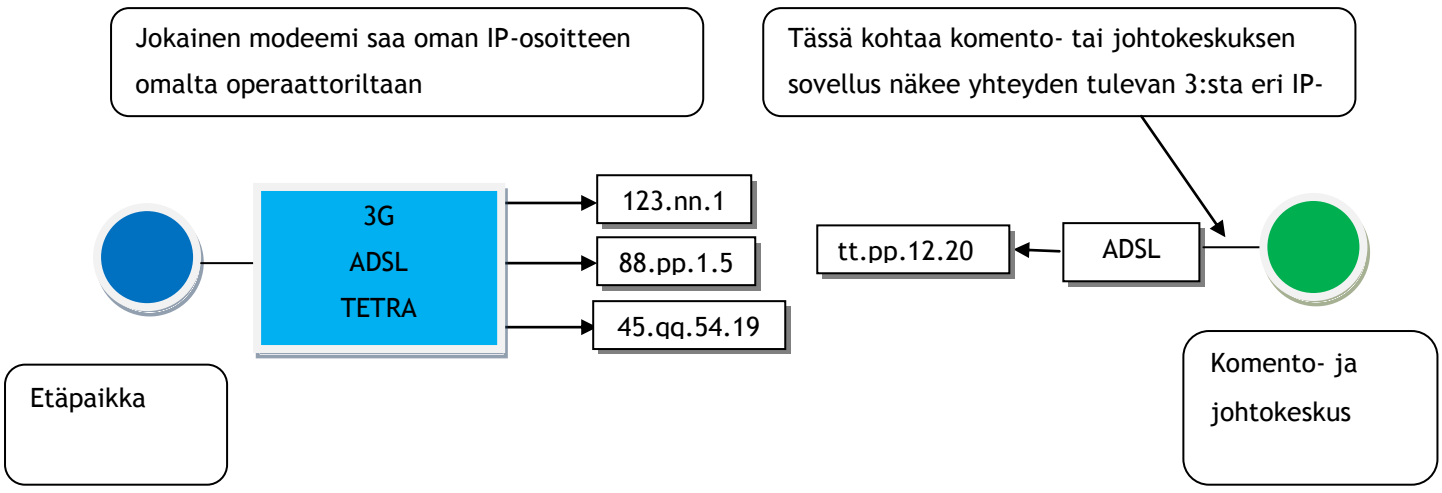
5.3.1 Tiivistelmä

Luotettavan tietoliikennepohjaisen viestinnän merkitys kasvaa kokoajan. DSiP-ratkaisu mahdollistaa kaiken tietoliikenteen jakamisen, niin että se toimii useamman operaattorin ja menetelmän kautta, jolloin puhutaan todellisesta monikanavaisuuteen perustuvasta järjestelmästä. Monikanavareititykseen perustuva DSiP kasvattaa luotettavuutta, turvallisuutta ja yhteentoimivuutta ja mahdollistaa yleisempien tietoliikennemenetelmien hyödyntämisen kriittisen viestinnän järjestelmissä. Jakamalla tietoliikenneyhteksiin liittyvät riskit useammalle operaattorille ja menetelmälle saavutetaan parempi reititys ja voidaan ottaa turvallisuuteen ja tunkeutumiseen liittyvät riskit huomioon. Sen avulla lisätään myös järjestelmien modulaarisuutta.

Internet kehitettiin 1970-luvun alussa, jolloin kaksi henkilöä Robert E. Khan ja Vinton Derf kehittivät Internet Protokollan (IP). IP-protokolla on yleisesti ottaen hyväksi havaittu protokolla, mutta kukaan ei osannut varautua siihen, että erilaisten tietoliikenneyhteyksien kautta kulkeva viestintä nousee niin suureen rooliin, kuin se nykypäivänä on. Nykypäivänä kustannustehokkain tapa tiedonsiirrolle on hyödyntää tietoliikenneverkkoja, jotka perustuva IP-protokollaan. Myös monikanavareititykseen perustuvia IP-verkkoja on tutkittu jo vuosien ajan, jotta voitaisiin vähentää tietoliikenneyhteyksien ruuhkapiikkejä. Suurin osa liiketoiminnan tueksi kehitetyistä organisaation toiminnan kannalta kriittisistä sovelluksista hyödyntävät IP-protokollaa, joka on kustannustehokas protokolla maanlaajuista tiedonsiirtoa varten. On tärkeää kiinnittää huomiota siihen, että kaikki liiketoiminnan kannalta kriittiset internetyhteydet ja tärkeät VPN-yhteydet ovat aina toiminnassa. Kehittyneimmät monikanavareitityseen perustuvat tietojärjestelmät valvovat jatkuvasti organisaatiton toiminnan kannalta kriittistä tietoliikennettä. Törmättäessä tietoliikenneongelmiin järjestelmällä on mahdollisuus ottaa käyttöön vaihtoehtoinen reitti tiedonsiirtoa varten.

5.3.2 Tutkimusongelma

Kuvassa 3 esitetään, kuinka tyypillinen multimodeemi-järjestelmä toimii. Jokainen modeemi saa oman IP-osoitteen operaattoriltaan. Komento- tai johtokeskuksen sovellus näkee yhteyden muodostuvan monesta eri IP-osoitteesta. Tämän kaltainen multimodeemi-järjestelmä ei pysty jakamaan yhteyttä eri fyysisten menetelmän kesken ilman, että sovellus uudelleen kirjoitetaan tekemään niin, koska IP ei tue monikanavaista viestintää, mikä kulkisi useamman eri fyysisen menetelmien kautta. Sovelluksen uudelleenkirjoittaminen tekemään niin, on todella haastava tehtävä.



Kuva 3: Tyypillinen multimodeemi-järjestelmä

Virtual Private Network (VPN)-yhteyksiä käytetään tyypillisesti multimodeemi tietoliikenneympäristössä, mutta siihen liittyy puutteellisuuksia sillä, VPN-ratkaisut antavat tyypillisesti luoda yhteyden yhdellä menetelmällä kerrallaan. Jos yhteydessä kohdataan ongelmia, VPN:n tulee uudelleen käynnistää yhteys toisen menetelmän avulla. Rajoitteet ja puutteet liittyvät IP-osoitteiden luomiseen ja siihen kuinka IP-osoitteiden yhteyksiä käsitellään.

5.3.3 Tutkimuskysymys

IP-protokolla on erinomainen protokolla tiedonsiirtoa varten, mutta ei ole riittävä, kun kyseessä on kriittinen tietoliikenne tai erittäin tärkeä tietojärjestelmä. Tutkimuskysymys kuuluu:

”Onko olemassa sellaista ratkaisua, joka mahdollistaa myös tavanomaisten viestintäkeinojen hyödyntämisen kriittisessä telemetria-järjestelmässä?”

5.3.4 Ongelman ratkaisu

Uusi monikanavaisuuteen perustuva tietoliikenne-konsepti mahdollistaa yhtenäisen tavan olla yhteydessä käytännössä lähes minkä tahansa viestimen avulla niin, että useat, joskus rinnakkaisetkin tietoliikenneyhteydet, näyttäytyvät yhtenä vankkana, turvallisena ja luotettavana tietoliikenneyhteytenä.

Seuraavassa esitetty ratkaisu perustuu Ajeco Oy:n kehittämään Distriputed Systems intercommunication -Protokollaan (DSiP). Tämä protokolla määrittää valitun tietoliikenneyhteyden ja sulkee pois kysymykset liittyen tietoliikenneyhteyden perustamiseen, kun laite ja/tai sovellus haluaa ottaa yhteyden toiseen laitteeseen/sovellukseen. DSiP on samanaikaisesti protokolla- sekä reititystason tietoliikennetekniikan ohjelmistoratkaisu, joka käsittelee älykkäästi tiedon reitittämistä. Tämä sisältää sekä IP- ja ei IP-pohjaisen tiedonsiirron. Tietojärjestelmien luotettavuus ja hallittavuus kasvaa merkittävästi niiden ollessa täysin riippumattomia yhteyksien mahdollistavista operaattoreista. DSiP:iä voidaan pitää tietoliikenneyhteyden suunnittelukerroksena, ”puuttuvana OSI-kerroksena” IP-kerroksen yläpuolella.

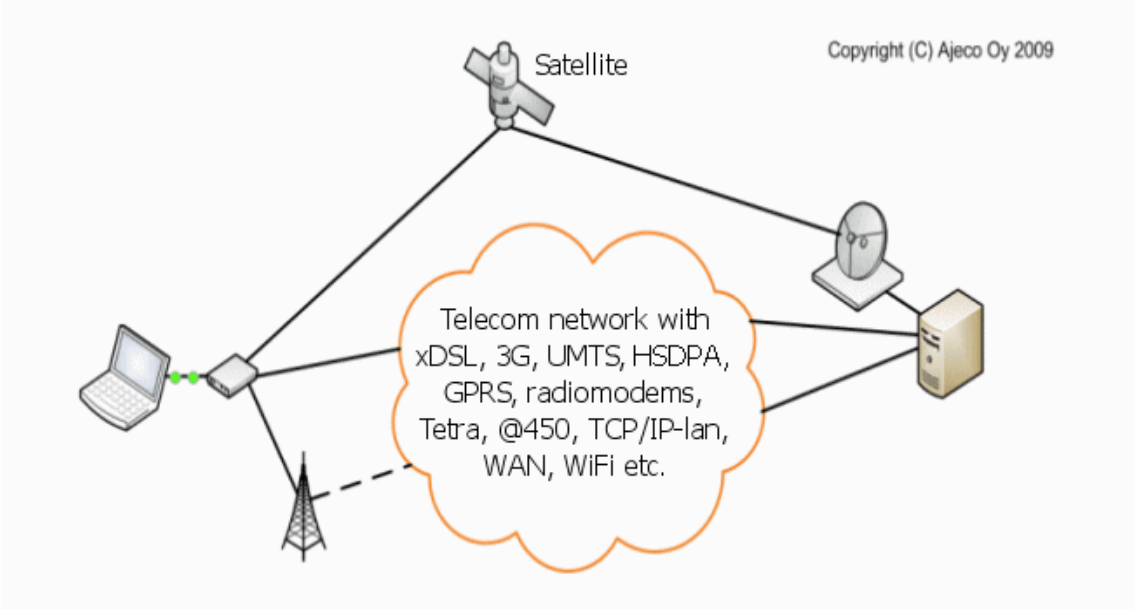
DSiP mahdollistaa:

1. Tietoliikennemenetelmien hyödyntämisen rinnakkain, niin että useat rinnakkain toimivat yhteydet näyttäytyvät yhtenä luotettavana yhteytenä. DSiP voi reitittää tiedot sekä IP- ja ei IP-pohjaisten yhteyksien yli.

2. Itsenäisyyden ja riippumattomuuden liittyen yhteyksiä tarjoaviin operaattoreihin. Se mahdollistaa käyttäjän ostaa ja hyödyntää tietoliikenneyhteyksiä miltä tahansa operaattorilta.
3. Protokollien käännöstavat niin, että laitteet, järjestelmät ja ohjelmistot voivat olla yhteensopivia.
4. Turvallisuusmekanismien hyödyntämisen ja vähentää riskejä liittyen esimerkiksi DOS-hyökkäyksiin ja virus-infusiooneihin.
5. Tiedon paremman hallittavuuden, reitittämisen ja priorisoinnin.

5.3.5 Järjestelmän kuvaus

Kuvassa 4 esitellään yleiskuvaus DSiP-telemetriajärjestelmästä. Se kykenee reitittämään tietoa minkä tahansa (IP ja ei IP) yhteyden kautta. Se toimii usean toimijan/operaattorin ympäristössä ja soveltaa seuraavia yhteyksiä: satelliitit, 3G, GRPS, UMTS, HDSPA, IP-verkko, TETRA, sarjayhteydet ja radiomodeemit.

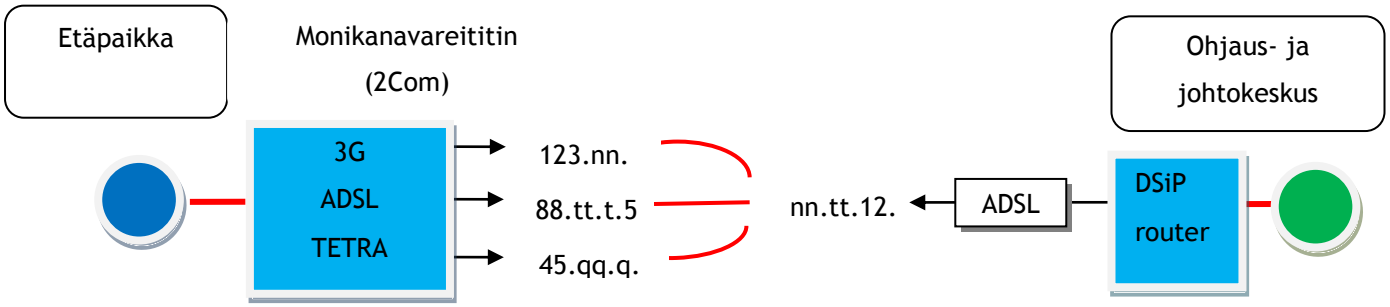


Kuva 4: DSiP Telemetria-järjestelmä

5.3.6 Vankka ja turvallinen tietoliikenneyhteys

DSiP-protokolla tukee VPN-tunnelin jakamista useaan fyysiseen kanavaan ilman kuvassa 5 esitettyjä rajoitteita. Lisäksi se ratkaisee yhteensopivuusongelmia sekä fyysisellä että loogisella tasolla tarjoten modulaarisuutta, tietojen eheyttä, turvallisuutta ja monipuolisuutta niin pienille kuin erittäin suurille tietojärjestelmille. DSiP:in loogisia sääntöjä noudattamalla ja käyttämällä IP:n keinoja tiedon kuljettamiseen, niin eri toimittajien sovellukset, laitteet ja ohjelmistot voivat olla yhteydessä toisiinsa keskenään

riippumattomasti. Näin ollen sovellukset voivat vastata sekä pyytää palveluksia ilman, että niiden erikseen tarvitsee tietää fyysisistä toteutuksista.



Kuva 5: DSiP-monikanavajärjestemä

5.3.7 Modulaarisuus

DSiP-telemetriajärjestelmä koostuu aina kolmesta elementistä:

- Etäpaikka (esimerkiksi poliisiauto tai sähköasema)
- Tietoliikennejärjestelmä
- Ohjaus- ja johtokeskus

Jos joku kolmesta elementistä vaihtuu, niin se ei vaikuta muiden elementtien toimintaan.

5.3.8 Sovellukset

Suomen pääsähköverkkoja kontrolloidaan SCADA-järjestelmän avulla ja se siihen sovelletaan DSiP-telemetriajärjestelmää. Telemetriatietojen valvomiseen ja saamiseen hyödynnetään rannikon valvontakameroita. Suomen saaristo ja sen ankaraan ilmastoon liittyvät olosuhteet lisäävät laitteisiin kohdistuvaa stressiä, kun ne on asennettu merivalvontajärjestelmiin.

DSiP-järjestelmä mahdollistaa sijainnista riippumattoman toiminnan eli valvomo voidaan sijoittaa mihin tahansa haluttuun paikkaan.

5.3.9 DSiPiin liittyvä keskustelu

DSiPiä hyödyntävät tahot voivat hyödyntää useita viestintäkanavia rinnakkain, siten että loppukäyttäjät ”ajattelevat”, että he käyttävät vain yhtä kanavaa. DSiP jakaa tietoliikenneresurssit eri laitteistojen ja ohjelmistojen moduuleille; ne reitittävät automaattisesti ja käyttävät vaihtoehtoista reittiä ensisijaisen yhteyden katketessa. Se on aina tietoinen oikeasta vastaanottajasta ja oikeasta lähettäjästä sekä käyttää vahvaa salausta

ja aikaleimoja. Näin ollen DSiP tekee viestinnästä vahvempaa ja edistää sen tietoturvaan liittyviä seikkoja.

DSiPin myötä sen käyttäjillä on tehostetut kontrollointimahdollisuudet:

1. Priorisointi: tärkeä tieto reititetään ensin, vähemmän tärkeä myöhemmin
2. Verkkojen aikalisien kontrollointi: ei määrittelemättömiä viivästyksiä tai odoteluita
3. Käytössä olevien kaistaleveyksien valvonta: DSiP tiedostaa kaikkien reitittimien tilan joka hetki
4. Sen avulla on helpompi kontrolloida ylläpitoa ja konfigurointia

DSiP yhdistää IP- ja ei IP- protokollaan perustuvaa liikennettä yhdeksi kontrolloitavaksi järjestelmäksi. DSiP ei ole raskas tai hankala protokolla ja sen voi upottaa erilaisiin laitteisiin ja alustoihin. DSiP sisältää seuraavat ominaisuudet:

- Ratkaisut liittyen tiedon eheyteen, turvallisuuteen ja autentikointiin
- Automaattinen uudelleenreititys backup-yhteyksien avulla
- Hallittavuus, kaistanleveyksien hallinta
- Standardoidut rajapinnat sovelluksille ja laitteistoille, ratkaisee monia yhteentoimivuusongelmia
- Skaalattavuus, järjestelmä on joustava sekä siihen on helppo lisätä uutta ja vanhaa laitteistoa sekä ohjelmistoa
- Täysin riippumaton tiedonsiirtomenetelmistä
- Reaaliaikainen tieto verkkotopologiasta – ei toivotut yhteydet hylätään

Laurea-ammattikorkeakoulun Leppävaaran yksikköön on perustettu testiympäristö, jonka tarkoituksena on testata ja demonstroida monikanareititinjärjestelmä-ratkaisua. Luomalla erilaisia ongelmatilanteita ja skenaarioita, voidaan testata DSiP-järjestelmän luotettavuutta ja vakautta. Tähänastiset tulokset ovat olleet rohkaisevia ja useat yhteydet näyttäytyvät kuin yhtenä vakaana tietoliikenneyhteytenä, kuten pitääksin. Kun yksi yhteys epäonnistuu, DSiP löytää helposti uuden rinnakkaisen reitin. Se kuinka uusi yhteys on luotu, voidaan lukea logeista jälkikäteen. Logit eivät ole kovinkaan kuvaavia, joten sen vuoksi kehitetään uusia visualisointiin työkaluja (Holmström, Rajamäki ja Knuuttila 2010, 24-25).

5.3.10 Johtopäätökset

Monikanavaisen tiedonsiirron tarve on maailmanlaajuinen ja kasvava. DSiP-pohjainen ratkaisu mahdollistaa yleisien tietoliikennemenetelmien käyttämisen kriittisessä telemetriajärjestelmässä. Se mahdollistaa myös monenlaisen tietoliikenneresurssien hyödyntämisen: IP- tai EI IP-pohjainen tiedonsiirto, TETRA-verkko, sateliittiyhteyksien, sarjayhteyksien jne. ja nämä kaikki ovat yhdessä hallittavassa järjestelmässä.

5.4 Tulevaisuuden monikanavareititykseen perustuvat turvalliset teknologiaratkaisut

Luotettavan tietoliikenteen merkitys kasvaa jatkuvasti. Tämä luku esittelee monikanavaisuuteen perustuvan tietoliikennekonseptin. Sen avulla mahdollistetaan yhtenäinen tapa olla yhteydessä minkä tahansa viestintävälineen kautta, niin että usea ja joskus jopa rinnakkain kulkevat tietoliikenneyhteydet näkyvät yhtenä vankkana, keskeytymättömänä, turvallisena ja luotettavana viestintälinkkinä yhteydessä olevien laitteiden välillä. Ratkaisun nimi on DSiP (Distributed Systems intercommunication Protocol) ja se mahdollistaa kaikenlaisen tietoliikenteen jakamisen usean operaattorin ja menetelmän kautta, minkä tuloksena on monikanavareititysjärjestelmä. DSiP-monikanavareititysjärjestelmä kasvattaa tavanomaisten viestintämenetelmien luotettavuutta, turvallisuutta ja eheyttä ja mahdollistaa niiden käyttöönoton kriittisessä telemetriajärjestelmässä. Tämä saavutetaan jakamalla riskit useamman operaattorin tarjoaman tietoliikenneyhteyden kesken. Tämä mahdollistaa paremman reitituksen ja priorisoinnin ottaen samalla huomioon turvallisuuteen ja tunkeutumiseen liittyvät riskit. Ratkaisun avulla lisätään myös modulaarisuutta.

Nykyään kustannustehokkain tiedonsiirtokeino maailmanlaajuiseen viestintään on hyödyntää tietoverkkoja, jotka perustuvat IP-protokollaan. Monikanavareititykseen perustuvia IP-tietoverkkoja on tutkittu jo vuosia. Tämän päivän monet IP-pohjaiset ratkaisut on kehitetty kriittisiä liiketoimintasovelluksia varten. Näitä ratkaisuja käytetään maailmanlaajuisesti ja niiden tarkoitus on helpottaa yrityksiä varmistamaan, että liiketoiminnalle kriittiset Internet-yhteydet ja VPN-yhteydet ovat aina toiminnassa. Pitkälle kehitetyt monikanavajärjestelmät seuraavat jatkuvasti kriittistä liikennettä ja, jos verkossa havaitaan tietoliikenneongelmia, niin järjestelmä on valmis käyttämään vaihtoehtoista reittiä (Holmström, Rajamäki & Hult 2011, 57-60).

Organisaatioiden operatiiviset tehtävät ovat kehittyneet ja muuttuneet vuosien aiana. Yhä suuremmassa roolissa ovat useat viestintälaitteet, ohjelmistot, palvelut ja internetin tai muiden yhteysien kautta toimivat tietokannat. On tärkeää, että kaikki prosessien kannalta tärkeä tieto on saatavilla keskeytyksittä missä tahansa ja millon tahansa.

Tietojärjestelmien luotettavuuteen ja turvallisuuteen vaikuttavat monet tekijät. Turvallisuus- ja luotettavuusriskit tulee ottaa tarkasti huomioon, kun aloitetaan uusia tietojärjestelmäprojekteja tai tehdään integrointeja olemassa oleviin tietojärjestelmiin. Edellämainitut asiat ovat välttämättömiä esimerkiksi kriittisissä kontrollointijärjestelmissä ja silloin, kun määritetään viestinnän tarkoitus. Viestintä on kriittisessä roolissa monessa

organisaatiossa. Erittäin kriittisessä roolissa se on palo-, etsintä- ja pelastusaloilla sekä lainvalvontaviranomaisten keskuudessa.

Cyber-, luotettavauus- ja tuvallisuusriskit, mitkä liittyvät viestintäjärjestelmiin ja kanaviin, tulee tunnistaa ja tuntea ennen kuin tehdään mitään hankintapäätöksiä (Hult, Rajamäki & Hult 2011, 143-148). Riskit ja uhat voidaan määrittää useasta eri näkökulmasta. Luotettava ja turvattu kriittinen viestintä riippuu siitä keneltä kysyy. Elinkeinoelämän organisaatioiden ja siviiliviranomaisten kriittisen viestinnän tulee pysyä niin paljon verkossa ”onlinena” ja he hyödyntävät usein tavanomaisten teleoperaattoreiden palveluita. Kun taas puolustusvoimien taktinen viestintä ei voi hyödyntää tavanomaisten teleoperaattoreiden palveluita ja niiden tulee olla verkosta ”offlinena” niin usein kuin mahdollista. Molemmille käyttäjäryhmille tulee kuitenkin taata, että viestintä on luotettavaa, turvattua, tehokasta, yhteentoimivaa, rehellistä jne.

Tietojärjestelmien integrointi on vallitseva trendi yrityksissä ja organisaatioissa (Litan 2011, 250-256). Integraatioden avulla suunnataan kohti liikkuvuuden mahdollistamista ja tietoliikenneyhteydet ovat keskeisessä roolissa. Erilaisten tietoliikenneyhteyksien avulla tarjotaan liiketoiminnan kannalta tärkeitä tietoja, sovelluksia ja palveluita mobiilikäyttäjille. Palveluntason vaatimukset ovat merkittävässä roolissa, mutta näitä vaatimuksia on kuitenkin määrällisesti hankalaa ilmaista, kun integroinnissa ollaan vielä suunnitteluvaiheessa. Seuraavia aineettomia arvoja voidaan kuitenkin käyttää ohjainviivojen laatimista varten: käytettävyys, suorituskyky, skaalautuvuus, luotettavuus, saatavuus, laajennettavuus, ylläpidettävyys, hallittavuus, luotettavuus ja turvallisuus. Vasta käyttöönoton jälkeen näitä ominaisuuksia voidaan mitata. Jokaisen WEB-pohjaisen tietojärjestelmän tarkoituksena on tukea yrityksien ja organisaatioiden tarpeita. Jokaisessa uudessa projektissa painopisteen muutos saattaa olla tarpeen ja lisäksi web-arkkitehtuurin toimintaan tulisi nähdä enemmän vaivaa, kiinnitettävä enemmän huomiota ja ottaa vakavammin (Tumin & Encheva 2011, 245-249).

Tämä on johtanut monien tietojärjestelmäintegraatioiden käynnistymiseen. Integroinnin avulla pyritään kehittämään muun muassa liikkuvuutta, jotta prosessien kannalta tärkeät toiminnot voidaan toteuttaa ajasta ja paikasta riippumatta. Tietoliikenneyhteydet toimivat keskeisessä roolissa, sillä niiden avulla mahdollistetaan tiedon, sovelluksien ja palveluiden saatavuus paikasta riippumatta.

Myös poliisi- ja pelastusviranomiasten toiminnalliset tehtävät ja työmenetelmät ovat kehittyneet ja muuttuneet vuosien aikana. Kentällä tapahtuva pelastus- ja hälytystehtävien suorittamiseen vaaditaan erilaisia järjestelmiä, viestintälaitteita, sovelluksia ja tietokantoja. Näiden toiminnan takaamiseksi tietoliikenneyhteydet ovat suuressa roolissa. On tärkeää, että

tehtävän suorittamisen ja mahdollisen kriisitilanteen selvittämisen kannalta tärkeää tilannetietoa voidaan jakaa kaikille sitä tarvitseville. Lisäksi tehtävien suorittamisen kannalta tärkeä tieto tulee olla saatavilla ongelmitta ja keskeytyksittä milloin vain ja missä tahansa.

5.4.1 Turvallisuusviranomaisten viestinnän tarpeet

Koivukoski (2011, 245-249,) kuvailee väestön turvaamisen viranomaistoiminnan viestinnän vaatimukset:

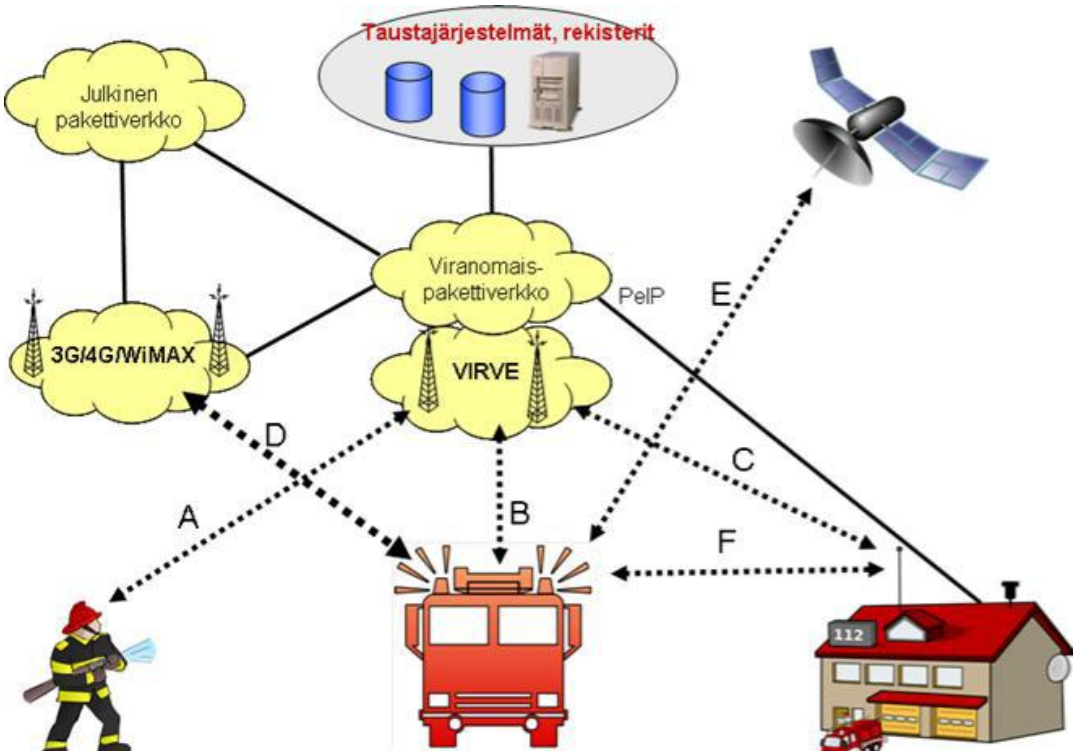
1) Luotettava ja vakaa puheviestintä paikasta riippumatta
2) Yhteistyön ja viestinnän helppous koko organisaation kesken
3) Lyhytsanomaviestit hälyttämiseen, kenttätehtävän välittämiseen ja tiedon paikkansapitävyyden tarkistamiseen
4) Tiedostojen välittäminen onnettomuuspaikalta/onnettomuspaikalle
5) Päivittäiseen kenttätyöskentelyyn tarjottavat kommunikointiyhteydet

Nyky-yhteiskunnassa tarvitaan tietoliikenneyhteyksiä, että taataan olennaiset palvelut myös hätätilanteissa. Haastavissa tilanteissa kriittiset tietoliikenneyhteydet helpottavat merkittävästi pelastusviranomaisten yhteistyötä, tilannetietoisuuden optimointia sekä niiden avulla parannetaan vasteaikoja ja tilanteen kontrollointia. Eritysryhmille tulee taata turvalliset ja häiriöttömät ääni- ja tietoliikennepalvelut. Ammattikäyttöön suunnattu analoginen radioverkko on tietoliikenneyhteys, jota ei pääsääntöisesti ole suojattu salakuuntelulta. Se tarjoaa myös rajallisen äänen laadun. Radioverkon laitteet perustuvat yleensä TETRA- ja TETRAPOL-standardiin.

Puheviestintäjärjestelmän tärkeimmät ominaisuudet ovat:

1. Ryhmälähetysviestintä (Point to multipoint communication)
2. Ominaisuudet “Push-to-talk”, “releaste to listen”
3. Laaja kuuluvuusalue
4. Suljetut käyttäjäryhmät
5. VHF- ja UHF- taajuuksien käyttömahdollisuus

Kuvassa 6 esitetään pelastustoiminnan langattomien tietoliikenneyhteyksien rajapinnat.



A: TETRA air interface of handheld radio
B: TETRA air interface of vehicle radio/modem
C: TETRA air interface of station radio/modem
D: Air interface for commercial networks
E: SATCOM
F: WLAN Interface between Rescue vehicle and Fire station LAN/Intranet

Kuva 6: Pelastusviranomaisten kenttätyön langattoman tiedonsiirron rajapinnat (Rantama & Junttila 2011)

5.4.2 TETRA ja TETRAPOL

The Terrestrial Trunked Radion (TETRA) on kehittänyt Euroopan televiestintä standardien instituutti ETSI. Se sisältää sarjan erilaisia standardeja. Käytännössä nämä standardit sisältävät erilaisia teknologioihin liittyviä määritelmiä, kuten radiorajapinnat, verkkorajapinnat sekä palvelut ja laitteiston.

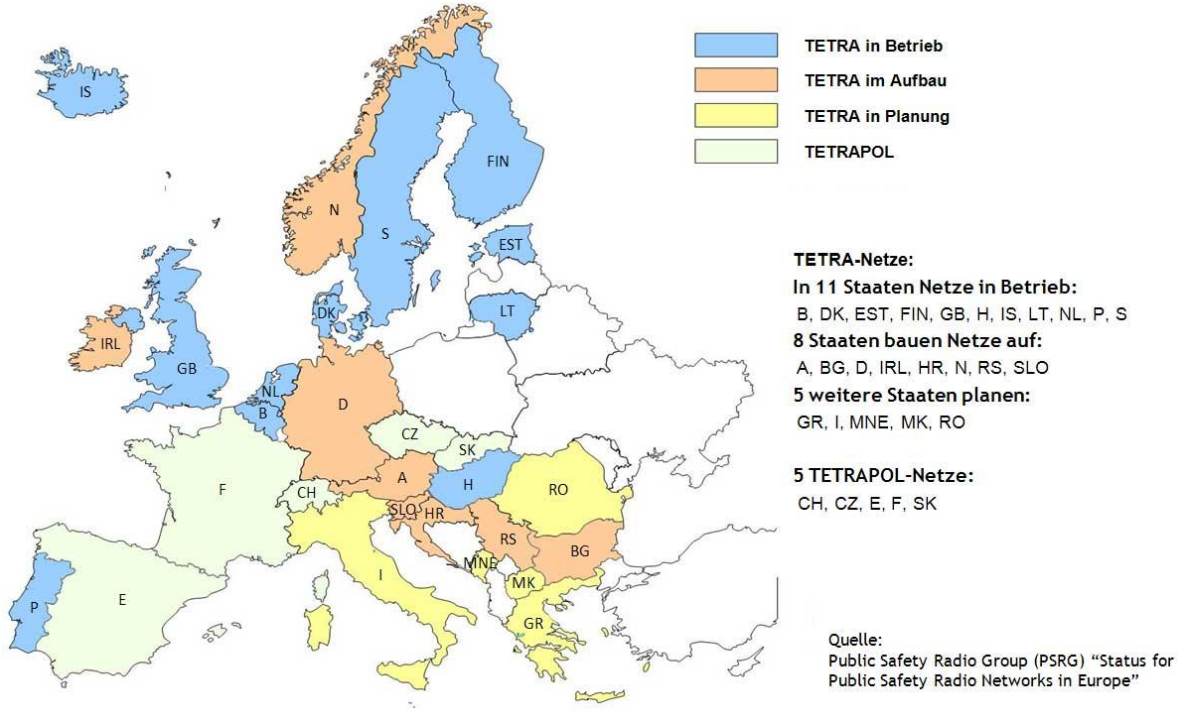
TETRA on maailmanlaajuisesti käytössä oleva standardi ja sen avulla on rakennettu jo satoja TETRA-verkkoja ympäri maailman. TETRA-järjestelmillä on monia hyviä etuja ja sitä voi hyödyntää kaikki turvallisuustoimijat sen ollessa samalla myös taloudellinen ratkaisu. Se

tarjoaa turvatun tietoliikenneyhteyden hätätilanteiden ja katastrofien aikana ja se on täysin digitaalinen järjestelmä. TETRA-järjestelmä tarjoaa käyttäjilleen korkealaatuisen puheviestintäkanavan ja mahdollisuuden piirikytkentäiselle ja pakettikytkennäiselle tiedonsiirrolle.

TETRA perustuu VPN-teknologiaan, joka tarjoaa yhden fyysisen verkon eri organisaatioiden kesken. Kriisitilanteen luonne vaikuttaa käytössä oleviin viestintäkeinoihin. Esimerkiksi ylikuormittuessa runsaan matkapuhelinliikenteen takia suuren yleisön keräävässä tapahtumassa (rock-konsertti, jääkiekko-ottelu yms.).

Riippumatta TETRA-standardin hyödyistä, kuten taloudellisuus ja toimintavarmuus vaativissakin olosuhteissa, niihin perustuvissa verkoissa on kuitenkin yksi suuri heikkous: datasiirtokapasiteettiin liittyvät rajoitukset. TETRAPOL on toinen digitaalinen puheviestintätekniikan standardi yleistä turvallisuutta ylläpitäville tahoille.

Kuva 7 esittää Euroopan maailmanlaajuiset radioverkot. TETRA-pohjaiset verkot toimivat Suomessa, Englannissa, Hollannissa, Belgiassa, Unkarissa, Virossa, Liettuassa, Tanskassa ja Portugalissa.



Kuva 7: Valtakunnalliset puheviestintäverkot Euroopassa (Rantama & Junttila 2011)

5.4.3 Monikanavareititykseen pohjautuva viestintä

Suomalainen VIRVE-viranomaisradioverkko on mahdollistanut useille viranomaiselle korkeatasoisen yhteistyömahdollisuuden (onnettomuuden) tapahtumapaikalta. Jokaisella viranomaisella ovat samat perustarpeet, mitä he odottavat tietoliikennejärjestelmältä, mutta jokainen käyttäjäryhmä asettaa sille omat erityisvaatimuksensa. Tarkoituksena on löytää yhtenäiset ratkaisut ja toimintamallit, jotka helpottavat järjestelmäintegraatiota ja mahollistaa yhtenäisen järjestelmäsuunnittelun. Haluna on parantaa toiminnallisuuksia, tehdä kustannussäästöjä ja parantaa viranomaisten välistä yhteistyötä (Rantama & Junttila 2011).

VIRVEn tarjoama puheviestinnän palvelut toimivat hyvin korkealla luotettavuudella, nopeilla yhteyksillä ja hyvällä kattavuusalueella. Viranomaiset ovat yleisellä tasolla tyytyväisiä VIRVEn tarjoamiin palveluihin puheviestinnän suhteen ja suuria mullistuksia sen kehittämisen suhteen ei olla tekemässä. Lisäksi VIRVEn tarjoama tiedonsiirto-palvelut ovat luotettavia ja kattavuus on hyvä. Mutta VIRVEn tiedonsiirrolle tarjoama kapasiteetti on kapea, joten viranomaiset ovat tyytymättömiä sen osalta VIRVEn toimintaan. VIRVEn tarjoaman tiedonsiirtokapasiteetin ei ole tiedossa kehitystyötä lähitulevaisuudessa, mikä täyttäis kaikkii tarpeet. Mahdollinen TETRA Enchanced Data Service, TEDS:in päivitys saattaa tuoda osaratkaisuja datakapasiteetin rajoittavuusasiaan (Rantama & Junttila 2011).

Rantama & Junttila (2011) kuvailee eri teknologiaratkaisujen tulevaisuutta seuraavanlaisesti:
1) @450/WiMAX/CDMA,LTE
Poliisiviranomaisilta tullut positiivista palautetta kattavuuden ja käytettävyyden suhteen. Teknologian tulevaisuus epävarmaa.

2) 2G/EDGE/GRPS
Nämä teknologiat ovat saavuttamassa elinkaarensa loppua.

3) 3G/HSPA
Hyvä kattavuus, mutta heikkoutena kaupallisten verkkojen saatavuus- ja kapasiteettiongelmat tungosalueiden suuronnettomuuksissa.

4) Ensimmäinen 4G/LTE -verkko
Ei toimi maaseudulla.

5) WLAN-teknologia mahdollistaa 3 datasiirtomahdollisuutta:
a) Vehicle - Fire station at the garage (Ajoneuvosta paloaseman autotalliin)
b) Paikallinen langaton verkko ajoneuvosta onnettomuuspaikalle
c) Vehicle - public WLAN “WLAN fire plug”

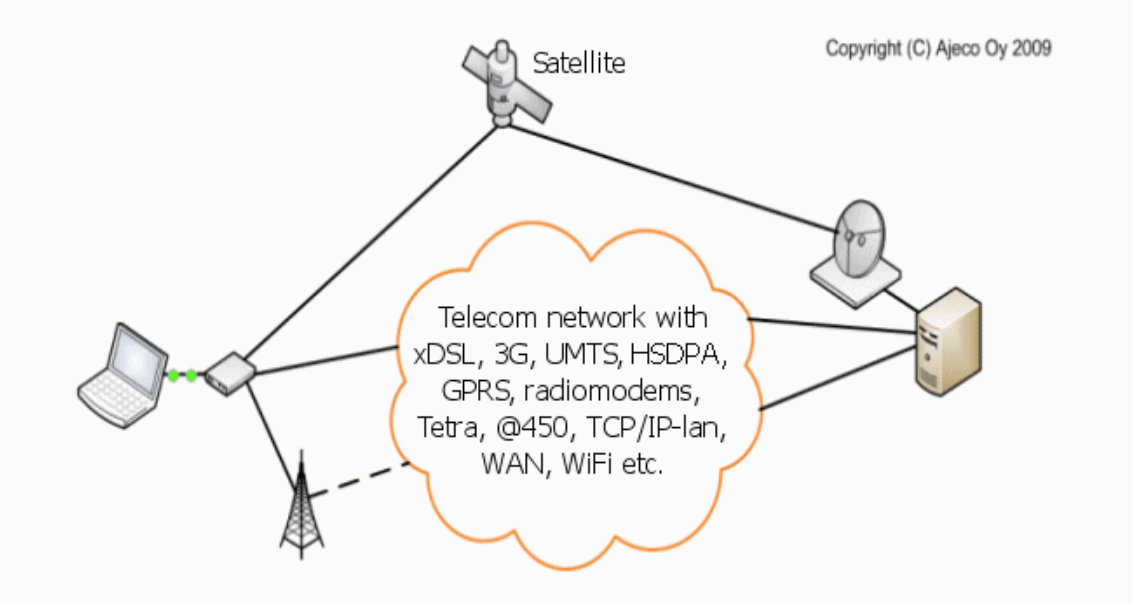
6) Satelliittiteknologialla on täydentävä rooli, kun maanpäällistä kattavuusaluetta ei ole.

TETRA/TETRAPOL on paras ratkaisu puheviestinnälle, koska sillä ei käytännössä katsoen ole kilpailijoita. Toisaalta TETRAn tarjoama tiedonsiirron kapasiteetti ei täytä vaatimuksia tulevaisuuden tarpeille, vaikka hitaasti siirrettävä data on varmaa ja toimii hyvin. Järjestelmää on mahdollista kehittää tulevaisuudessa laajakaistaiseksi, mutta se ei tule ratkaisemaan kaikkia ongelmakohtia. Suunnitteilla oleva TETRA Rel. 3 ei ole saatavilla ennen vuotta 2020 ja se sisältää jonkin asteista toteutukseen liittyvää epävarmuutta. Edellä mainitut asiat vaikuttavat siihen, että TETRA tarvitsee täydentäviä tiedonsiirtoteknologioita: nykypäivän ja tulevaisuuden valinnat sisältävät 3G-/HSPA-, 4G-/LTE-, WLAN- ja sateliittiteknologioihin perustuvaa viestintää. 450 MHz:n taajuusalueella hyvällä läpäisykyvllä toimiva NMT-teknologia, joka perustuu FLASH OFDM 450-teknologiaan, on yleisesti käytetty ratkaisu Suomessa. Tähän kuitenkin liittyy huolenaiheita, jos Flash OFDM-teknologiasta tulee vallitseva.

Ratkaisu millä taataan kriittisen viestinnän laatu on käyttää useita viestinnänreittejä, joita tarjoavat useat operaattorit. Viestintäkanavien datayhteyksien rinnakkaiskäyttö tekniikasta riippumatta ratkaisee monet ongelmat. Tekniikan edistämistä on mahdollistaa vaihoehtoiset viestintäkanavata. Suurin kysymys onkin se, että kuinka paljon pitäisi ja voisi yleisestä turvallisuudesta vastuussa olevat tahot luottaa kaupallisiin laajakaistapalveluihin? Mikä on julkisten verkkojen saatavuus kohdattaessa suuronnettomuus? Edellä mainitut kysymykset tarkoittavat sitä, että monikanavareitittimen tulee järkevästi ja jatkuvasti olla tietoinen käyttökelpoisista verkon resursseista ja kattavuudesta (TETRA, 3G, 4G, WiMAX, WLAN, jne.) Lisäski WLANin saatavuus tulisi ottaa huomioon.

5.4.4 Järjestelmän kuvaus

Kuvassa 8 esitellään yleiskuvaus DSiP-telemetriajärjestelmästä. Se kykenee reitittämään dataa minkä tahansa (IP ja ei IP) yhteyden kautta. Se toimii usean toimijan/operaattorin ympäristössä ja soveltaa seuraavia yhteyksiä: satelliitit, 3G, GRPS, UMTS, HDSPA, IP-verkko, TETRA, sarjayhteydet ja radiomodeemit.



Kuva 8: DSiP Telemetria-järjestelmä

5.4.5 Vankka ja turvallinen tietoliikenneyhteys

DSiP-protokolla tukee VPN-tunnelin jakamista useaan fyysiseen kanavaan ilman tutkimusongelmaa kuvaavassa kuvassa11 esitettyjä rajoitteita. Lisäksi se ratkaisee yhteensopivuusongelmia sekä fyysisellä että loogisella tasolla tarjoten modulaarisuutta, tietojen eheyttä, turvallisuutta ja monipuolisuutta niin pienille kuin erittäin suurille tietojärjestelmille. DSiP:in loogisia sääntöjä noudattamalla ja käyttämällä IP:n keinoja kuljettamiseen, niin eri toimittajien sovellukset, laitteet ja ohjelmistot voivat olla yhteydessä toisiinsa riippumattomasti. Näin ollen sovellukset voivat vastata sekä pyytää palveluksia ilman, että niiden erikseen tietää niiden fyysisistä toteutuksista.

5.4.6 Modulaarisuus

DSiP-telemetriajärjestelmä koostuu kolmesta elementistä: kauko-ohjaus paikka (remote site), tietoliikennejärjestelmä sekä komento- ja kontrollihuone. Jos joku kolmesta elementistä vaihtuu, niin se ei vaikuta muiden elementtien toimintaan.

5.4.7 Sovellukset

A. SCADA järjestelmät

DSiPiä hyödynnetään Suomen pääsähköverkon SCADA-järjestelmässä. Suurinta osaa Vattenfallin sähkönjakelusta Suomessa hallinnoidaan DSiP-järjestelmän avulla.

Sähköverkkojen katkoksia seurataan ja kontrolloidaan SCADA-järjestelmän avulla, joka toimii DSiP-järjestelmän avulla.

A. Rajavartiolaitoksen järjestelmät

Suomen rajavartiolaitos käyttää valvontakameroita kontrolloidakseen ja saadakseen telemetriatietoa jatkuvasti. Järjestelmä on tärkeä osa yleistä valvontaa ja SARilla on operatiivinen asema ja sen tulee pysyä toiminnassa 365/24/7. DSiP-järjestelmä mahdollistaa sen, että valvomot voidaan sijoittaa mihin tahansa haluttuun paikkaan. DSiP on samalla myös keskusviestinnän ratkaisu.

B. Ulkovalojen kontrollointi

Helsingin energia on käynnistänyt pilottikokeilun, jossa hyödynnetään Mobile Television Broadcast- (DVB-H), DSiP- ja GPRS-teknologiaa. Tämäkin ratkaisu perustuu DSiP-järjestelmään.

5.4.8 Keskustelu

DSiP:in avulla loppukäyttäjät voivat käyttää useampaa tietoliikenneyhteyttä kuin yhtenä toimivana vakaana kanavana. DSiP jakaa tietoliikenneresurssit eri laitteisto- ja ohjelmistomoduuleille ja reitittää tiedon automaattisesti vaihtoehtoisia kanavia pitkin, jos ensisijainen yhteys on rikki. Se tietää aina oikean lähettäjän ja vastaanottajan sekä käyttää vahvaa salausta ja aikaleimoja. DSiP tekee tietoliikenneyhteyksien kautta kulkevasta viestinnästä vakaampaa ja lisää tiedon tuvallisuutta.

Kun loppukäyttäjä käyttää DSiPiä, on hänellä tehostetut kontrollointimahdollisuudet valvoa tietovirtaa eli liikennettä:

- Priorisointi – ensin reititetään tärkeä tieto, vähemmän tärkeä myöhemmin
- Verkkojen ”timeouttien” kontrollointi - ei määrittelemättömiä viivästyksiä tai odotuksia
- Yhteyksien seuraaminen ja kontrollointi, DSiP tiedostaa reittien kunnon
- Huollon ja konfiguroinnin helppous
- Järjestelmässä on sisäänrakennettu ruuhkanhallinta
- Vähemmän tärkeä liikenne suodatetaan ja käytettävän tietoliikenneyhteyden kapasiteettiä alennetaan tarvittaessa

DSiP voi yhdistää ja käyttää sekä IP- että ei IP-pohjaisia tietoliikenneyhteyksiä ja tunneloida IP-liikennettä jonkin ei IP-yhteyden kautta. DSiP mahdollistaa tunneloinnin myös muille

protokolleille itsensä kautta. Kun on riippumaton yhdestä operaattorista tai mistään fyysisestä tiedonsiirron menetelmästä, loppukäyttäjät voivat jakaa operaattoreihin liittyvät riskit käyttämällä useammasta operaattorista koostuvaa verkkotopologiaa. DSiP ei ole raskas tai vaikea protokolla ja se voidaan upottaa useisiin laitteisiin ja alustoihin. DSiP sisältää seuraavat ominaisuudet:

- Ratkaisut liittyen tiedon eheyteen, turvallisuuteen ja autentikointiin
- Automaattinen uudelleenreititys backup-yhteyksien avulla
- Hallittavuus, kaistanleveyksien hallinta
- Standardoidut rajapinnat sovelluksille ja laitteistoille, ratkaisee monia yhteentoimivuusongelmia
- Skaalattavuus, järjestelmä on joustava sekä siihen on helppo lisätä uutta ja vanhaa laitteistoa sekä ohjelmistoa
- Täysin riippumaton fyysisistä tietoliikennemenetelmistä
- Reaaliaikainen tieto verkkotopologiasta – ei toivotut yhteydet hylätään
- Keskitetty autentikointi – verkon hallinta ja konfigurointi – työkalut järjestelmän hallintaan

Laurea-ammattikorkeakouluun on perustettu testiympäristö, jonka tarkoituksena on testata ja demonstroida monikanareititinjärjestelmä-ratkaisua luomalla erilaisia ongelmatilanteita, voidaan testata järjestelmän luotettavuutta ja vakautta. Tähänastiset tulokset ovat olleet rohkaisevia ja useat yhteydet näyttäytyvät kuin yhtenä vakaana tietoliikenneyhteytenä. Kun yksi yhteys epäonnistuu, DSiP löytää helposti uuden reitin. Se kuinka uusi yhteys on luotu, voidaan lukea logeista. Logit eivät ole kovinkaan kuvaavia, joten sen vuoksi kehitetään uusia visualisointi työkaluja (Holmström, Rajamäki ja Knuuttila 2010, 24-25,).

5.4.9 Johtopäätökset

Monikanavaisen viestinnän tarve on maailmanlaajuinen ja kasvava. DSiP-pohjainen ratkaisu mahdollistaa yleisien tietoliikennementelmien käyttämisen kriittisessä telemetriajärjestelmässä. Se mahdollistaa myös monenlaisen tietoliikenneresurssien hyödyntämisen: IP- tai EI IP-pohjainen tiedonsiirto, TETRA-verkko, sateliittiyhteyksien, sarjayhteyksien jne. ja nämä kaikki ovat yhdessä hallittavassa järjestelmässä.

6 Johtopäätökset ja keskustelu

Tämän tutkimuksen tavoitteena oli tutkia pelastus- ja turvallisuusviranomaistoiminnan kriittistä tietoliikennettä (mission critical communication) ja siihen liittyviä eritysvaatimuksia sekä tulevaisuuden haasteita. TETRA-pohjaiset VIRVE-viranomaisradioverkot eivät sellaisenaan vastaa nykypäivän ja tulevaisuuden vaatimuksia, mitä kriittiselle tietoliikenteelle

asetetaan. Työssä esiteltiin DSiP-järjestelmään perustuva monikanavareititys-pohjainen ratkaisu, jolla voitaisiin mahdollistaa vakaa ja turvallinen kriittinen viestintä kriittisten toimintojen suorittamiseen kentällä nykypäivänä ja tulevaisuudessa. Toinen tutkimuksessassa käsitelty aihe oli palvelupohjainen ohjelmistoarkkitehtuuri, jolla voitaisiin parantaa hälytysajoneuvojen tieto- ja viestinjärjestelmien yhteentoimivuutta. SOAn avulla pelastus- ja turvallisuusviranomaisten nykyisistä järjestelmistä voidaan koostaa uusi web-sovelluspalveluista koostuva kokonaisuus, joka voidaan monistaa myös like-minded maihin Eurooppaan. Sen avulla tieto ja palvelut olisivat saavutettavissa kaikille viranomaistahoille yhtenäisessä ICT-palveluiden kokonaisuudessa. Palvelut ja erilaisiin järjestelmiin tai sen osiin pääsy voitaisiin rajoittaa käyttäjäryhmäkohtaisesti alakohtaisesti esimerkiksi poliiseille ja pelastuslaitokselle. ICT-konseptin hallinnointi olisi keskitettyä.

Yksi ICT-Integraation päämääristä on tehostaa järjestelmien välistä yhteentoimivuutta tavoitteenaan lisätä:

- Kustannussäästöjä
- Tehokkuutta
- Järjestelmien skaalattavuutta
- Käyttötapojen yhtenäistämistä
- Tiedon saatavuutta
- Muuntautumiskykyä

Opinnäytetyössä käsitellyt aiheet liittyvät seuraaviin MOBI-hankkeen työpaketteihin ja täydentävät niihin liittyvää esitutkimustyötä:

- Työpaketti 2: Käyttäjän vaatimukset
- Työpaketti 4: Tietoliikenne
- Työpaketti 5: Sovellusten infrastruktuuri

6.1 Miksi valita DSiP?

DSiP-ratkaisu vastaisi MOBI-hankkeen kriittisen tietoliikenteeseen liittyviä vaatimuksia, joten se voisi olla hyvä valinta. Sen avulla järjestelmien välisestä tiedonsiirrosta saataisiin monikanavaista eli ominaisuuksiltaan turvallista ja vakaata, mitkä ovat elinehtona kriittiselle tietoliikenteelle. Sen hyödyntämiseen liittyviä edellytyksiä ja haasteita tulee kuitenkin tutkia vielä perusteellisemmin, sekä teoriittsella tasolla että laboratorio- ja kenttäympäristössä toteutettavissa tutkimuksissa.

6.2 Miksi valita palvelupohjainen ohjelmistoarkkitehtuuri?

SOA-ratkaisu valitaan useimmiten sen takia, että se parantaa organisaatioon muuntautumiskykyä, kun esimerkiksi yrityksen toiminnan kannalta tärkeät palvelut muuttuvat ja kehittyvät. Sen tarjoamia ominaisuuksia ovat:

- Uudelleenkäytön mahdollisuus
- Uusien liiketoimintaprosessien luomisen mahdollistaminen
- Olemassaolevien liiketoimintaprosessien tai palveluita tarjoavien sovelluksien muuntamisen mahdollistaminen
- Järjestelmään tehtävien muutoksien mahdollistaminen
- Palveluntarjoajia koskeviin muutoksiin mukautuminen
- Hallinnallisuuden parantaminen ja em. mainitut asiat voidaan tehdä turvallisesti

Liiketoiminnan kannalta tärkeitä järjestelmiä kehitetään jatkuvasti, että ne vastaisivat vaatimuksia tässä muuttuvassa maailmassa. Myös järjestelmien välisiä tiedonsiirron rajapintoja ja protokollia tulee kehittää saman tahtiin. Väestön turvaamisen ja pelastustoiminnan toimintaympäristö on muuttuva esimerkiksi toimintamallien kehittymisen sekä lakimuutosten takia. SOA mahdollistaisi tietojärjestelmien välisen joustavan ja järjestelmäriippumattoman vuorovaikutuksen ja palvelut sekä sovellukset voitaisiin määrittää käyttäjäryhmäkohtaisesti niin poliisiautoon, ambulanssiin ja paloautoon.

Useimmat Web-sovelluspalveluihin nykyisin perustuvat SOAn suunnittelumallit, kuten myös terveydenhuollon tietojärjestelmät. Suomen terveydenhuollon tietojärjestelmäarkkitehtuuriksi on valittu palvelupohjainen arkkitehtuuri. Aaltonen (2010, 23) kuvaa opinnätyetyössään Palokan terveyden huollolle toteutettua järjestelmäintegraatiota ja siitä ilmenee, että myös terveydenhuolto käyttäää VIRVEä esimerkiksi tilanteessa, jossa terveysasema ilmoittaa, ettei paikalla ole yhtään lääkäriä, jolloin alueen sairaankuljetukset saavat tiedon, ettei kyseiseen asemaan voi viedä välitöntä hoitoa tarvitsevia potilaita (Aaltonen 2010, 45). Mykkänen, Pöyhölä, Toroi, Riikkonen & Riekkinen ovat tulkinneet, että palvelupohjaisen arkkitehtuurin avulla terveydenhuolto tavoittelee mm. toiminnallisuuteen liittyvää joustavuutta, sovellusten liitettävyyden paranstamista, jo tehtyjen investointien hyödyntämistä, olemassa olevien sovellusten uudelleenkäyttöä ja järjestelmien käytettävyyden parantamista jne.

Koen, että SOA soveltuisi myös MOBI-hankkeessa toteutettavaan järjestelmien ja laitteston ICT-konseptin ohjelmistoarkkitehtuuriksi. Seuraavassa käyn läpi ratkaisun soveltamiseen liittyviä seikkoja.

Palvelupohjaiseen arkkitehtuurin ei voida ihan hetkessä siirtyä, vaan se tapahtuu pitkällä aikavälillä. Siitä koituvien etujen saavuttaminenkaan ei ole aina automaattista. Jos nykyiset järjestelmät ja palvelut sisältävät suurta määrää tietoa ja toiminnallisuutta, eivät ne ole yhtä uudelleenkäytettäviä kuin pieniä määriä palveluita ja järjestelmiä sisältävät kokonaisuudet. (Mykkänen, Pöyhölä, Toroi, Riikkonen & Riekkinen 2007, 22).

Sovellusten liitettävyyden mahdollistaminen perustuu rajapintoihin, riippumattomuuteen toteutustekniikoista (avoimet tekniikat), teknisiin ja sisällöllisiin standardeihin ja arkkitehtuurin joustavuuteen. Tämä kuitenkin edellyttää:

- Toiminallisuuden ja tiedollisen yhteensopivuutta
- Tekniikoiden yhdenmukaista soveltamista
- Standardien käyttöä ja sopimista
- Yhdenmukaisia toimintatapoja (kun integroidaan järjestelmiä palvelupohjaisesti)

Jos tavoitteena on hyödyntää aiemmin sovellettuja hyväksi havaittuja ratkaisuja, tulee huomioida se, että ne eivät saa vaikuttaa liikaa uusien ratkaisujen yksityiskohtiin. Vanhojen ratkaisujen hyödyntäminen uuden järjestelmän yhteydessä voi olla työlästä, kun niitä mukautetaan sisällöllisesti ulkoisiin määräyksiin tai standardeihin. Standardointi on myös avainasemassa, sillä vaikka tekniset ominaisuudet olisivatkin helposti liitettävissä eri alustoihin, niin toiminnallisten ominaisuuksien yhdistäminen vaatii kehitystyötä ja paikallista sopimista. Se tulee myös huomioda, että jos pieniä (palvelu)kokonaisuuksia on paljon, voi riskit ja poikkeamat jäädä havaitsematta helpommin. (Mykkänen ym. 2007, 10)

SOA-ratkaisulla voidaan parantaa myös järjestelmien käytettävyyttä, jota myös MOBI-hankkeessa tavoitellaan. Käytettävyydellä SOA-ratkaisussa tarkoitetaan sitä, että käyttäjien ei tarvise syöttää samaa tietoa useaan eri järjestelmään. Eli käyttäjän tarvitsee kirjautua vain kerran ja heille on saatavilla monen eri järjestelmän tiedot, jota ylläpidetään keskitetysti. Käyttäjille on saatavilla ajantasaista yhteisesti jaettua tietoa, toiminnallisuudet ja näkymä on yhdenmukainen kaikille, mutta sitä voidaan myös personoida eri käyttäjien tarpeiden mukaisesti. Jotta järjestelmiä voidaan muokata käyttäjätarpeiden mukaan vastaamaan ajoneuvokohtaisesti poliisiautoon, paloautoon ja pelastusauton tarpeita ja vaatimuksia, tulee palveluita voida vaihtaa ja niiden liitoksia muokata.

6.3 Oman työn osuus julkaisuissa

Tutkimukseeni liittyvä alustustyö käynnistyi jo syksyllä 2009, kun osallistuin Laurea-ammattikorkeakoulun järjestelmälle opintojaksolle ”Tietoverkkopalvelujen kehittäminen”. Opintojaksolla esiteltiin tässäkin tutkimuksessa esitelty MOBI-hanke. Opintojaksolla

ryhmätyönä toteutetussa tukimushankkeessa perehdyttiin MOBI-hankkeeseen ja tehtiin siihen liittyvää taustatutkimusta.

Syksyllä 2010 käynnistyi tutkimukseni orientaatiovaihe ja sain samalla kuulla, että pääsen edustamaan Laurea-ammattikorkeakoulua eräässä kansainvälisessä tietoliikenne-konferensissa, joka järjestettäisiin maaliskuussa 2011 Espanjan Kanariansaarilla. Sain tehtäväkseni esittää konferenssissa kaksi konferenssipaperia:

- ICT Integration of Public Protection and Disaster Relief (PPDR): Mobile Object Bus Interaction (MOBI) Research and Development Project
- DSiP Distributed Systems intercommunication Protocol - A Traffic Engineering Solution for Secure Multichannel Communication

Minun osuuteni konferenssipapereissa ja julkaisuissa liittyy MOBI-hankkeen vaatimusmäärittelyyn. Esittelin konferenssissa edellä mainitut konferenssipaperit kokonaisuudessaan. Molemmista konferenssipapreista kirjoitettiin myöhemmässä vaiheessa vielä tieteelliset artikkelit kahteen eri tieteelliseen lehteen. Kaikki paperit ja julkaisut löytyvät tämän työn liitteistä.

6.4 Tulevan tutkimustyön aiheita

Ennen kuin SOA-ratkaisua mietitään sovellettavan pelastus- ja turvallisuuviranomaisten uuteen ICT-konseptiin, tulee seuraavat toimenpiteet ainakin suorittaa (suluissa mihin toimenpiteellä tähdätään):

- Nykyiset palvelut ja järjestelmät määritellä ja priorisoida (vanhojen palveluiden/järjestelmien hyödyntäminen)
- Pitää tarkistaa nykyisten sovellusten liitännät (vanhojen palveluiden/järjestelmien hyödyntäminen)
- Erilaisiin tarpeisiin vaadittavien ratkaisujen ominaisuudet tulee tunnistaa ja määrittää, vaatimismäärittely (käytettävyyden parantaminen)
- Standardien käytöstä tulee sopia (sovellusten liitettävyys)
- Standardeista ja arkkitehtuurista tulee määrittää pelisäännöt (toiminnallinen joustavuus muutoksia varten)
- Rajapintamäärittely, miten palvelua voi käyttää eri tilanteissa (palveluiden ja komponenttien uudelleenkäyttö)

Jotta yhteentoimivasta järjestelmästä saadaan täysin tekniikkariippumaton, voidaan ratkaisun tavoittelussa käyttää mallipohjaista lähestymistapaa (esimerkiksi MDA). Näitä lähestymistapoja kannattaisi siis tutkia tarkemmin.

Tulee myös rakentaa abstrakti esityskerros, jolla piilotetaan tekniikat. Jos järjestelmästä halutaan eri tekniikoila ja alustoilla toteutettujen sovellusten ja palveluiden kokonaisuus, tulee luoda yksinkertainen perusmekanismi sovellusten liittämiseen. Tällä tavoin saavutetaan riippumattomuus palveluiden sijannista, toteutuksessa käytetyistä tekniikoista ja käyttöliittymässä kätevvistä laitteista. Tekniikoista tulee erottaa siirtoprotokollat laajennuksineen ja rajapintämäärittelyineen. (Mykkänen ym. 2007, 19)

Palveluarkkitehtuurilla ja Web-sovelluspalveluilla voidaan yhdistää uudella tavalla järjestelmäintegraatio sekä hajautettujen ja komponenttipohjaisten sovelluksien keskeiset elementit. Jos SOA-ratkaisuun päädytään, niin tulisi valita millä lähestysmistavalla se toteutetaan:

- Top-Down
- Bottom-Up
- Meet-In the Middle

Näitä menetelmiä kannattaa tutkia syvällisemmin, sillä niillä on vaikutusta projektitekijöihin ja sisäisen rakenteen ohjelmisto-ominaisuuksiin (Mykkänen ym. 2007, 30).

Jotta voitaisiin arvioida DSiPin soveltamista järjestelmien tietoliikenneratkaisuksi, tulee DSiP-tietoliikenneratkaisua tutkia syvällisemmin ja laboratorioympäristössä saaduista tuloksista voisi luoda oman julkaisunsa. Myös DSiPiä jo hyödyntäneisiin toimijoihin kannattaa olla yhteydessä ja kartoittaa siihen liittyneitä etuja ja ongelmakohteita. Koska Laurea-ammattikorkeakoulu on saanut myös oman demoajoneuvon käyttöönsä Poliisin tekniikkakeskukselta, niin se voitaisiin varustaa mahdollisimman pian saatavilla olevilla tarpeellisella laitteistolla, kuten monikanavareitittimellä, joka tukee DSiP-protokollaa ja tarvittavilla tietoliikenneyhteyksillä. Näin laboratorioympäristössä tehtyjä tutkimuksia voitaisiin toteuttaa myös kenttäympäristössä, jolloin saataisiin tutkimuksen kannalta tärkeää tietoa heti alkumetreillä.

Lähteet

Kirjat ja julkaisut

Ardissono, L., Petrone, G & Segnan, M. 2004. Conversational Approach to the Interaction with Web Services. Computational Intelligence, Vol. 20(4).

Baldini, G. 2010. Report of the workshop on “Interoperable communications for Safety and Security”, Publications Office of the European Union.

Bell, M. 2008. Introduction to Service-Oriented Modelling. 3. Wiley & Sons.

Fielding, R.T. 2000. Architectural Styles and the Design of Network-based Software Architectures. Doctoral dissertation, University of California, Irvine.

Hansen, M. 2007. SOA Using Java Web Services. Upper Saddle River. NJ: Pearson Education.

Haikala, I. & Märijärvi, J. 2004. Ohjelmistotuotanto, Hämeenlinna: Talentum Media Oy.

Hevner, A., March, S., Park, J. & Ram, S. 2004. Design science in information systems research, MIS Quarterly 28, No 1, 2004.

Holmström, J. Rajamäki, J. & Hult,T. 2011. “DSiP Distributed Systems intercommunication Protocol - A Traffic Engineering Solution for Secure Multichannel Communication” in Proc. 9th WSEAS International Conference on Applied Electromagnetics, Wireless and Optical Communications (ELECTROSCIENCE '11). Meloneras, Gran Canaria, Canary Islands Spain, March 24-26, 2011. Sivut 57-60.

Hult, T. & Rajamäki, J. 2011. ICT Integration of Public Protection and Disaster Relief (PPDR): Mobile Object Bus Interaction (MOBI) Research and Development Project”, in Proc. 9th WSEAS kansainvälinen konferenssi, Applied Electromagnetics, Wireless and Optical Communications (ELECTROSCIENCE '11). Meloneras, Gran Canaria, Kanarian saaret Espanja. 24.-26.3 .2011

Ilmavirta, V. 2010. “IPR management and industrial cooperation in the new Aalto University, the technology and innovation heart of the Otaniemi Science Park”, Intelektinės Nuosavybės Valdymas Mokslo Ir Studijų Institucijose: Jo Vaidmuo Technologijų Perdavimo Procese, Vilna, Lithuania.

Kivimäki, A. 2007. Wireless telecommunication stardardization processes – actors’ viewpoint, ACTA Univ. Oul. A 483, Oulu University Press.

Kruchten, P. 2004. The Rational Unified Process: An Introduction. Addison-Wesley Professional.

Litan, D & Mocanu, A-M. “Information systems integration, a new trend in business”, ”, in Proc. 9th WSEAS International Conference on Applied Electromagnetics, Wireless and Optical Communications(ELECTROSCIENCE '11), Meloneras, Gran Canaria, Canary Islands Spain. March 24-26, 2011, pp.250-256.

March, S. & Smith, G.1995. Design and natural science research on information technology, Decision Support Systems 15

Nunamaker, J., Chan, M. & Purdin, T. 1991. Systems Development in Information Systems Research, Journal of Management Information Systems I Winter 1990-91. Vol. 7, No. 3, 1991.

Nunamaker, J. 2010. Toward a Broader Vision of IS Research. 5/2010. Business & Information Systems Engineering.

Nurhonen, P. 2008. “POKE – GIS-based field command system for police”, presented at the Nordic Seminar of the Use of Geographic Information in Crises Management, May 19th 20th 2008, Bergen, Norway

Pohjonen, R. 2002. Tietojärjestelmien kehittäminen. Jyväskylä: Docendo Finland Oy.

Rajamäki, J & T. Villemson, T. 2009. Creating a service oriented architectural model for emergency vehicles, International Journal of Communications, Iss. 1, Vol. 3, 2009, pp.44-53

Rajamäki, J & Villemson, 2009. T. Designing Emergency Vehicle ICT Integration Solution, Proc. of the 3rd International Conference on Communications and Information Technology, Athens, Greece, Dec. 29-31, 2009, pp. 83-90

Rajamäki, J. Holmström, J & Knuuttila, J. 2010. Robust Mobile Multichannel Data Communication for Rescue and Law Enforcement Authorities, Proc. of the 17th Symposium on Communications and Vehicular Technology in the Benelux, Twente, The Netherlands Nov. 24-25, 2010.

Rajamäki , J.& Villemson, T. 2009. Creating a service oriented architectural model for emergency vehicles, International Journal of Communications, Iss. 1, Vol. 3, 2009. Sivut 44-53.

Rajamäki , J.& Villemson, T. 2009, Designing Emergency Vehicle ICT Integration Solution, Proc. of the 3rd International Conference on Communications and Information Technology, Atheena, Kreikka, Dec. 29. Sivut. 83-90.

Tumin, S. & Encheva, S. 2011. A brief look at Web architecting. in Proc. 9th WSEAS International Conference on Applied Electromagnetics, Wireless and Optical Communications (ELECTROSCIENCE '11),Meloneras, Gran Canaria, Canary Islands Spain, March 24-26, 2011. Sivut 245-249.

VanAken, J.2004. Management research based on the paradigm of the design sciences: The quest for field-tested and grounded technological rules, Journal of Management Studies 41, No, 2 2004.

Vilppunen, H. 2006. “TETRA data services & applications”, presented at the TETRA Congress, Warsaw,Poland.

Vilppunen, H.“TETRA data services & applications”, presented at the TETRA Congress, June 13th -14th 2006, Warsaw, Poland. [

Sähköiset lähteet

Ajeco Oy. 2009. The DSiP-solution with multichannel routing capability. Viitattu 19.5.2012. http://www.ajeco.fi/product1.html

Aronsson, H. 2012. Kriittinen kommunikaatio: Trendejä ja Appseja. Viitattu 18.5.2012. http://www.erillisverkot.fi/public/files/Tetra%20ominaisuudet%20ja%20standardointiprosessi_Aronsson.pdf

BSi. 2012. What is a standard? Viitattu 3.6.2012. http://www.bsigroup.com/en/standards-and-publications/about-standards/what-is-a-standard/

Berners-Lee, T. 1998, Uniform Resource Identifiers (URI). Viitattu 19.5.2012 http://tools.ietf.org/html/rfc2396

Cosafe. 2012. Suuronnettomuuksiin varatuminen harvaanasutuilla alueilla. Viitattu 19.5.2012 http://www.cosafe.eu/PDF/FIN_booklet_major_incidents%20%28FINAL%29.pdf

EJN. 2012. Viitattu 19.5.2012. http://www.ejn-crimjust.europa.eu/ejn/EJN_StaticPage.aspx?Bread=2.

Eur-Lex. 2003. Maailman radioviestintäkonferenssi 2003 (WRC-03) /* KOM/2003/0183 lopull. */ Viitattu 20.5.2012
http://eur-lex.europa.eu/LexUriServ/LexUriServ.do?uri=CELEX:52003DC0183:FI:HTML

Euroopan unioni. 2012. Viitattu 19.5.2012.
http://europa.eu/agencies/regulatory_agencies_bodies/pol_agencies/eurojust/index_fi.htm.

Europol. 2012. Viitattu 19.5.2012
https://www.europol.europa.eu/content/page/mandate-119.

Interpol. 2012. Viitattu 19.5.2012.
http://europa.eu/agencies/regulatory_agencies_bodies/pol_agencies/eurojust/index_fi.htm.

Mykkänen, J. Pöyhölä, A. Toroi, T. Riikkonen & P. Riekkinen, A. 2007. Palveluarkkitehtuurin soveltaminen terveydenhuollossa. Viitattu 21.5.2012.
http://www.serapi.fi/menetelmat/WS-opas_osa1_final.pdf

Niemenkari, A. "Integrated border management – case Finland", Euromed migration II project,23 FEB 2010, Rome, Italy, available:
http://www.euromedmigration.eu/e1152/e1483/e2556/e2585/e2641/presen92NiemenkarM2s21feb2325rome2010.pdf

Poliisi. 2012. Viitattu 19.5.2012
http://www.poliisi.fi/krp.

Rantama, M. & Junttila, K. 2011. Pelastustoimen langattoman tiedonsiirron tarpeet ja toteutusmahdollisuudet tulavaisuudessa. Pelastusopisto. ISBN: 978-952-5905-06-9
http://www.intermin.fi/pelastus/images.nsf/files/F596094E0B96B2C6C22578630042D86F/$file/Pelti%20loppuraportti%20liitteineen.pdf

Pelastustoimen strategia 2025. Sisäasiainministeriö. 2012. Viitattu 3.5.2012.
http://www.intermin.fi/intermin/biblio.nsf/1360D4E89C5D0E8EC22579C7004D295D/$file/082012.pdf

Tekes, 2012. Viitattu 3.4.2012. Safety and Security Programme Projects.
http://www.tekes.fi/programmes/Turvallisuus/Projects

TCCA. 2012. Kriittinen kommunikaatio: Trendejä ja Appseja. Viitattu 17.5.2012.
http://www.erillisverkot.fi/public/files/Tetra%20ominaisuudet%20ja%20standardointiprosessi_Aronsson.pdf.

Tietotekniikan termitalkoot, 2012. Web-sovelluspalvelu. Viitattu 18.5.2012.
http://www.tsk.fi/tsk/termitalkoot/hakemistot-267.html?page=get_id&id=ID0176&vocabulary_code=TSKTT.

W3C, 2000. Simple Object Access Protocol. Viitattu 19.5.2012.
http://www.w3.org/TR/2000/NOTE-SOAP-20000508/

W3C, 2012. About W3C. Viitattu 18.5.2012
http://www.w3.org/Consortium/

W3C, 2012. Extensibile Markup Language. Viitattu 18.5.2012.
http://www.w3.org/XML/

Julkaisemattomat lähteet

Aaltonen, E. 2010. Jyväskylän ammattikorkeakoulu. ICT-järjestelmien integraatio terveydenhuollossa. http://urn.fi/URN:NBN:fi:amk-201005098454

EUROSUR. Communication of 13 February 2008 from the Commission to the European Parliament, theCouncil, the European Economic and Social Committee and the Committee of the Regions: Examining the creation of a European border surveillance system (EUROSUR) [COM(2008)68 final].

Kuviot

Kuvat

Taulukot

Liitteet

Liite 1: Julkaisu 1, ICT Integration of Public Protection and Disaster Relief (PPDR): Mobile Object Bus Interaction (MOBI) Research and Development

Liite 2: Julkaisu 2, ICT integration of public protection and disaster relief: services for fire and rescue personnel

Liite 3: Julkaisu 3, DSiP Distributed Systems intercommunication Protocol - A Traffic Engineering Solution for Secure Multichannel Communication

Liite 4: Julkaisu 4, The future solutions and technologies of public safety communications - DSiP traffic engineering solution for secure multichannel communication

ICT Integration of Public Protection and Disaster Relief (PPDR): Mobile Object Bus Interaction (MOBI) Research and Development Project

TAINA HULT & JYRI RAJAMÄKI
Laurea SID Leppävaara
Laurea University of Applied Sciences
Vanha maantie 9, FI-02650 Espoo
FINLAND
taina.hult@laurea.fi http://laureasid.com

Abstract: - In field operations of Public Protection and Disaster Relief (PPDR) services, vehicles are the most important tools. Today, the vehicles are increasingly dependent on ICT systems. PPDR responder's need is to enhance mission critical voice with broadband data. Command and control applications aboard a vehicle are commonplace. There is a need to ease situational awareness and decision making by utilizing sensor information, such as satellite or network based position information, living video images. However, each countries and even every single user organization is developing their own solutions according to their legislation and requirements, because uniform standards are missing. The Mobile Object Bus Interaction (MOBI) research project is a kick off for creating a common international ICT infrastructure for all PPDR vehicles. MOBI researches possibilities to further develop and integrate ICT systems, applications and services of PPDR vehicles. MOBI aims at starting development of standards used by like-minded countries and possibly with the European Commission, the European Law Enforcement Agency EUROPOL and the European Agency for the Management of Operational Cooperation at the External Borders FRONTEX.

Key-Words: - Data communications, ICT**,** Low enforcement, Professional mobile radio, Public safety, Search and rescue, Systems integration

1 Introduction

Public Protection and Disaster Relief (PPDR) services such as law enforcement, fire fighting, emergency medical, and disaster recovery services, bring value to society by creating a stable and secure environment. The protection to be ensured by PPDR responders covers people and the environment and property. It addresses a large number of threats both natural and man-made. One important task of PPDR services is to deal with emergency and surveillance situations on land, sea and air. The most important part of this work is done in the field, so all the tools must match the needs accordingly. When working in the field, vehicles with its devices, systems and services are the most important tools, in which occupational safety, efficiency and ergonomics must be taken into account. Vehicles used and devices installed, must be robust, secure and suitable for very demanding and variable conditions.

The amount of technical devices, applications and services in PPDR vehicles has been increasing during the past few decades. This progression has also increased the volume of different user interfaces and generated new problems, e.g. vehicle airbags have less room to fill. Also technical problems especially with power consumption and cabling have been reported.

Another problem is the poor documentation of applied solutions because there has been no standardization in the field, partially because of the diversity of equipment suppliers. E.g. in fire and rescue service field in Finland, the country is divided into multiple regions, where each and one of those regions have their own fire and rescue departments responsible to deliver fire and rescue services to the public. As the technology develops and becomes more utilized in everyday life, so it does in fire and rescue environment. This will develop services, make them more efficient and especially help the process of the rescue services. Unfortunately so far, there has been no standardization in the equipment and system side of these services. The number of equipment suppliers is large and complex. Yearly delivery volumes have not been helping development of standardization. The aforementioned presents needs for new business models [1], [2].

With an increased number of applications also the amount of transferred data has exploded. In the field, wireless communications' role is to support

ISBN: 978-960-474-286-8

the mobility of first time responders by providing continuous connectivity among responders and with the headquarters. The support includes: maintain voice communication to coordinate the relief efforts for the resolution of the crisis; creation and distribution of a common operational picture among all the responsible parties; collect and distribute data on the operational context or the environment from sensors; retrieve data from central repositories (e.g. building plans, inventory data) to support their activity; support the tracking and tracing of the supply chain of goods and materials needed in the response and recovery phases of a crisis. [3]

In Europe, many dedicated secure network infrastructures have been built and deployed to provide the necessary capabilities for PPDR organizations. These networks, generally realised by TETRA/TETRAPOL are narrowband. Lack of broadband connectivity of wireless communications for existing and future PPDR applications is a real problem [3]. Many new applications require wideband data rates usually provided by commercial operators. For that reason, separate parallel data communication channels are needed. A robust multichannel data communication concept that is independent of single operators, is presented in [4].

The European Commission, the European Law Enforcement Agency EUROPOL and the European Agency for the Management of Operational Cooperation at the External Borders FRONTEX have recognized that lack of interoperability limits the effectiveness of PPDR practitioners in actual operations, and an evident lack of understanding as to whether these limitations arose from technology, operational procedures, gaps in procurement or research [3]. A scientific proven fact is that standardization strongly affects businesses that develop and sell technologies and technology-based products and services; standards are one main enabler for fast growth [5]. For improving interoperability, standardization development with like-minded countries should be started.

Chapter 2 of this paper illustrates the operating environment especially from end-users' perspective. Chapter 3 presents the research, development and innovation programme 'Mobile Object Bus Interaction (MOBI)' being made up of two industrial projects and a research project. Chapter 4 describes the research project in more detailed. Chapter 5 presents the needs for further research and discussions.

2 ICT Systems of PPDR Services

PPDR field operations are increasingly dependent on ICT systems, especially on wireless and mobile communications. In PPDR vehicles, data communication is mission critical. It is necessary to ensure that information and "on-demand" services provided by these technologies are delivered reliably and securely through one or more of the recently developed wireless architectures.

2.1 End-user Perspective

According to [3], the main effort in developing ICT systems of PPDR should be to standardize the interoperability architecture for applications (e.g. command and control) and infrastructure (e.g. interface gateways, mobile unit). Usability is also a main concern as many solutions are not ergonomic or easy to adapt to existing vehicles or infrastructures. The following recommendations are provided [3]: (1) Inter-System Interface (ISI) is an open interface standard used to connect two TETRA networks together. A joint ISI development should be started with roaming as a primary objective. (2) Harmonized frequency bands for PPDR broadband data services should be investigated and identified. (3) There is the need to conduct a feasibility study of TETRA Enhanced Data Service (TEDS) services to confirm if they are able to address the needs of PPDR organizations in Europe. (4) PPDR broadband data network needs standardized and harmonized technologies.

3 MOBI Programme

The target of a Finnish national research, development and innovation programme 'Mobile Object Bus Interaction (MOBI)' is to create a common ICT hardware and software infrastructure for all emergency vehicles. This infrastructure includes devices for voice and data communications, computers, screens, printers, antennas and cablings. Additional, the interlinking with factory-equipped vehicles' ICT systems is research.

The programme consists of two industrial projects and a research project that generates research data for industrial projects by researching and documenting the needs and requirements of the users, power generating and supplying and specifying the existing solutions. One industrial project, led by Cassidian Finland Ltd., develops vehicle installed professional mobile radio concept for law enforcement and fire and rescue operations. Another industrial project, led by Insta DefSec Ltd., develops secure software services. The project utilizes the results of the related research project and aims to develop product concepts which have potential in both domestic and export markets.

ISBN: 978-960-474-286-8

Additionally, Insta DefSec Ltd. will further develop its business model in order to be able utilize growth potential of the product concepts. [5]

This research, development and innovation work starts in Finland, because of Finland has

- evidences of success of developing wireless telecommunications, e.g. 1G - Nordic Mobile Telephone (NMM), 2G – Global System Mobile (GSM), 3G – Universal Mobile Telecommunications System (UMTS) [6]
- the world's first nationwide TErrestrial TRunked RAdio (TETRA) network - the "Viranomaisradioverkko" or VIRVE network - commonly used by Finnish authorities. The VIRVE network is used by the emergency and fire and rescue services, the police, the Finnish Defence Forces, the Frontier Guard, social and health services, the Finnish Maritime Administration and different government departments. Today, the VIRVE network enables the world's best interoperability between different PPDR services.
- extensive experiences in field command systems, e.g. the Police Field Command System POKE has been in operational use since 2006 [7], [8]. From the base of the POKE system, a dedicated system 'PEKE' for fire and rescue work has been developed.
- well operating and organized co-operations between authorities at different levels, e.g. national police – customs – border guard cooperation [9]
- innovation success supporting atmosphere, e.g. Finnish companies are doing R&D with universities and with their competitors, with popular slogan: "Finland is a club, rather than a country" [10].

4 MOBI Research Project

Amount of different technical systems in emergency vehicles has been growing significantly which has caused problems for example in vehicles safety systems and power supply. Documentation of existing solutions varies and there are no standards in the business. Research project generates research data for industrial projects by researching and documenting the needs and requirements of the users, power generating and supplying and specifying the existing solutions. Based on the research a demo vehicle with working ICT-integration will be made. A commercial product including commercializing plans, to be offered in European market is going to be the final outcome of the project. This three-year project started in September 2010.

4.1 Consortium and Founding

The project consortium, led by Laurea University of Applied Sciences, consists of three research institutes, two industrial partners, three small and medium size enterprises (SMEs), several end-user organizations and a public financier; Tekes – the Finnish Funding Agency for Technology and Innovation. The budget of MOBI research projects is 800 000 € and Table 1 shows funding shares.

Table 1 Funding of MOBI Research Project

Participant	€	%
Tekes	480 000	60
Research institutes	108 000	13
Industrial partners	110 000	14
SMEs	63 000	8
End-users	39 000	5
TOTAL	800 000	100

4.2 Work Packages

Fig. 1 shows MOBI's Work Packages (WPs). The project starts by researching user requirements (WP2). The common ICT infrastructure is composed of four layers and their standardised interfaces: vehicle ICT infrastructure and power generation (WP3), data communications (WP4), common software infrastructure (WP5), and ICT services for PPDR practitioners (WP6). Also, a demonstration vehicle is equipped (WP7), new business models studied (WP8) and coordination taken care of (WP1).

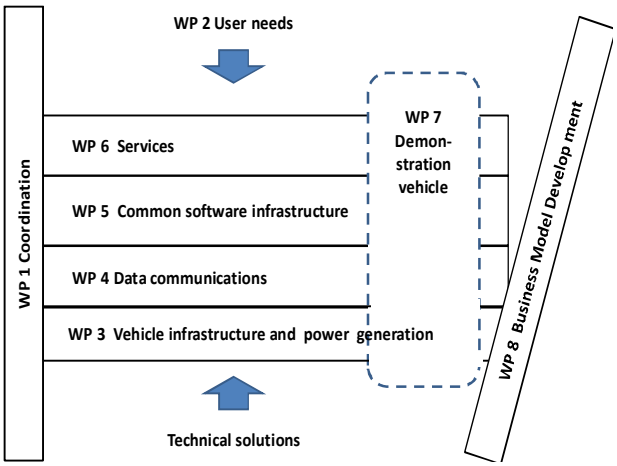


Fig. 1 Work Packages of MOBI Project

4.2.1 Coordination

WP1 includes tasks considering project management, which main objective is to ensure that MOBI research project generates research data for the parallel corporate projects. This work package includes cooperation and exchange of information with other relevant projects, such as MOBI-projects parallel corporate projects, EU FP7/SEC Project

ISBN: 978-960-474-286-8

AIRBorne information for Emergency situation Awareness and Monitoring (AIRBEAM), EU FP7/SEC Project Policy-oriented marine Environmental Research in the Southern EUropean Seas (PERSEUS) and SCientific innOvation Product concept (SCOPE) .

Work package 1 uses Wise Guys-panels that are also common sessions for all the work packages to present what has been done and to plan the future actions. Results from other work packages will be brought to the Wise Guys-panels to be presented. Wise Guys-panels will be scheduled so that they can be arranged before the deadlines of other work packages.

4.2.2 User requirements

In this work package the present electrical- and ICT-systems are being surveyed (for example in case of police vehicles: power supply technologies, radio equipment, video equipment, radars and other speed monitoring devices, IT-workstations, printers, biometric devices, navigation and tracking devices). User and authority requirements for these systems and devices are also being surveyed. Former studies will be used as a source for information.

In this work package administrative and operative systems will be identified and priority and manageability requirements for these systems will be defined. Different authority adoptions (e-adoption, RTTE- and EMC-directives) required for different systems will also be researched. This work package delivers an updated description of the IT-solutions of Finnish emergency vehicles. In this description the requirements are being organized to be used by the companies involved in this research project.

4.2.3 Vehicles infrastructure and power supply

Power consumption is one of the biggest challenges of emergency vehicles and their ICT-systems. Number of computers needed will be optimized and power consumption of the other electrical devices in different operational modes will be researched in this work package. Different kinds of power generating possibilities, such as fuel cells, will also be researched. How could ensuring power supply, power control and sleep-mode control be done in a consistent manner will be researched in this work package.

4.2.4 Data communications

The capability of exchanging information (e.g. voice or data) is essential to improve the coordination of PPDR officers during their operations; especially, wireless communications are important in the response and mitigation of emergency crisis to support the mobility of first responders [3].

Data communications of PPDR vehicles can be divided into three levels. The first level is represented by long distance communications e.g. between vehicles and command and control rooms often realized by narrow band TETRA or TETRAPOL systems, but also e.g. @450, 2G, 3G, 4G and WiMAX are used. Also, FM radio and GPS systems could be referred to, as long distance communications. Normally, the media used depends on the application or is selected manually by the user.

The second level is represented by local network data communication including e.g. CAN, LAN, WLAN and wide band ad-hoc –communications between vehicles. The third level is the accessory communications of different data systems used in vehicles.

The ICT-solutions of PPDR must be robust and easy to install. Misinterpretations or connectivity failures can cause loss of life or delay the resolution of the crisis. Information security and reliability must be properly considered and taken care of. Different encryption methods of different systems cause their own challenges. In addition, different organizations have their own requirements for arranging the information security of their vehicles' systems.

Research of the requirements to be set for data bus and the planning of on-line systems' basic and back-up connections and connections used in off-line systems synchronizing will be carried out in this work package. Different antennas and cabling solutions will also be researched, considering placement, possibilities of interference and possibility of joint cabling.

4.2.5 Common software infrastructure

In this work package the IT-integration of emergency vehicle will be planned. Overview of the vehicle's IT-architecture both in online and off-line situations will be created. In this matter the security of the data in local storing and classified data that can be replicated must be taken into consideration. When planning the vehicle, safety matters must also be considered (such as functioning of vehicles safety devices), which will be one of the major improvements that the integration of systems will bring. Results of the work package 2 will be used as a base for planning of architecture and user interfaces.

The objective of this work package is a description of the architecture which includes description of which components the system

ISBN: 978-960-474-286-8

consists of and how it is being placed. This description consists of application architecture, IT-architecture, technical architecture and layout diagram –levels. There will also be a interface definition which describes applications' connectivity to the system. Light-control systems available in present markets will also be studied.

4.2.6 Services

The main applications and the services they offer for each end-user group (e.g. video surveillance and speed radars for police) will be chosen for further research. The objective of this work package is to define the emergency vehicles' main applications' functionality and to plan the technical planning of these main applications.

4.2.7 Equipping of demonstration vehicle

Industrial participants and end-user organizations are able to test chosen solutions in research environment. Test vehicle built by industrial participants of the project will act as testing environment for the representatives of end-user organizations. A demo-vehicle will be made as cooperation between different participants. Demo-vehicle will be made according to one user-group's requirements meaning that the vehicle will not be a combination of for example police vehicle and rescue service's vehicle. This vehicle will be made for one authority only.

Field testing for the demo-vehicle will be carried out either in Police College of Finland or in Rescue College of Finland.

4.2.8 Business models

Development of ICT-concept is significantly expensive so access to the international markets is desirable. There are good chances to develop the industry in Finland because cooperation between different authorities is efficient and highly developed. The problems mentioned above are similar in all countries: new IT-equipment must be added to authorities' vehicles. A much needed standardization has not happened in the industry. The purpose is to create an international standard Industry's de facto and/or de jure) to the industry, which makes cooperation between authorities easier and more efficient. Objective is to make the final result suitable also for others than just authorities. For example some industry companies, private security services and fleet management-services could have the need for a moving office-type of vehicle solution. These kinds of needs will be considered especially when developing commercial solutions.

Solutions for question: how a developed solution or part of it could be sold as compatible set, will be studied in the work package of business models. Industry's market and volumes, international and national and Public-Private partnerships' regulation will be studied in this work pack-age. One of the main tasks is to monitor the development of markets in this industry in the EU-area. There is an attempt to create scenarios from the business models which will help one to find out who should be responsible for integration work and further equipment acquisition and administration. A Finnish model to act as a base for creating RFQ-documents will be developed and documented in this work package. Development in EU-area (for example EUROSUR) as well as markets' and regulation's (for example outer borders' exit-entry-system which creates new challenges for identification of persons and which is currently being processed by the Parliament of EU) development will be monitored in this work package. Laurea has become a member of Centre for Identification Research, CITeR, as a partner of the University of Arizona and any development in the field of CITeR will be monitored also.

This work package produces new business models for security and safety industry to be used, new concepts, business plan and possibly an FP7-application. User requirement definition will be done in Finland and market research internationally.

4.3 Requirement Analysis

This phase determines and defines what the system should do. Requirement Analysis will be create from results of requirement research. The goal is to recognize requirements and to do functional specification for the system. Requirements will be divided in two groups: Functional Requirements and Non-functional Requirements. These requirements define operations, functions and constraints of the system. [11]-[13]

Functional Requirements define the expectations of its behavior or functions. It describes how it works, how it will communicate with other systems, what kind of stakeholders or users there are, how stakeholders and users can use it and how do they work with it. Generally these are the actions that this system must be able to perform. Non-functional requirements also known as quality requirements define features and constraints of the system. The requirements define nonfunctional quality attributes for the system like usability, reliability, performance and supportability. [11]-[13]

The purpose of this work package processes is to assure that the project outcome meets the expectations of the customers and other (internal or

external) stakeholders. After Requirement Analysis process there will be naturally design process. The purpose of these two processes is to translate the requirements into a specification that describes how to implement the system. [11]-[13]

5 Discussions

Regulations and standardization play an important role in applying the results of research to the market and to PPDR end-users. The on-going planning of European external border surveillance system (EUROSUR) [14] and EU´s enhanced powers in the field of internal security by the Treaty of Lisboa pace the way for further standardization efforts. Finland has one nation-wide TETRA network used by various PPDR organizations. As a consequence, there is full domestic interoperability. Finland has evidences of developing wireless communications standards and well operating and organized co-operations between authorities at different levels. Here, a prototyping environment with de facto standards could be made.

To implement and manage a prototyping environment that can develop and prove standards for interoperability for the 'meaning' of data that enable information to be shared between security providers, both within and between nations. The prototyping environment should provide for candidate operational scenarios to be synthesised (for example a trans-border incident) emulating the data flows between systems and operators, and so show that information exchange retains consistent meaning as well as timeliness when portrayed in different systems. The aim would be to provide a focus for researchers, system designers, information system operators and security front line operators to develop and validate semantics, syntax and meta-data so that such standards can be rolled out by security providers with confidence.

References:

[1] J. Rajamäki and T. Villemson, Creating a service oriented architectural model for emergency vehicles, *International Journal of Communications*, Iss. 1, Vol. 3, 2009, pp. 44-53.

[2] J. Rajamäki and T. Villemson, Designing Emergency Vehicle ICT Integration Solution, *Proc. of the 3rd International Conference on Communications and Information Technology*, Athens, Greece, Dec. 29-31, 2009, pp. 83-90.

[3] G. Baldini, *Report of the workshop on "Interoperable communications for Safety and Security"*, Publications Office of the European Union, 2010.

[4] J. Rajamäki, J. Holmström and J. Knuuttila, Robust Mobile Multichannel Data Communication for Rescue and Law Enforcement Authorities, *Proc. of the 17th Symposium on Communications and Vehicular Technology in the Benelux*, ,Twente, The Netherlands Nov. 24-25, 2010.

[5] Tekes, Safety and Security Programme Projects http://www.tekes.fi/programmes/Turvallisuus/ Projects

[6] A. Kivimäki, *Wireless telecommunication stardardization processes – actors' viewpoint*, ACTA Univ. Oul. A 483, Oulu University Press, 2007.

[7] H. Vilppunen, "TETRA data services & applications", presented at the TETRA Congress, June 13th -14th 2006, Warsaw, Poland.

[8] P. Nurhonen, "POKE – GIS-based field command system for police", presented at the Nordic Seminar of the Use of Geographic Information in Crises Management, May 19th – 20th 2008, Bergen, Norway.

[9] A. Niemenkari, "Integrated border management – case Finland", Euromed migration II project, 23 FEB 2010, Rome, Italy, available: http://www.euromed-migration.eu/e1152/e1483/e2556/e2585/e2641/presen92NiemenkarM2s21feb2325rome2010.pdf

[10] V. Ilmavirta, "IPR management and industrial cooperation in the new Aalto University, the technology and innovation heart of the Otaniemi Science Park", Intelektinės Nuosavybės Valdymas Mokslo Ir Studijų Institucijose: Jo Vaidmuo Technologijų Perdavimo Procese, Vilna, Lithuania, 2.3.2010.

[11] R. Pohjonen, *Tietojärjestelmien kehittäminen*. Jyväskylä: Docendo Finland Oy, 2002.

[12] P. Kruchten, *The Rational Unified Process: An Introduction,* 2004.

[13] I. Haikala and J. Märijärvi, *Ohjelmistotuotanto,* Hämeenlinna: Talentum Media Oy, 2004.

[14] Communication of 13 February 2008 from the Commission to the European Parliament, the Council, the European Economic and Social Committee and the Committee of the Regions: Examining the creation of a European border surveillance system (EUROSUR) [COM(2008) 68 final].

ICT integration of public protection and disaster relief: services for fire and rescue personnel

Jyri Rajamäki, Taina Hult and Paulinus Ofem

***Abstract*—**In field operations of Public Protection and Disaster Relief (PPDR) services, vehicles are the most important tools. Today, the vehicles are increasingly dependent on ICT systems. PPDR responder's need is to enhance mission critical voice with broadband data. Command and control applications aboard a vehicle are commonplace. There is a need to ease situational awareness and decision making by utilizing sensor information, such as satellite or network based position information, living video images. However, each country and even every single user organization is developing their own solutions according to their legislation and requirements, because uniform standards are missing. The Mobile Object Bus Interaction (MOBI) research project is a kick off for creating a common international ICT infrastructure for all PPDR vehicles. MOBI researches possibilities to further develop and integrate ICT systems, applications and services of PPDR vehicles. MOBI aims at starting the development of standards used by like-minded countries and possibly with the European Commission, the European Law Enforcement Agency EUROPOL and the European Agency for the Management of Operational Cooperation at the External Borders FRONTEX. This paper concentrates on services for fire and rescue personnel and researches the Finnish fire and rescue environment and the ICT systems used in action. PPDR services constitute a distributed system. Software development paradigms which have been used in the past for distributed systems have inherent limitations that do not support integration, interoperability and reusability. To contribute towards resolving the well known issues of integration and interoperability between ICT systems in emergency vehicles which often work in a collaborative fashion, a preliminary investigation of the applicability of SOA and Web Services Standards towards the optimization of ICT systems and services provided by emergency vehicles is presented.

***Keywords*—**Data communications, Fire and rescue services, ICT, Professional mobile radio, Public safety, Search and rescue, Service-oriented architecture, Systems integration, Web services

I. Introduction

PUBLIC Protection and Disaster Relief (PPDR) services such as law enforcement, fire fighting, emergency medical, and disaster recovery services, bring value to society by creating a stable and secure environment. The protection to be ensured by PPDR responders covers people, the environment and property. It addresses a large number of threats both natural and man-made. One important task of PPDR services is to deal with emergency and surveillance situations on land, sea and air. The most important part of this work is done in the field, so all the tools must match the needs accordingly. When working in the field, vehicles with their devices, systems and the services they provide are the most important tools, in which occupational safety, efficiency and ergonomics must be taken into account. The vehicles used and devices installed must be robust, secure and suitable for very demanding and variable conditions. [1]

The amount of technical devices, applications and services in PPDR vehicles has increased during the past few decades. This progression has also increased the volume of different user interfaces and generated new problems, e.g. vehicle airbags have less room to fill. Also technical problems especially with power consumption and cabling have been reported.

Another problem is the poor documentation of applied solutions because there has been no standardization in the field. This is partially because of the diversity in equipments and the vendors who supply them. The diversity in the equipment supplied raises issues of system integration and interoperability between collaborating units such as the emergency control unit or the command control with the emergency vehicles in the field. The issue of interoperability also negatively impacts the administration of the emergency services since services are observed to be managed on national regional and local basis. Information inter-change is therefore critical. For instance, in fire and rescue service field in Finland, the country is divided into multiple regions, where each and one of those regions have their own fire and rescue departments responsible to deliver fire and rescue services to the public. As the technology develops and becomes more utilized in everyday life, so it does in fire and rescue environment. These technology advancements would help to develop services, make them more efficient and especially help the rescue services unit to better deliver effective and efficient service. Unfortunately so far, there has been no standardization in the equipment and systems utilized by these emergency service vehicles. The number of equipment suppliers is large and complex. Yearly delivery volumes have not been helping development of standardization. The aforementioned problems present the need for new business models [2], [3].

Manuscript received April 23, 2011. This work was supported in part by Tekes – the Finnish Funding Agency for Technology and Innovation – as a part of the research project 40350/10 Mobile Object Bus Interaction (MOBI).

J. Rajamäki and T. Hult are with the Laurea SID Leppävaara, Laurea University of Applied Sciences, Vanha maantie 9, FI-02650 Espoo, Finland. (e-mail: jyri.rajamaki@laurea.fi, taina.hult@laurea.fi).

Paulinus Ofem is post-graduate student at School of Computing, University of the West of Scotland, Paisley, PA1 2BE, Scotland, UK. (e-mail: paulinusofem@gmail.com).

More so, with the increased number of applications, the amount of transferred data has exploded. In the field, wireless communications' role is to support the mobility of first time responders by providing continuous connectivity among responders and with the headquarters. The support includes: maintain voice communication to coordinate the relief efforts for the resolution of the crisis; creation and distribution of a common operational picture among all the responsible parties; collect and distribute data on the operational context or the environment from sensors; retrieve data from central repositories (e.g. building plans, inventory data) to support their activity; support the tracking and tracing of the supply chain of goods and materials needed in the response and recovery phases of a crisis. [4]

In Europe, many dedicated and secured network infrastructures have been built and deployed to provide the necessary capabilities for PPDR organizations. These networks, generally realized by TETRA/TETRAPOL are narrowband. Lack of broadband connectivity of wireless communications for existing and future PPDR applications is a real problem [4]. Many new applications require wideband data rates usually provided by commercial operators. For that reason, separate parallel data communication channels are needed. A robust multichannel data communication concept that is independent of single operators is presented in [5] and the protocol enabling this, in [6].

The European Commission, the European Law Enforcement Agency EUROPOL and the European Agency for the Management of Operational Cooperation at the External Borders FRONTEX have recognized that lack of interoperability limits the effectiveness of PPDR practitioners in actual operations, and an evident lack of understanding as to whether these limitations arose from technology, operational procedures, gaps in procurement or research [4]. A scientific proven fact is that standardization strongly affects businesses that develop and sell technologies and technology-based products and services; standards are one main enabler for fast growth [7]. Towards improving interoperability, standardization development with like-minded countries should be started.

Chapter 2 of this paper illustrates the operating environment especially from end-users' perspective. Chapter 3 presents the research, development and innovation programme 'Mobile Object Bus Interaction (MOBI)' being made up of two industrial projects and a research project. Chapter 4 describes the research project in more detailed. Chapter 5 presents an initial investigative report on the applicability of SOA and Web services standards in the emergency services domain for the purpose of realizing standardization while tackling software system integration and interoperability concerns across domain. Chapter 6 presents the needs for further research and discussions.

II. ICT SYSTEMS OF PPDR SERVICES

Information systems integration is a current trend in all businesses and organizations [8]. Working manners are trending toward more of mobility and the Web plays a major role in providing critical business data, applications and services to mobile users. In this respect, service-level requirements play an important role in the process. However, service-level requirements are difficult to quantify during the project planning phase. As an example, only the following intangible values could be used as guide lines for drawing up the operational constraints and goals required: 1) usability, 2) performance, 3) scalability, 4) reliability, 5 availability, 6) extensibility, 7) maintainability, 8) manageability, and 9) trustworthiness and security. These attributes can be quantified only after the real deployment. To meet pertinence requirements, the production system needs changing and tuning; if not possible, service-level requirements should be readjusted to conform the operational environment. The reasons for existence of any Web system are to support business and organizational needs. A shift in focus is needed, so that Web architecting activities in any new project can be given more effort, attention and seriousness. [9]

A. End-User Perspective

PPDR field operations are increasingly dependent on ICT systems, especially on wireless and mobile communications. In PPDR vehicles, data communication is mission critical. It is necessary to ensure that information and "on-demand" services provided by these technologies are delivered reliably and securely through one or more of the recently developed wireless architectures.

According to [4], the main effort in developing ICT systems of PPDR should be to standardize the interoperability architecture for applications (e.g. command and control) and infrastructure (e.g. interface gateways, mobile unit). Usability is also a main concern as many solutions are not ergonomic or easy to adapt to existing vehicles or infrastructures. The following recommendations are provided: 1) Inter-System Interface (ISI) is an open interface standard used to connect two TETRA networks together. A joint ISI development should be started with roaming as a primary objective. 2) Harmonized frequency bands for PPDR broadband data services should be investigated and identified. 3) There is the need to conduct a feasibility study of TETRA Enhanced Data Service (TEDS) services to confirm if they are able to address the needs of PPDR organizations in Europe. 4) PPDR broadband data network needs standardized and harmonized technologies. [4]

B. Main PPDR Practitioners in Finland

There are 24 regional police departments in the organization of Finnish police with the National Bureau of Investigation and the National Traffic Police as national units. Modern police vehicles hold more ICT systems and other technical devices than ever. Police vehicles are nowadays mobile offices, in which all kinds of customer contact–related issues ranging from fining can be resolved. Police vehicles also contain numerous systems including cameras and other technical devices for speed monitoring and control together with other traffic surveillance.

Finland has been divided into 22 regional rescue

departments, which are responsible for areal emergency and rescue services. In the biggest cities and towns, hired professionals carry out the major part of the fire and rescue missions while in other parts of Finland, the rescue work rests mainly within the provisions and the functions carried out by the volunteer fire-brigade. The use of ICT in fire and rescue operation management has increased and there are already several different systems in use for different purposes in the field.

In Finland, Emergency Medical Services (EMS) has been outsourced to private companies in 200 municipalities. In 60 out of the 200 municipalities, EMS are being carried out by regional rescue departments and in 40 municipalities the EMS are provided by the municipality itself. Nowadays, patient examination, treatment and condition stabilization is started in the field thus making the possibility for condition deterioration more unlikely during transportation. Patient's treatment in the field sets own requirements for the EMS vehicle. Information technology is replacing the traditional paper forms and the use of technology has increased in other processes as well.

III. MOBI Programme

The target of a Finnish national research, development and innovation programme 'Mobile Object Bus Interaction (MOBI)' is to create a common ICT hardware and software infrastructure for all emergency vehicles. This infrastructure includes devices for voice and data communications, computers, screens, printers, antennas, cablings, and additionally, interlinking with factory-equipped vehicles' ICT systems is researched.

The programme consists of two industrial projects and a research project that generates research data for industrial projects by researching and documenting the needs and requirements of the users, power generation and supply and specifying the existing solutions. One industrial project, led by Cassidian Finland Ltd., implements a vehicle-installed professional mobile radio concept for law enforcement, fire and rescue operations. Another industrial project, led by Insta DefSec Ltd., develops secured software services. The project utilizes the results of the related research project and aims to develop product concepts which have potentials in both domestic and export markets. Additionally, Insta DefSec Ltd. will further develop its business model in order to be able to utilize growth potential of the product concepts. [10]

This research, development and innovation work starts in Finland, because Finland has

- evidences of success in developing wireless telecommunications, e.g. 1G - Nordic Mobile Telephone (NMM), 2G – Global System Mobile (GSM), 3G – Universal Mobile Telecommunications System (UMTS) [7].
- the world's first nationwide TErrestrial TRunked RAdio (TETRA) network - the "Viranomaisradioverkko" or VIRVE network - commonly used by Finnish authorities. The VIRVE network is used by the emergency, fire and rescue services, the police, the Finnish Defence Forces, the Frontier Guard, social and health services, the Finnish Maritime Administration and different government departments. Today, the VIRVE network enables the world's best interoperability between different PPDR services network-wise.
- extensive experiences in field command systems, e.g. the Police Field Command System POKE has been in operational use since 2006 [11], [12]. From the base of the POKE system, a dedicated system 'PEKE' for fire and rescue work has been developed.
- well operating and organized co-operations between authorities at different levels, e.g. national police – customs – border guard cooperation [13].
- an atmosphere which supports successful innovation; e.g. Finnish companies are doing R&D with universities including their competitors, with the popular slogan: "Finland is a club, rather than a country" [14].

IV. MOBI Research Project

As it has been acknowledged, the number of different ICT systems in emergency vehicles has been growing significantly which to a considerable extent has caused problems for example in vehicles safety systems and power supply. Documentation of existing solutions varies and there are no standards in the business. There is also the problem of integration and interoperability between these varying ICT systems since emergency vehicles need to collaborate during an incident for the purpose of information sharing. The research project generates research data for industrial projects by researching and documenting the needs and requirements of the users, power generation and supply together with specifying the existing solutions. The research also investigates how SOA and Web services standards can support the software application requirements of these vehicles in order to enable standardization, integration and interoperability between the vehicles and their control centers. Based on the research a demo vehicle with working ICT-integration would be made. A commercial product including commercializing plans to be offered in the European market is going to be the final outcome of the project. This three-year project started in September 2010.

A. Consortium and Founding

The project consortium, led by Laurea University of Applied Sciences, consists of three research institutes, two industrial partners, three small and medium size enterprises (SMEs), several end-user organizations and a public financier; Tekes – the Finnish Funding Agency for Technology and Innovation. The budget of MOBI research projects is 800 000 € and Table 1 shows funding shares.

TABLE 1 FUNDING OF MOBI RESEARCH PROJECT

Participant	€	%
Tekes	480 000	60
Research institutes	108 000	13
Industrial partners	110 000	14
SMEs	63 000	8
End-users	39 000	5
TOTAL	800 000	100

B. Work Packages

Fig. 1 shows MOBI's Work Packages (WPs). The project starts by researching user requirements (WP2). The common ICT infrastructure is composed of four layers and their standardized interfaces: vehicle ICT infrastructure and power generation (WP3), data communications (WP4), common software infrastructure (WP5), and ICT services for PPDR practitioners (WP6). Also, a demonstration vehicle is equipped (WP7), new business models studied (WP8) and coordination taken care of (WP1).

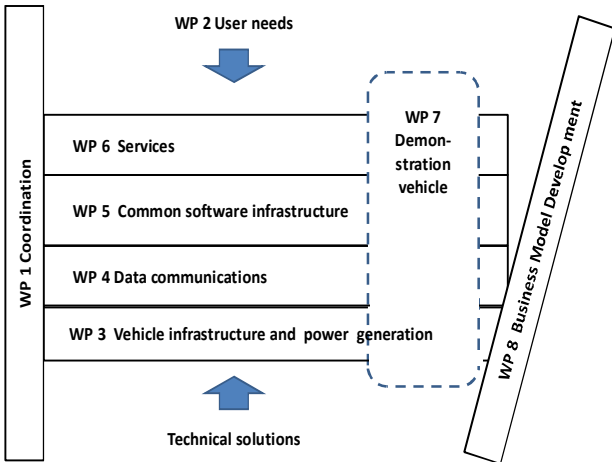


Fig. 1 Work Packages of MOBI Project

1) Coordination

Work package 1 includes tasks considering project management, of which the main objective is to ensure that MOBI research project generates research data for the parallel corporate projects. This work package includes cooperation and exchange of information with other relevant projects, such as MOBI-projects parallel corporate projects, EU FP7/SEC Project AIRBorne information for Emergency situation Awareness and Monitoring (AIRBEAM), EU FP7/SEC Project Policy-oriented marine Environmental Research in the Southern European Seas (PERSEUS) and Scientific innovation Product concept (SCOPE).

WP1 uses Wise Guys-panels that are also common sessions for all the work packages to present what has been done and to plan the future actions. Results from other work packages will be brought to the Wise Guys-panels to be presented. Wise Guys-panels would be scheduled so that they can be arranged before the deadlines of other work packages.

2) User Requirements

In this work package the present electrical- and ICT-systems are being surveyed (for example in case of police vehicles: power supply technologies, radio equipment, video equipment, radars and other speed monitoring devices, IT-workstations, printers, biometric devices, navigation and tracking devices). User and authority requirements for these systems and devices are also being surveyed. Former studies will be used as a source for information.

In this work package administrative and operative systems will be identified and priority and manageability requirements for these systems will be defined. Different authority adoptions (e-adoption, RTTE- and EMC-directives) required for different systems will also be researched. This work package delivers an updated description of the IT-solutions of Finnish emergency vehicles. In this description the requirements are being organized to be used by the companies involved in this research project.

3) Vehicles Infrastructure and Power Supply

Power consumption is one of the biggest challenges of emergency vehicles and their ICT-systems. The number of ICT systems needed to be optimized and power consumption of the other electrical devices in different operational modes will be researched in this work package. Different kinds of power generating possibilities, such as fuel cells, will also be researched. How to ensure that power supply, power control and sleep-mode control is done in a consistent manner would be researched in this work package.

4) Data Communications

The capability of exchanging information (e.g. voice or data) is essential to improving the coordination of PPDR officers during their operations; especially, wireless communications are important in the response and mitigation of emergency crisis to support the mobility of first responders [4].

Data communications of PPDR vehicles can be divided into three levels. The first level is represented by long distance communications e.g. between vehicles and command and control rooms often realized by narrow band TETRA or TETRAPOL systems, but also e.g. @450, 2G, 3G, 4G and WiMAX are used. Also, FM radio and GPS systems could be referred to as long distance communications. Normally, the media used depends on the application or is selected manually by the user.

The second level is represented by local network data communication including e.g. CAN, LAN, WLAN and wide band ad-hoc –communications between vehicles. The third level is the accessory communications of different data systems used in vehicles.

The ICT-solutions of PPDR must be robust and easy to install. Misinterpretations or connectivity failures can cause loss of life or delay the resolution of the crisis. Information security and reliability must be properly considered and taken care of. Different encryption methods of different systems cause their own challenges. In addition, different organizations have their own requirements for managing the information security of their vehicles' systems.

Research of the requirements to be set for data bus and the planning of on-line systems' basic and back-up connections and connections used in off-line systems synchronizing will be carried out in this work package. Different antennas and cabling solutions will also be researched while considering placement, possibilities of interference and possibility of joint cabling.

5) Common Software Infrastructure

In this work package the ICT-integration of emergency vehicle will be planned. Overview of the vehicle's IT-architecture both in online and off-line situations will be created. In this matter the security of the data in local storing

and classified data that can be replicated must be taken into consideration. When planning the vehicle, safety matters must also be considered (such as functioning of vehicles safety devices). This would be one of the major improvements that the integration of systems will bring. Results of the work package 2 will be used as a base for planning of the architecture and user interfaces.

The objective of this work package is a description of the architecture which includes a description of the components the system consists of and how they are being placed. This description would consist of an application architecture, IT-architecture, technical architecture and layout diagram –levels. There will also be an interface definition which describes applications' connectivity to the system. Light-control systems available in present markets would also be studied.

6) Services

The main applications and the services they offer for each end-user group (e.g. video surveillance and speed radars for police) will be chosen for further research. The objective of this work package is to define the emergency vehicles' main applications' functionality and to plan the technical realization of these main applications.

7) Equipping the Demonstration Vehicle

Industrial participants and end-user organizations are able to test chosen solutions in a research environment. Test vehicle built by industrial participants of the project will act as testing environment for the representatives of end-user organizations. A demo-vehicle will be made in cooperation with different participants. Demo-vehicle will be made according to one user-group's requirements meaning that the vehicle would not be a model representing the requirements of both police vehicles and rescue service vehicles. This vehicle will be made for one authority only.

Field testing for the demo-vehicle would be carried out either in the Police College of Finland or in the Rescue College of Finland.

8) Business Models

Development of an ICT-concept is significantly expensive so access to the international markets is desirable. There are good chances to develop the industry in Finland because cooperation between different authorities is efficient and highly developed. The problems mentioned above are similar in all countries: new IT-equipments must be added to authorities' vehicles. A much needed standardization has not been introduced in the industry. The purpose is to create an International Standard Industry's De facto and/or de jure to the industry which makes cooperation between authorities easier and more efficient. The objective is to also make the final result suitable for others than just the authorities. For example, some companies in the industry, private security services and fleet management services could have the need for a moving office-type of vehicle solution. These varying needs would be considered especially when developing commercial solutions.

Question: how a developed solution or part of it could be sold as a compatible set, will be studied in the work package of business models. Industry's market and volumes, national and international public-private partnership regulations will be studied in this work package. One of the main tasks is to monitor the development of markets in this industry within the EU. There is an attempt to create scenarios from the business models which will help one to find out who should be responsible for integration work and further equipment acquisition and administration. A Finnish model to act as a base for creating RFQ-documents would be developed and documented in this work package. Developments in EU-area (for example EUROSUR) as well as markets and regulations (for example outer borders' exit-entry-system which creates new challenges for identification of persons and which is currently being processed by the EU parliament) would be monitored in this work package. Laurea has become a member of the Centre for Identification Research, CITeR, and a partner of the University of Arizona.Developments in the field of CITeR would also be monitored.

This work package produces new business models for the security and safety industry to be used. These new concepts, business plan and possibly an FP7-application user requirement definition would be done in Finland and market research internationally.

C. Requirement Analysis

This phase determines and defines what the system should do. Requirement Analysis would be based on the results of requirements research. The goal is to recognize requirements and to do functional specification for the system. Requirements will be divided in two groups: Functional Requirements and Non-functional Requirements. These requirements define operations, functions and constraints of the system. [15]

Functional Requirements define the expectations of systems behavior or functions. It describes how it works, how it will communicate with other systems, what kind of stakeholders or users it can accommodate, how stakeholders and users can use it. Generally these are the actions that this system must be able to perform. Non-functional requirements also known as quality requirements define features and constraints of the system. The requirements define non-functional quality attributes for the system like usability, reliability, performance and support. [16].

The purpose of this work package processes is to ensure that the project outcome meets the expectations of the customers and other (internal or external) stakeholders. After Requirement Analysis process there will be naturally a design process. The purpose of these two processes is to translate the requirements into a specification that describes how to implement the system [17].

V. Services for Fire and Rescue Personnel

The main objective of this chapter is to commence a preliminary investigation into the applicability of Service Oriented Architecture (SOA) and Web services standards in the emergency vehicles domain. It would seek to explore whether SOA and Web services can support integration, interoperability and reusability of ICT systems and services in emergency vehicles. The knowledge gained could enable us

determine whether SOA can be adopted to fulfill the software application requirements of emergency vehicles.

A. ICT Systems and Services in the Fire and Rescue Department

The way and manner emergency vehicles such as medical ambulances, fire and rescue vehicles deliver their services represents a distributed system. This is further buttressed by the fact that emergency services provision and administration is performed in Finland under national, regional and local basis [18]. When an emergency occurs, ICT systems which are manned in various emergency vehicles are called to play in resolving the incident. These vehicles must network with their command and control centers while they are on the field. It has been acknowledged that past software development paradigms do not provide adequate support for standardization, integration and interoperability between systems in a distributed platform such as the one envisaged by this research. As evident in [18], real-time information interchange between collaborating systems and the headquarters during an emergency is critical. SOA is thought to hold the promise of resolving the aforementioned issues.

When considering a transition to a SOA solution in order to enable the day-to-day operations of fire and rescue personnel and the optimization of the ICT systems that enable these operations, it would be worth to take stock of the existing services and the business requirements of the fire and rescue department since SOA attempts to align business with technology. There are some major pertinent questions that would give direction to the overall research concerning SOA application in our problem domain. Because the project is in its preliminary phase, we would not answer some of the questions in this paper but in a later paper. The questions include:

- Did fire and rescue department adopt the SOA paradigm when developing their ICT systems or any aspect of their system?
- If yes, to what extent does this architecture support standardization , integration, interoperability, reusability and extensibility for future services and how can SOA support via Web services provide for mobile or internet support while allowing access to emergency vehicles and personnel?
- If no, what kind of solution can we manage?

Based on the interview that was held with some personnel of one of the Finnish fire departments, rescue service chain starts when a call is placed to the emergency rescue centre. This centre receives the call, processes it and forwards same to the scheduled rescue units. These units can be for example fire units, ambulance and emergency medical units and the police units. The calls to either of the units are prioritized based on the severity of the situation. The emergency rescue centre usually makes the decision of how many units are sent to the scene of an incident. As the mission is delivered to the units and departments, the chain does not break up. Moving units and rescue centre are in constant contact with each other. Units can therefore move in advance to the location while at the same time receives more information about the mission. It is possible to have an incident which would not only require fire and service vehicles but ambulance vehicles at the same time. This means that all units involved would be reporting to their various control centers and they would need to share information about the situation.

The above description partly defines the process and information flow when the control centre receives a call. The rescue centre can receive new information from the caller and convey the same information directly to the fire officers who are already on the move thus; previous knowledge about the situation is updated with current information. While in the rescue vehicles, rescue personnel are also able to monitor the situation via different user interfaces on their laptops. These interfaces display a series of vital information that they need to accomplish the task. They work in union with the emergency rescue centre which commands the mission.

Every emergency call that is placed to the command centre has its designated code which describes the severity of the incident being reported. This call code is directly received by the fire Chief in-charge who is presented with the corresponding mission and objective regarding the code on his terminal. He is able to gauge the scale of the incident and the number of units to be deployed. The vehicle has on-board a computer which runs an application called Merlot Mobile 4.1 provided by Logica. The Merlot Mobile system essentially enables the field personnel to receive up to date information about the reported incident. The ambulances and rescue helicopters use an extended version which includes the patient personal data and his or her medical history. This is a highly restricted system which permits access to only the doctor or a designated person.

In some cases the character or nature of the mission changes and if the fire Chief at the controls needs to make any changes, system automatically refreshes itself at the field terminals. The control centre is able to monitor the field events in real-time. When the unit arrives at the incident scene, the field commander must scroll the blueprints of the building, and what area to turn out. One major issue is that the objective cards (blueprints) are not current while some suffer from wear and tear. This has a great impact on how fast the fire is turned off. This manual process that involves looking up blueprint would require improvement.

The rescue personnel have VIRVE which they can use in large operations. It is a dedicated network for army, police, fire and rescue department, sea patrol, rescue helicopters and other public safety practitioners. There also exists a system which automatically sends a warning signal to the 112 centre if it detects fire or smoke. This is also related to the blueprint section where the blueprints are currently manually used and if this could be viewed digitally in the Merlot system or added as a Web service it would be of immense benefit as losses are reduced and process improved.

B. Challenges within Fire and Rescue Services and Emergency Services in General

It has been established that, PPDR services are supported by

different agencies which include the police, fire and rescue, emergency medical services etc. It is also well known that the provision and management of PPDR services is not central as it is performed on national and regional basis. All these agencies have different ICT systems which enable them to carry out their roles. During an emergency, field officers and their systems on-board the vehicles are required to collaborate in resolving the emergency. A well known challenge within PPDR services is the integration of all potential ICT systems and services that are needed to support an incident and their command and control centers. This would bring about efficient and effective real-time information exchange and provide a common pool of shared services among collaborating partners.

Currently, the fire and rescue service as we have earlier on stated runs a software application known as Merlot Mobile. This software essentially enables the effective deployment and monitoring of field units which provides a means of updating field officers as situation changes. One key aspect that this current system does not support is the electronic availability and management of blue prints of buildings. This gap is evident when field officers are only able to locate areas of an affected building by flipping books that hold the building's blue prints at the scene of incident. It is possible to have a consolidated and integrated database of electronic blue prints of all buildings which is updated on regular basis. This would enable the command and control centre to have the exact locations of concern within the building well in advance before the field officer arrive the scene.

However, it is common knowledge that, PPDR services such as the medical emergency services are tilting towards the adoption SOA for an effective and efficient healthcare delivery. The Finnish government has already adopted SOA for the national health archive and still considering its adoption other health care domains. It is possible to have a private or public service registry which would contain Web services that can be shared between PPDR services. Common Web services that enable the resolution of emergency crisis can be shared by EU member countries who wish to pursue a similar business model for PPDR services. In order to benefit from a future adoption of SOA, PPDR services would need to investigate the feasibility of SOA application towards achieving standardization and integration. Part of this study sets out to achieve this.

C. What Role can SOA and Web Services Play in the Fire and Rescue Domain Including Emergency Vehicles in General?

In order to answer the above question, we would first present a brief overview of what SOA and Web services entail.

SOA is an architectural paradigm of which main characteristic is to promote loose coupling during the design and implementation of a software system. According to the World Wide Web Consortium (W3C), SOA is ''a set of components which can be invoked, and whose interface descriptions can be published and discovered''. The SOA paradigm creates room for loose coupling, interoperability and standards-based computing. SOA is also a way of designing new applications which involves the incorporation of "services" from existing systems and provides a key solution to overcoming the challenge faced by organizations in their desire to display data in a way that involves effective and efficient human interaction [19]. Also in [20] and [21] loose coupling is a key property of SOA which enables interoperability and effective design and management of systems. This research would adopt the SOA definition giving in [22] and which defines SOA as "an [enabling] framework for integrating business processes and supporting information technology infrastructure as [loosely] coupled and secure, standardized components-services-that can be reused and combined to address changing business priorities". Fig. 2 shows a typical SOA architecture which consist of a registry of Web services that are made available by the Service Provider and consumed by the Service Requesters. It also depicts the collaborations between these three major components.

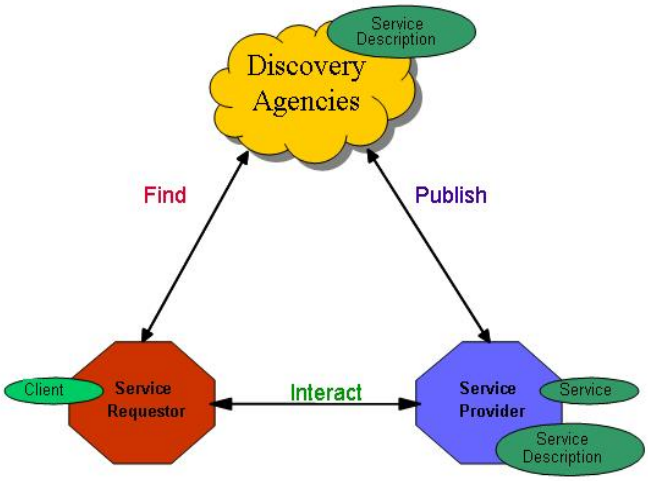


Fig 2 SOA Architecture [23]

Web services though not quite new have witnessed a remarkably wide acceptance in the industry as a very vital means of implementing SOA. This acceptance is owing to the fact that, Web services are able to provide a distributed computing style which makes it possible to integrate heterogeneous applications across the Web. The Web services specifications are such that they are totally independent of any programming language, hardware and operating system thereby enhancing loose coupling between service requesters and providers hence fulfilling the loose coupling principle of SOA.

According to W3C Services Architecture Working Group, "a Web service is a software application identified by a URI, whose interfaces and bindings are capable of being defined, described, and discovered as XML artifacts. A Web service supports direct interactions with other software agents using XML-based messages exchanged via Internet-based protocols." In [23] Web services are defined as "a family of technologies that consist of specifications, protocols, and industry-based standards that are used by heterogeneous

applications to communicate, collaborate, and exchange information among themselves in a secure, reliable, and interoperable manner." It is also worth to add that, SOAP and REST are currently the major paradigms which can be used to further implement Web services.

The Web services technology is based on open source technologies which include: eXtensible Markup Language (XML), Simple Object Access Protocol (SOAP), REST, Universal Description, Discovery and Integration (UDDI) and Web Services Description Language (WSL). As earlier mentioned, the use of the above named open standards enables the applications that have been developed using different vendor platforms to easily interoperate. The attainment of interoperability between vendors implies that, public and private organizations do not need to have knowledge about the would-be service requesters before they consider or implement Web services and vice versa. The benefit as we would explain later is easy integration and adaptation to changes in the business goals of the organization.

Given the overview of SOA and Web services above, there is no doubt that their application in a distributed domain like the one presented in this research could be of immense benefit.

D. SOA Standards

The success of the application of SOA as a key to resolving issues of standardization, integration and interoperability across our problem domain mainly begins with the incorporation of SOA principles to the analysis and design of the intended SOA solution. We would now briefly look at these key principles as given in [24].

1) The Standardized Service Contract Principle

This principle is mainly about the compliance of service descriptions with design standards. The description of service capabilities must be understood by other parties who are interested in using such service. The properties of such service should conform to the service contract which in this case is the design standard. The service contract would usually carry information which can be used to identify any service such as textual description, URL, name etc.; it would also have functional properties, like the type of input/output parameters, interaction model; also non-functional properties which include, QoS, the location of service, security constraints just to mention a few.

The provision of standardization enables the interpretability of services, which gives rise to the predictability of the service behaviour. This prediction of the future behaviour of services is an important mechanism which enables the attainment of scalability owing to the fact that, it makes room for the evaluation of the vital computational resources required to authenticate a targeted service. This key mechanism facilitates smart provisioning of resources so as to prevent a decline in software resources.

2) Loose Coupling Principle

According to this principle, the interface of a service should impose low consumer coupling and should also be orthogonal to its surrounding environment. In [25], loose coupling is intended to replace precision in the description of the interfaces of service for a better reason which is achieving flexibility in the interoperability between systems which are heterogeneous with respect to technology, location, performance and availability. This principle enables the development of loosely coupled applications which are more reusable and can better adapt to changing requirements. Tightly coupled systems are not highly scalable and as explained in [26], even-driven systems which are loosely coupled and also in [27]; space-based systems have been proven to be more highly scalable than the tightly coupled systems.

3) Abstraction Principle

This principle states that, the details of software artifacts which are not indispensable for others to effectively use it should be hidden. It therefore means that all the important information which is required to invoke a service is contained in the service contract while the entire knowledge of the underlying loge, technology, etc. should be completely hidden. Some authors have termed this principle "black boxing" which is synonymous with the concept of black boxing in the old software engineering concept. The principle of abstraction facilitates replaceability.

4) Reusability Principle

The principle states that, the functionality that is provided by services is as domain and context independent as feasible, enabling reuse. The application of this principle results in the provision of the logic of a service that is highly generic, independent of its original usage situation. This principle is one of the keys to enabling SOA infrastructures due to its ability to make room for the creation of huge libraries of domain-independent services that leverages the construction of new complex context-dependent services.

5) Autonomy Principle

The principle of autonomy posits that, the processes that are attached to services should be carried out in such a way that, they are independent of any external influences. Therefore, if in any way the outcome of any service is to be changed, it has to be via the modification of the input parameters as stated in the service contract.

6) The Statelessness Principle

The principle of Statelessness specifies that, services should minimize resource consumption by deferring the management of state information when necessary. This principle has been redefined and taken beyond its limits courtesy of the REST architectural paradigm by [28]. REST has been effectively and successfully applied to SOA in the past. In order to achieve any reasonable scalability of a given SOA infrastructure, it is very important that there exist a conformance with this principle. This is due to the known fact that state maintenance is among the most difficult resource consuming tasks in computing. Any ample reduction in the amount of state information that is to be taken into account by any given service results in a large reduction of the resources that would be used by the entire SOA system.

7) The Discoverability Principle

This principle which is closely related to the principle of Standardized Service Contract states that, there should be

annotation of services with metadata so as to enable their discovery by parties who may be interested in any of the services. Collaborating emergency vehicles and their control centers are able to find these services and use on a 24hr basis since they are hosted online.

8) The Composablity Principle

As stated in [24], this principle identifies services as effective composition participants without minding the size and complexity of the composition. This composition could be in two perspectives; a bottom-up perspective would consider a combination of small and simpler services into larger and complex services while a top-down perspective would the other way round. Based on literature, the latter service composition perspective is the most effective way to resolve the complex nature of some given processes. This principle has been noted to be one of the core elements within the definition of a Web Service due to the fact that, the ability to easily create new services is preliminary requirement to the global adoption of SOA.

The incorporation of the above principles in any SOA solution is fundamental to realizing the much needed interoperability among collaborating systems in an enterprise.

E. Web Services Standards

In this section we would to a large extent focus on two prominent Web services implementation standards (SOAP and REST) though we would still explore other standards that enable SOA realization. These two standards are currently generating a debate within the Web community concerning which of them should better be adopted.

1) SOAP

SOAP is originally an acronym for Simple Object Access Protocol now just known as SOAP rather than an acronym. It is a Web service standard which supports communication between Web services (www.w3.org/2000). SOAP was initially developed by Microsoft and thereafter further developed in collaboration with UserLand, Lotus, IBM and Developmentor. SOAP is typically an XML-based specification which can be used for messaging and remote procedure call (RPC). The SOAP protocol depends on already existing transport protocols which include Hyper Text Transfer Protocol (HTTP), Simple Message Transfer Protocol (SMTP) and Message Queue Series (MQSeries)

The SOAP standard specifies a messaging model which establishes the way message recipients must process messages sent via SOAP. The specification also provides for actors that can process the message. SOAP messages are able to locate and identify their respective actors that are required to process various parts of the message. There could therefore be an exchange between actors for the message to be processed.

According to [29], the WWW is such that it is "intrinsically distributed and heterogeneous in nature, communication mechanisms must be platform-independent, international, secure, and as light as possible". In order to address these issues, XML came to the fore. XML has been established as a machine readable language which supports data and information encoding in a way that addresses systems independence. They opined that, communication protocols which are developed based on XML are primarily the answer to realizing Web services. XML provides a common representation of information thereby enabling information interchange between heterogeneous systems. The SOAP protocol which is built based on XML and operates on HTTP therefore holds the promise for Web services implementation. We now look at the two core benefits of SOAP.

2) REST

REST is an acronym which stands for Representational State Transfer. Roy Fielding of the University of California, Irvine U.S.A first coined the acronym and introduced REST in his 2000 PhD thesis. Though REST was not embraced in its early years of conception, it has now enormously achieved wide acceptability across the Web community. In the past few years, REST has witnessed global adoptions as it is perceived to be a true representation of the Web, simple and more viable option to SOAP-WSDL based Web Services. This recent and rapid trend of REST adoption has triggered an ongoing debate about these two leading SOA implementation paradigms. Some aspects of this study would attempt to weigh into this debate based on the feedback we would receive from experts in the industry via questionnaire and interviews. This feedback would help inform decision makers in the health sector on which paradigm to adopt in transitioning to a SOA infrastructure.

The motivation for the REST paradigm is to reap from the WWW characteristics which make the WWW successful. It is these characteristics that actually guide and enable the way the WWW has evolved and continuing to evolve. Moreover, REST views the WWW as an information system and expects other information systems to be integrated into it via Web gateways. The main goals of REST are:

1. The scalability of components or resources interactions
2. Achieving uniform interfaces
3. The independence of the deployment of resources
4. The provision of intermediate components to lessen interaction latency, improve security and enable legacy system encapsulation.

We next look at how these goals are achieved. The following key constraints and architectural principles which form the REST paradigm and achieve the REST goals stated above have been derived by [28]

a) Statelessness of RESTful Services

In this principle, Fielding opines that, individual requests that emanate from client applications to any specified server must have all the vital information which is necessary for it to be able to understand the client's request. However, this request must not depend on any information that resides or stored on the server. Clients must therefore be able to successfully complete their request independently of states that are stored on the server.

Since this principle does not require Web service clients to take advantage of any states that are stored on the server for them to complete a request, a RESTful service client is expected to provide all the information such as state,

parameters and other data which the server needs to generate and issue a response it. This important information must reside within the HTTP headers and BODY of the client's request. This principle has been acknowledged to be very useful as it adds to the effective performance of the Web service. Moreover, the design and implementation of components that reside on the server is made simple since it has also been acknowledged that, the non-existence of states on the server means that session data need not be synchronized with outside applications.

b) Uniform Interface of RESTful Service

This principle requires that a RESTful service be able to explicitly use HTTP operations according the defined RFC 2616 protocol. These HTTP operations or methods which include GET, POST, PUT and DELETE must be the only methods that are allowed within the HTTP protocol. They must also be strictly used as they are originally meant to be used.

This principle is coming on the heels that, the same HTTP methods have been grossly used for purposes which they are not intended for. For instance, the GET method is specifically required by clients to retrieve information from the server but it is being misused by developers to execute queries and also perform remote procedure calls. This however introduces design flaws which inhibits the achievement of uniform interfaces for all RESTful service clients.

It is there beneficial to incorporate this design principle in any RESTful service realization.

c) Resources and Resources Identification

In (Fielding, 2000), resource is the main representation of information for REST paradigm. He opines that, certain information that one can name could represent a resource. A resource could therefore be a document, an image, a collection of resources and all other things that can be considered as resources. It therefore holds that, the whole REST architecture revolves around the concept of resources. The next concept is that of URIs. Any resource that can be named must have its own URI which uniquely identifies it. This is another fundamental characteristic of REST.

As explained in [30], RESTful client applications utilize resources via URIs. The URIs facilitates the intuitiveness of the Web service when they are well defined. The URIs used by RESTful services should be able to point to specific resources without much ambiguity. This according to Rodriquez encourages usability which can be achieved the more by exposing URIs in the form of a directory structure that is more readable and understandable. An invoice submission service in our problem domain can therefore have a URI which represents and invoice document.

d) Exchange of Resource Representations

Information is represented as a resource. This representation could mimic the context state of the resource and all its attributes at the time a client application sends a request to the server. The components that constitute a RESTful service are operated upon via the exchange of representations of the resources that are involved. One could have a representation of an order record in a database. This representation would have direct relations between the field names and the XML tags respectively together with the location of elements that contain a given row of values. In contrast to SOAP-based architectures communication, states that "REST-based architectures communicate primarily through the transfer of representations of resources…" This according [31] is primarily distinct from the Remote Procedure Call (RPC) which tends to hide the invocation of a procedure on the remote server.

In order to accomplish effective exchange of representations, RESTful services are encouraged to adhere to appropriate formats of the data which the client application and the Web service exchange within the request and response payload and even within the HTTP body.

REST goal of achieving scalability of component interaction has been achieved since the exponential growth of the WWW has not gone low in performance. One instance is in variety of client software applications that are made available for other applications and can also be accessed by other applications. More interestingly is the goal of uniform interfaces which pitches REST advocates and SOAP advocates. The advocates of REST believe that the REST paradigm is better than SOAP paradigm since HTTP client applications can communicate with HTTP remote server without the need for re-configuration. SOAP on the hand requires knowledge of the methods to invoke and is also a protocol framework unlike HTTP which is an application protocol.

As we have pointed out earlier, there is an ongoing debate on whether REST is better to adopt than SOAP. Some experts in the industry and in research have advised that, REST cannot always be the appropriate style to use in designing and implementing Web services in some circumstances. In the face of this debate, experts agree that, the introduction of REST makes it possible to design and implement Web services that are independent of proprietary middleware such as the Oracle Application Server and similar servers. This however contrasts SOAP-WSDL based implementations of Web services. REST is however a true representation of the WWW as its principles encourages a strict adherence to the original WWW, URI and HTTP standards. In (Richardson & Ruby, 2007), the realization of Web services via REST makes it possible to achieve integration requirements which are necessary when building enterprise systems. Enterprise system resources can therefore be exposed through RESTful services which are able to provide different client applications with data which is formatted according to standards.

3) SOAP OR REST

SOAP and REST are currently the two competing standards for implementing Web services. The problem with developers does not stem from a lack of understanding of these implementations but rather the choice of implementation to use. As [31] acknowledges, SOAP and REST only two styles

of interfacing the WWW with Web services. These two approaches really work but have pros and cons. The onus on the developer to chose which approach is suitable for his or her use. The decision making process is perhaps what translates into a debate and brings about the need to consider the various benefits the two specifications bring. SOAP which is a is widely used for Enterprise Application Integration (EAI) for a host of different web-based applications coupled with legacy system integration. Google is a well known implementer of Web services using SOAP. On the other hand, REST primarily provides standardization for URI which is used to represent resources. HTTP operations such as GET etc are used to manipulate these resources. Though SOAP has been around before REST, REST has proved itself to be the most popular. Currently, key Web services that are available online make use of REST. These Web services are provided by Yahoo, Flickr, pubsub, bloglines, del.icio.us, Twitter among several others. Amazon and eBay provide Web services that utilize SOAP and REST.

We now focus on issues surrounding this debate in the following headings:

a) Security

Security is one significant aspect of the SOAP-REST debate. We have seen earlier that, SOAP can be used for RPC calls over HTTP. Forwarding RPC calls over HTTP standard ports has been considered a better way to support Web services within the length and breadth of an organization's boundaries. This is the position of the proponents of SOAP which the REST proponents believe that this compromises the security of the network. Though REST RPC are carried over HTTP, a firewall is able to detect the motive of client messages by filtering the HTTP command used in the client request. Since REST is strict about the HTTP operations it allows, a GET command cannot do more than query the server for information retrieval. This is not the case for SOAP which is not strict about HTTP verbs and which for instance uses POST to serve up client requests.

When it comes to security such as authentication, the REST style takes advantage of the authentication and authorization processes which are already provided by Web servers. Industry-standard security certificate coupled with identity management systems can be enable developers secure the network layer. The Lightweight Directory Access Protocol (LDAP) is an example of such of a system and developers can afford to utilize Access Control List (ACL) file to manage Web services and similar to URIs.

Both proponents agree that, for better security, sensitive data should not be passed as parameters via URIs while enormous packets of data on the URI should be discouraged as the URI may not accommodate it. Concerning attachments, SOAP performs better than REST but it is generally thought that SOAP for attachment should be considered only when necessary this because it does not still providefor the simplicity that REST provide.

b) Handling of Types

SOAP supports a fixed set of data types. This makes SOAP to provide a tougher typing than REST. The benefit of this is that, in any given platform, a value that is returned is made accessible in a corresponding native type.

c) Caching

SOAP client requests make use of the POST HTTP verb which often need a sophisticated XML request to be formulated thus making caching of client responses herculean. REST APIs can easily be consumed by clients via the GET operation which make it easy for proxy servers to cache responses. SOAP messages are therefore not easily cacheable.

d) Server-side /Client Side Complexity

It has been generally agreed that REST is easier to use than SOAP. Even at this, it is evident that, many of the programming languages enable developers to expose their class methods via SOAP since the serialization and deserialization is managed by the SOAP's server library. This is not so simple with HTTP API as the method to be exposed would sometimes need the resulting XML to be serialized. This however brings an overhead task of having to map URIs of resources to specified handlers and then import the representation of the HTTP request within the same scheme. SOAP therefore makes it easier to expose class methods rather than REST.

On the client side, it is understood that, placing service calls to HTTP APIs is far easier to accomplish compared to SOAP APIs. SOAP APIs would usually need a client library, a stub and lots of necessary skills to realize it while REST on the other is already local to a variety of programming languages and therefore very easy to create HTTP client request. Because REST resources are usually easy to be called from client interfaces which makes REST more beneficial than SOAP which finds its strength at the server-side.

e) Limited Bandwidth

REST is agreed to be a lightweight architecture which shortens client requests and responses and more suitable for the Web. SOAP normally needs an XML kind of wrapper to wrap client requests and response. The SOAP camp are of the opinion that, the provision of strong typing by SOAP makes service client and the service provider to have a fore knowledge of the types involved which makes it very beneficial. This is the question posed to the REST advocates. It is argued that, REST like SOAP need a document which defines the input and corresponding output parameters. REST proponents feel that, since REST is flexible, developers are still able produce WSDL files for Web services that would necessarily need an explicit declaration of parameters. This would be on-demand basis only.

In the light of this debate and based on the opinions of both proponents, this study does not see both REST and SOAP replacing each other. This study also agrees with both proponents about the complexity of implementing SOAP on

the client-side and the complexity of implement REST on the server-side. Given the merits and demerits of both styles, there is a general consensus that the adoption of either SOAP or REST implementation should best be determined by the domain of application and those characteristics of either SOAP or REST that are perceived to be of benefit to the domain.

We have developed a questionnaire which would enable assess the feasibility of either of these two standards.

F. Perceived Benefits of SOA

In this section we present the promised benefits of SOA and the rationale behind our proposal to investigate it for its probable adoption as an enabler for achieving systems integration and interoperability in the case of ICT systems and services in emergency vehicles and the control centre as opposed to other architectural paradigms.

It is a well-known fact that, company CIOs and top IT executives have been experiencing challenges which include: reduction in costs while maximizing the usage of technologies that have been in existence; achieving a better customer experience; having a better competitive advantage; and be more proactive and responsive to actualizing business goals. Heterogeneity and change are the underlying factors that have caused these challenges [32]. The enterprises that are currently in existence are a product of different architectures and technologies that have changed over time. The integration of these varying systems which are from different vendors is still a nightmare for organizations. This results in the heterogeneity problem. More so, improvements in technologies have accelerated in recent times and organizations need to change and adapt quickly to these improvements if they desire to gain competitive advantage and meet changing client's requirements including reduced cost in the provision of services.

The above named challenges gave rise to SOA and [32], [24] among others have identified the following benefits of SOA:

1) Leveraging the existing assets of organizations

Since SOA is service and business centric, it provides an abstraction layer which makes it possible for organizations to effectively leverage their IT investments via the wrapping of their existing infrastructure as services which would represent business task as is explained in [24] and [32]. This is where SOA aligns business goals with technology. Therefore, without rebuilding new IT infrastructures, companies can still profit from using their existing technologies. The services which have been identified have interfaces. The interfaces for the services are designed by adopting an outside-in approach instead of following the details of their implementation. The idea is to design the interfaces with a main focus on how the services could suit in a bigger business process environment. SOA is acknowledge to be business process centric instead of technology centric when compared to other architectures hence a service would usually align itself with a given business task. Following from the design principles of SOA, the interface of a service would mostly be coarse-grained and stateless. It is also based on messages and document interchanges. The object oriented paradigm is different since it does not support this aspect of service orientation. It rather deals with individual objects and their attributes in a tightly coupled manner.

2) Integration, interoperability and management of complexity

OA enables easy integration and management of complexity due to the provision of service specifications which in turn brings about transparency in implementation thereby reducing the impact which arises when implementation and IT infrastructures are changed. The service specification which wraps the existing infrastructure makes integration easier since the complexities have been isolated. SOA enables the design and development of software systems that are interoperable based on standards that have been defined and agreed to by key industry players. Major players include: IBM, Oracle, Microsoft etc. Since "service" is the key in an SOA-based solution, interoperability is supported via the abstraction of the interface that a given service exposes from the implementation of the service itself.

According to (Wright and Reynolds, 2009) [33], the consistency in the SOA architecture together with SOA standards helps to achieve interoperability between heterogeneous systems. SOA is not however, not technology-specific and its principles can be utilized via assembler just as it is obtainable in high level languages. Adopting the SOA model makes development easy as it is supported by tools that are interoperable and portable across different software vendors. Since web services which are standards controlled by notable groups including OASIS is the familiar and most common way of implementing SOA, these standards makes it possible to achieve interoperability between different vendor technology stacks. Erl opines that, SOA provides for native interoperability among services for the purpose of reducing the degree of integration.

Among other definitions of SOA is the inclusion of the property of "autonomy". It is stated that, the interoperable systems are also autonomous. This property according to [33] contradicts the interoperability property though the same authors went further to describe how the contradiction is addressed via the service-centric architectural principles which we have talked about under the section "principles of SOA" earlier in this chapter.

3) Cost and reusability

Service oriented computing through SOA purpose to support the creation of solution logics which are not tied to any particular purpose [34] and [32]. These solutions are therefore agnostic in nature and reusable solutions which in turn leverage the interoperability of SOA as it is realized during the design of services. The adoption of SOA makes it possible for major business services to be exposed in a loosely coupled fashion unlike the case in other architectural paradigms that are tightly coupled. This facilitates easy use of services and they can be combined as business needs arises. The duplication of software resources is reduced as resources can be reused thereby bringing about reduced cost.

Organizations that seek to determine the cost effectiveness of the IT platforms they run would usually take a measurement of the return on investment. If the return on investment is high, the more they stand to benefit from the solution they have adopted. The adoption of SOA is seen to cut-down organizations budget and gives a greater return on investment than the traditional software paradigms.

4) Business and Technology alignment coupled with faster time-to-market

Business alignment and agility are well supported when SOA is adopted [34]. The idea of going through the SOA phases of analysis and modeling which conceives the conceptual service inventory blue print requires the services of business analysts or experts who have the know-how of the business case that needs SOA solution. The SOA design which follows provides the capability to clearly align the business goals with technology. This alignment is further supported by the interoperability which SOA provide via the design of interoperable services there by facilitating easy business changes.

Organizations that aim to be agile while responding to demanding business needs would have to take advantage of SOA which enables the composition of new services from existing ones. Using SOA to leverage existing company infrastructure reduces the time required to undertake a fresh software development which involves going through all the phases of the software development cycle (SDC). By-passing the SDC via SOA brings about a faster development of fresh services and makes it possible for organizations to respond and adapt quickly to change and the time-to-market is also reduced.

5) Adapting quickly to future changes and Vendor Diversification Alternatives

Also in [32], SOA adoption enables organizations to be better positioned and ready for future changes. Since organizations would have business processes that consist of a range of business services. These processes can be easily created and where need be, changed or managed to reflect current and future needs. The flexibility and responsiveness which SOA provides makes it adoption necessary for companies to survive, thrive and compete favorably.

It has been generally acknowledged that, while it is not a necessary benefit for organizations to have an IT platform with diversified vendors, it would however be beneficial if organizations can have the option to vendor-diversify when the need arises. The adoption of SOA makes this option possible since the architecture ensures that technologies which can be used to implement SOA solutions are independent of vendors or non-vendor specific. This makes organizations to easily change or extend their IT platforms. The vendor-neutrality provided by SOA further strengthens the ability of companies to make constant changes to their IT platforms since physical service contracts are shaped into standardized endpoints while service implementation details are abstracted in order to provide a consistent inter-service communication framework. In addition, the standards-based and vendor-independence of Web services also supports organizations to vendor-diversify since Web services do no restrict or impose proprietary communication criteria.

In brief summary, this chapter presents a background of SOA and Web services. We have shown that SOA and Web services are keys to achieving systems standardization, integration and interoperability in any enterprise based on secondary study. The information presented in this chapter would enable us plunge into the main investigation of the feasibility of applying SOA in PPDR services. We have developed a questionnaire which would enable us to further determine the choice of software architecture that best suite PPDR services. In our next paper we would present a service blue print for our problem domain and the final results of our investigation.

VI. Discussions

Regulations and standardization play an important role in applying the results of research to the market and to PPDR end-users. The on-going planning of European external border surveillance system (EUROSUR) [35] and EU´s enhanced powers in the field of internal security by the Treaty of Lisbon sets the pace for further standardization efforts. Finland has one nation-wide TETRA network used by various PPDR organizations. As a consequence, there is full domestic interoperability network-wise. Finland has evidences of developing wireless communications standards and well operating and organized co-operations between authorities at different levels. Here, a prototyping environment with de facto standards could be made.

In order to implement and manage a prototyping environment that can develop and provide standards for interoperability which would in turn enable information to be shared between security providers within and between nations, the prototyping environment should provide for candidate operational scenarios to be synthesized. This for example could be a trans-border incident emulating the data flows between systems and operators, and also so show that information and data exchange retains consistent meaning as well as timeliness when portrayed in different systems. The aim would be to provide a focus for researchers, system designers, information system operators and security front line operators to develop and validate semantics, syntax and meta-data so that such standards can be rolled out by security providers with confidence.

In pursuance of the need to contribute towards resolving the issues of standardization, integration and interoperability between ICT systems that are used in PPDR services, the idea of investigating the feasibility of applying SOA and its standards to this distributed domain is essential. This is even more required as SOA has positioned itself to be the most viable solution for an organization's enterprise system. Small and medium scale enterprises are gradually tilting towards the adoption of SOA so as to benefit from some of its promises. Web services would no doubt be an interesting technology to provide mobile and internet support for field units and their command and control centers. The national, regional and local administrative structure which describes our problem domain

could benefit from SOA adoption as it would present a common integrated abstract layer of administration which would facilitate sharing of common Web services, information exchange between PPDR agencies while making administration efficient and effective. Our study in this regard is to make useful recommendation concerning the probable software architecture that best meets the needs of PPDR services.

REFERENCES

[1] T. Hult and J. Rajamäki, "ICT Integration of Public Protection and Disaster Relief (PPDR): Mobile Object Bus Interaction (MOBI) Research and Development Project", in Proc. 9th WSEAS International Conference on Applied Electromagnetics, Wireless and Optical Communications (ELECTROSCIENCE '11), Meloneras, Gran Canaria, Canary Islands Spain, March 24-26, 2011, pp.143-148.

[2] J. Rajamäki and T. Villemson, Creating a service oriented architectural model for emergency vehicles, International Journal of Communications, Iss. 1, Vol. 3, 2009, pp. 44-53.

[3] J. Rajamäki and T. Villemson, Designing Emergency Vehicle ICT Integration Solution, Proc. of the 3rd International Conference on Communications and Information Technology, Athens, Greece, Dec. 29-31, 2009, pp. 83-90.

[4] G. Baldini, Report of the workshop on "Interoperable communications for Safety and Security", Publications Office of the European Union, 2010.

[5] J. Rajamäki, J. Holmström and J. Knuuttila, Robust Mobile Multichannel Data Communication for Rescue and Law Enforcement Authorities, Proc. of the 17th Symposium on Communications and Vehicular Technology in the Benelux, ,Twente, The Netherlands Nov. 24-25, 2010.

[6] J. Holmstrom, J. Rajamäki and T. Hult, "DSiP Distributed Systems intercommunication Protocol - A Traffic Engineering Solution for Secure Multichannel Communication" in Proc. 9th WSEAS International Conference on Applied Electromagnetics, Wireless and Optical Communications (ELECTROSCIENCE '11), Meloneras, Gran Canaria, Canary Islands Spain, March 24-26, 2011, pp.57-60.

[7] A. Kivimäki, Wireless telecommunication stardardization processes – actors' viewpoint, ACTA Univ. Oul. A 483, Oulu University Press, 2007.

[8] D. Litan, A.-M. Mocanu, "Information systems integration, a new trend in business", ", in Proc. 9th WSEAS International Conference on Applied Electromagnetics, Wireless and Optical Communications (ELECTROSCIENCE '11), Meloneras, Gran Canaria, Canary Islands Spain, March 24-26, 2011, pp.250-256.

[9] S. Tumin, S. Encheva, "A brief look at Web architecting", in Proc. 9th WSEAS International Conference on Applied Electromagnetics, Wireless and Optical Communications (ELECTROSCIENCE '11), Meloneras, Gran Canaria, Canary Islands Spain, March 24-26, 2011, pp.245-249.

[10] Tekes, Safety and Security Programme Projects http://www.tekes.fi/programmes/Turvallisuus/Projects

[11] H. Vilppunen, "TETRA data services & applications", presented at the TETRA Congress, June 13th -14th 2006, Warsaw, Poland.

[12] P. Nurhonen, "POKE – GIS-based field command system for police", presented at the Nordic Seminar of the Use of Geographic Information in Crises Management, May 19th – 20th 2008, Bergen, Norway.

[13] A. Niemenkari, "Integrated border management – case Finland", Euromed migration II project, 23 FEB 2010, Rome, Italy, available: http://www.euromed-migration.eu/e1152/e1483/e2556/e2585/e2641/ presen92NiemenkarM2s21feb2325rome2010.pdf

[14] V. Ilmavirta, "IPR management and industrial cooperation in the new Aalto University, the technology and innovation heart of the Otaniemi Science Park", Intelektinės Nuosavybės Valdymas Mokslo Ir Studijų Institucijose: Jo Vaidmuo Technologijų Perdavimo Procese, Vilna, Lithuania, 2.3.2010.

[15] R. Pohjonen, Tietojärjestelmien kehittäminen. Jyväskylä: Docendo Finland Oy, 2002.

[16] P. Kruchten, The Rational Unified Process: An Introduction, 2004.

[17] I. Haikala and J. Märijärvi, Ohjelmistotuotanto, Hämeenlinna: Talentum Media Oy, 2004.

[18] Mykkänen, J., Korpela, M. & Ripatti, S. Local, Regional and National Interoperabilityin Hospital-level Systems Architecture. Journal of Methods of Information in Medicine 2007 Vol. 46(4) pp. 470-475.

[19] Neubauer, B. J. Introducing SOA and Workflow Modeling to Non-technical Students. JCSC Vol. 22(4): pp. 101–107, 2007.

[20] Guidi, C., Lucchi, R. & Mazzara, M. A Formal Framework for Web Services Coordination. Electronic. Notes Theor. Comput. Sci., Vol. 180(2), pp.55–70, 2007.

[21] Ardissono, L., Petrone, G & Segnan, M. A Conversational Approach to the Interaction with Web Services. Computational Intelligence, Vol. 20(4), pp. 693–709, 2004.

[22] N. Bieberstein, S. Bose, M. Fiammante, et al. Service-Oriented Architecture Compass: Business Value, Planning, and Enterprise Roadmap. Pearson Education, Upper Saddle River, NJ, p.215. 2006

[23] Champion, M., Ferris, C. & Newcomer, E. et al (2002). Web Service Architecture. W3C Working Draft 2002 Available: http://www.w3.org/TR/2002/WD-ws-arch-20021114/

[24] Erl, T., SOA Principles of Service Design, USA, Prentice Hall, 2009.

[25] D. Kayne, Loosely Coupled, The Missing Pieces of Web Services. Dublin: RDS Press 2003.

[26] P. Eugster, P, Felber, & R. Guerraoui, et al "Event systems. How to have your cake and eat it too" 22nd International Conference on Distributed Computing Systems, Workshops (ICDCSW '02), 2002.

[27] R. Krummenacher, E. Simperl, and D, Fensel "Towards Scalable Information Spaces", Workshop on New forms of reasoning for the Semantic Web: scaleable, tolerant and dynamic. International Semantic Web Conference, 2007.

[28] R. T. Fielding,. Architectural Styles and the Design of Network-based Software Architectures. Doctoral dissertation, University of California, Irvine, 2000.

[29] Curbera, F., Duftler, M., Khalaf, R. et al (2002). Unravelling the Web Services Web An Introduction to SOAP, WSDL, and UDDI [Online] Available: http://www.cc.gatech.edu/classes/AY2004/cs6210_fall/ papers/ 00991449.pdf

[30] Rodriquez, A. (2008) RESTful Web services: The basics [Online] Available: https://www.ibm.com/developerworks/webservices/library/ws-restful/

[31] M. D. Hansen, SOA Using Java Web Services. Upper Saddle River, NJ: Pearson Education, 2007

[32] Endrei, M., Ang, J., Arsanjani, A. et al (2004). Patterns: Service Oriented Architecture and Web Services [Online] Available: http://www.redbooks.ibm.com/redbooks/pdfs/sg246303.pdf [Accessed 7 Feb 2011]

[33] F. Jammes, A. Mensch, and H. Smit, Service-Oriented Device Communications Using the Devices Profile for Web Services. In 3rd International Workshop on Middleware for Pervasive and Ad-Hock Computing, November 2005.

[34] Newcomer, E. & Lomov, G, Understanding SOA with Web Services. Upper Saddle River, NJ USA: Pearson, 2005 Pp. 96-97.

[35] Communication of 13 February 2008 from the Commission to the European Parliament, the Council, the European Economic and Social Committee and the Committee of the Regions: Examining the creation of a European border surveillance system (EUROSUR) [COM(2008) 68 final].

DSiP Distributed Systems intercommunication Protocol - A Traffic Engineering Solution for Secure Multichannel Communication

JOHN HOLMSTRÖM*, JYRI RAJAMÄKI** & TAINA HULT**
*Ajeco Ltd.
Arinatie 10, FI-00370 Helsinki
FINLAND
**Laurea University of Applied Sciences
Vanha Maantie 9, FI-02650 Espoo
FINLAND
john.holmstrom@ajeco.fi http://www.ajeco.fi/index.php?language=eng

Abstract: - The importance of reliable telecommunication is constantly increasing. The DSiP-solution makes it possible to distribute all telecommunication among several operators and methods, resulting in a true multichannel communication system. The DSiP-multichannel routing solution increases reliability, security and integrity in telecommunication and allows regular communication methods to be used in mission critical telemetry systems. This is achieved by splitting risks between operators and communication channels; better routing capabilities; taking security and intrusion risks into account; and adding modularity.

Key-Words: - Data communications, Data security, Data traffic engineering, IP, IP networks, Public safety, Security, Security communications

1 Introduction

The two persons who contributed big time to the existence of the Internet are Robert E. Kahn and Vinton Cerf. The Internet was developed in the early 70's. The Internet Protocol (IP) is a good protocol, but no one could foresee the need and amount of communication we have today. Some email applications came in the 80's. Tim Berners Lee specified HTML and wrote a browser in 1990.

Today, the most cost-efficient way to globally transport data is achieved by using networks based on the IP-protocol. Also, multi-path routing for IP networks has been explored for many years in order to mitigate the effect of congestion in the network. Today, many IP-based solutions have been developed for business critical applications. They are used around the world to help companies to make sure that their business critical Internet connections and VPN-tunnels are always online. Sophisticated multichannel systems are constantly monitoring critical traffic having capabilities for using alternative routes if data traffic problems are encountered in the network.

2 Problem Formulation

Fig. 1 shows how a typical multi-modem remote application works. All modems will get their own IP-address from their operators and the control room application will see connection attempts from multiple IP-addresses. This kind of a multi-modem system cannot share communication between different physical media without rewriting the application software to do so, because IP does not support multichannel communications by maintaining simultaneous socket connections over multiple physical media. The rewriting an application software to support multichannel communications is a very challenging task.

A typical security problem many times preventing Virtual Private Networks (VPN) from being used in a multi-modem data communication environment, is that VPN solutions typically allow for creating a secure link over only one physical media at a time. If the media encounters problems, the VPN must be re-established over another media. These limitations are related to IP-addressing issues and how the IP-stack handles socket connections.

2.1 Research Question

The IP-protocol is a great protocol for transporting data but it is not enough when considering mission critical or highly important systems. For that reason, the research question (RQ) of this study is formulated:

ISBN: 978-960-474-286-8

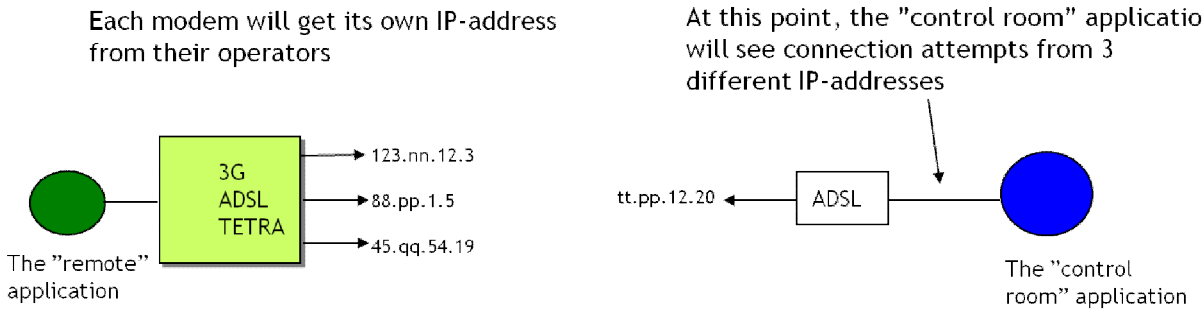


Fig. 1 Typical Multi-modem System

RQ: Is there any solution that allows also regular communication methods to be used in mission critical telemetry systems?

3 Problem Solution

The new multichannel data communication concept provides a uniform way to communicate over virtually any type of communications media in such a way that multiple, sometimes parallel communication paths appear as a single robust, secure and reliable communication link between communicating peers.

Our proposed solution is based on the Distributed Systems intercommunication Protocol® (DSiP) [1] which handles communication channel selection and hides link establishment issues from devices and/or software that wish to communicate with each other using the DSiP solution. DSiP is simultaneously a protocol-level and routing-level traffic engineering software solution for intelligently handling data routing, using all kinds of physical media, including IP and non-IP communication. It increases dramatically the reliability, security and controllability of communication systems being completely independent from operators. DSiP can be regarded as a traffic engineering layer above the regular IP-layer – "the missing OSI layer".

DSiP allows for:

1. Combining and using telecommunication methods in parallel so that multiple connections appear like a single reliable connection. DSiP can route data over both IP- and non-IP connections.
2. DSiP is independent from operators. It allows the user to shop and combine telecommunication from any operator.
3. DSiP contains protocol translation methods making equipment, systems and software compatible.
4. DSiP implements security mechanisms as well as reduces risk for DOS attacks and virus-infusion.
5. DSiP has better control over data routing, priorities and services.

3.1 System Overview

Fig. 2 shows an overview of the DSiP telemetry system, which is capable of routing data over any kind of connection, IP and non-IP, and works in multi-operator environments applying satellites, 3G, GPRS, UMTS, HDSPA, IP-network, TETRA, serial connections and radio modems.

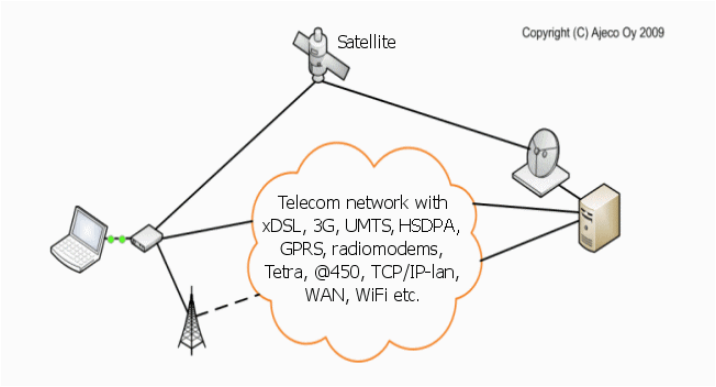


Fig. 2 DSiP Telemetry System

3.2 Robust and Secure Data Communications

The DSiP-protocol supports splitting a VPN tunnel over several physical media without the aforementioned constraints, as shown in Fig. 3. In addition, it solves incompatibility issues on both physical and logical levels in addition to providing modularity, data integrity, security and versatility to data communications systems ranging from small to very large size. By following a set of logical rules within the DSiP and by using IP as means for transport, applications, equipment and software from different vendors may intercommunicate transparently i.e. applications may respond to and ask for services without needing to know about

ISBN: 978-960-474-286-8

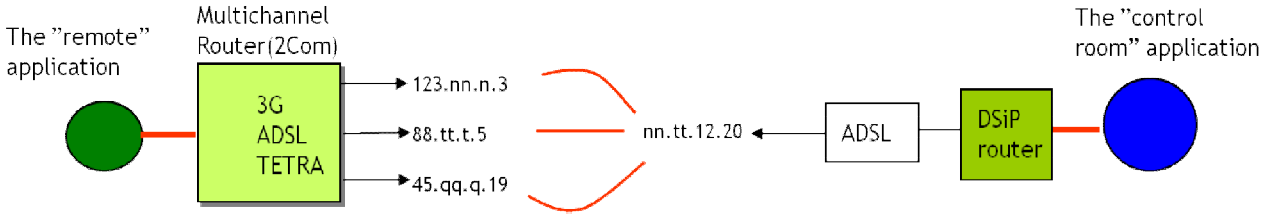


Fig. 3 DSiP Multichannel System

physical implementations [1]. The DSiP protocol enables an unbroken VPN link should traffic move to an alternative route with alternative physical media.

3.2 Modularity

A DSiP telemetry system always consists of three elements: the remote site, the telecommunication system and the command and control room. If one of these element changes, it do not affect the others, so DSiP solution is modular as Fig. 4 shows.

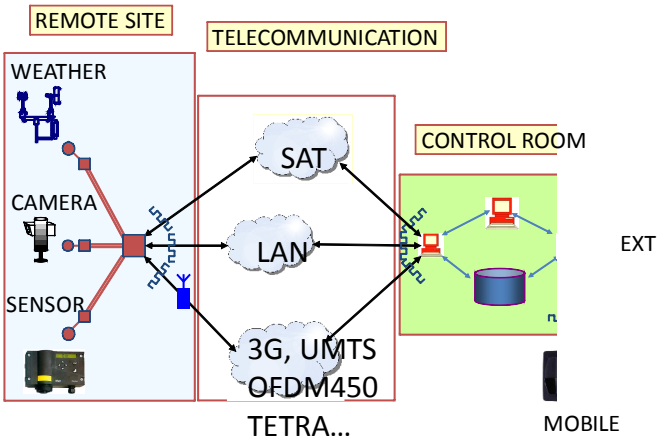


Fig. 4 Modularity of DSiP

4 Applications

4.1 SCADA Systems

DSiP is applied in controlling of Finland's main power grid. Furthermore, a major part of Vattenfalls power distribution network is managed and controlled by DSiP, AM08M RTU's and AM06T communication bridges. Power grid breakers are monitored and controlled by a SCADA-system via the DSiP-system. Fig. 5 shows how an operative system works.

4.2 Coast Guard Surveillance System

The Finnish Frontier & Coast Guard uses coastal surveillance cameras in order to continuously execute control and get telemetry information. The Finnish archipelago with its harsh climatic conditions put a lot of stress upon equipment installed in maritime surveillance systems. The DSiP-system allows for location independent operation i.e. control rooms can be placed at any desired location.

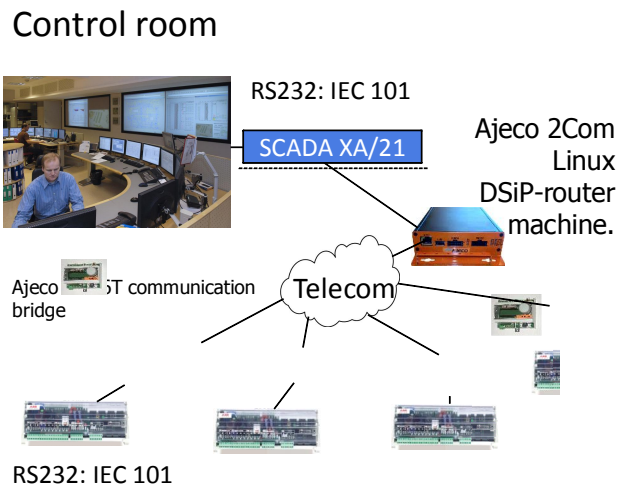


Fig. 5 DSiP-encapsulated IEC-messaging to electrical substations

DSiP is deployed, also, in the Integrated System for Interoperable sensors & Information sources for Common abnormal vessel behaviour detection & Collaborative identification of threat (I2C) integration project [2] and the Protection of European seas and borders through the intelligent use of surveillance (PERSEUS) demonstration project [3] both funded by EU's FP7.

4.3 Outdoor Lighting Control

The DVB-Gate-unit replaces ripple control receiver units in the power distribution network. It contains two communication interfaces: A DVB-T/H interface for receiving broadcasted commands and a GPRS interface for sensor- and energy meter feedback. The GPRS also acts as a reserve channel. The DSiP-system provides the data communication infrastructure together with its controller tasks and nodes.

ISBN: 978-960-474-286-8

5 Discussion

With DSiP, customers can use multiple communication channels in parallel in such a way, that ending peers ”think” they are using one channel. DSiP shares communication resources between different hardware equipment and software modules; automatically routes data and uses secondary routes if primary connections are broken. It always knows the correct sender and correct receiver and uses strong encryption and timestamps. So, DSiP makes communications more robust and improves data security.

With DSiP, customers have enhanced controlling possibilities: (1) control priorities – important information is routed first, less important later; (2) control over network timeouts – no undetermined delays or waits; (3) control the usage of communication and bandwidth – DSiP always ”knows” the condition of all routes; and (4) have better control over maintenance and configuration.

DSiP combines IP and non-IP communication into a single controllable system. Transparently communicate through DSiP-connections is reached, because DSiP allows tunneling of other protocols through itself. DSiP makes equipment and software compatible via very intelligent interface mechanisms.

Being independent from every single telecommunication operator, end-user could distribute the operator risk by using multi-operator network topology.

DSiP is not a heavy or difficult protocol to embed into various equipment and platforms. However, DSiP contains features like:

- Solutions for data-integrity and security and authentication
- Automatic re-routing of information via backup channels – redundancy
- A controllable method for multi & broadcasting – bandwidth control
- A standardized interface to software & equipment – solves compatibility issues
- Scalability – the system is very flexible – easily add new and old equipment & swr
- Complete independency of physical communication methods – any means for transmitting a bit is good
- Real-time online knowledge of the network topology – NO unwanted connection delays.

A DSiP testing environment is set up in Laurea University of Applied Sciences, which purpose is to test and demonstrate the functioning of the multichannel routing solution exploiting multiple communication paths in practice. By creating different problem situations, we are able to test the reliability and robustness of the communication system. So far, the results from the testing environment have been encouraging. Multiple connections over all tested types of media appear like a single ultra-robust communications channel. When one connection fails, DSiP easily finds another working route. The way how the new connections are created can be read from log files. However, this is not very illustrative and for that reason, we are developing new visualizing tools. [4]

6 Conclusion

The need for secure multichannel communication is global and exploding. DSiP is a solution that allows also regular communication methods to be used in mission critical telemetry systems. It also enables a combination of all kinds of telecommunication resources: IP traffic and non-IP traffic over TETRA, radio links, satellite communications, serial connections etc. can all co-exist forming a single maintainable system.

References:

[1] M. Nordman, M. Lehtonen, J. Holmström, K. Ramstedt and P. Hämäläinen, ”A TCP/IP communication architecture for distribution network operation and control”, in Proc. of the 17th Internal Conference on Electricity Distribution, Barcelona, Spain, May 12-15, 2003.

[2] M. Morel and S. Claisse, “Integrated System for Interoperable sensors & Information sources for Common abnormal vessel behaviour detection & Collaborative identification of threat (I2C)” in Proc. of the Ocean and Coastal Observation: sensors and observing systems, numerical models and information systems, Brest, France, June 21-23, 2010.

[3] Demonstration project on the Surveillance of the EU Sea Borders, by Europolice on 22. January2011, Available: http://euro-police.noblogs.org/2011/01/demonstration-project-on-the-surveillance-of-the-eu-sea-borders/

[4] J. Rajamäki, J. Holmström and J. Knuuttila, Robust Mobile Multichannel Data Communication for Rescue and Law Enforcement Authorities, Proc. of the 17th Symposium on Communications and Vehicular Technology in the Benelux, ,Twente, The Netherlands Nov. 24-25, 2010.

The future solutions and technologies of public safety communications - DSiP traffic engineering solution for secure multichannel communication

John Holmström, Jyri Rajamäki and Taina Hult

***Abstract*—** Importance of reliable telecommunication is constantly increasing. A new multichannel data communication concept presented in this paper, provides a uniform way to communicate over virtually any type of communications media in such a way that multiple, sometimes parallel communication paths appear as a single robust, uninterruptable, secure and reliable communication link between communicating peers. The solution named DSiP (Distributed Systems intercommunication Protocol) makes it possible to distribute all telecommunication among several operators and methods, resulting in a true multichannel communication system. The DSiP-multichannel routing solution increases reliability, security and integrity in telecommunication and allows regular communication methods to be used in mission critical telemetry systems. This is achieved by splitting risks between operators and communication channels; better routing and priority capabilities; taking security and intrusion risks into account; and adding modularity.

***Keywords*—**Data communications, Data security, Data traffic engineering, IP networks, Public safety, Security communications

I. Introduction

Two persons who contributed big time to the existence of the Internet are Robert E. Kahn and Vinton Cerf. The Internet was developed in the early 70's. The Internet Protocol (IP) developed by Kahn and Cerf with their team, is generally a "good" protocol, but no one could foresee the need and amount of communication we have today. Some email applications came in the 80's. Tim Berners Lee specified HTML and wrote a browser in 1990.

Today, the most cost-efficient way to globally transport data is by using networks based on the IP-protocol. Multi-path routing for IP networks has been explored for many years in order to mitigate the effect of congestion in networks. Today, many IP-based solutions have been developed for business critical applications. They are used globally for helping companies ensuring business critical Internet connections and VPN-tunnels are always online. Sophisticated multichannel systems are constantly monitoring critical traffic having capabilities for using alternative routes if data traffic problems are encountered in the network. [1]

Operational tasks and working methods in organizations have evolved and changed over the years. Various communication devices, software, services and databases operating via Internet and via other connections have an increasingly greater role. It is important that all valuable data in the processes is uninterruptedly and reliable available anywhere at any time without problems.

There are many aspects that affect the overall security and reliability of information systems. Security and reliability risks should be taken into account when creating new, or when integrating existing systems. The aforementioned is imperative for example among critical control systems and when selecting the means for communication.

Communication has a critical role in many organizations. Especially among Fire, Search and Rescue (SAR) and Law Enforcement Authorities' (LEA), systems communication methods and channels play a key role, not to forget communication related to critical infrastructure of a society.

Cyber-, reliability- and security risks and threats related to communication systems and channels should be known and identified before making any decisions of procurement, for example. [2]

Risks, reliability and threats can be analyzed and identified from many different angles. The nature of secure and reliable critical communication depends on who you ask. With regard to business organizations and Civilian Authorities, their critical communication must typically use regular telecommunication operator capacity and stay "on-line" as much as possible. However, when considering for example Military tactical communication, regular telecommunication operators can't be used and tactical communication systems stay "on-line" as little time as possible. Both user groups need however to ensure that communications reliability, security,

Manuscript received April 21, 2011. This work was supported in part by Tekes – the Finnish Funding Agency for Technology and Innovation – as a part of the research project 40350/10 Mobile Object Bus Interaction (MOBI).

J. Holmström is with Ajeco Ltd., Arinatie 10, FI-00370 Helsinki, Finland (corresponding author to provide phone: +358-9-4770 470; fax: +358-9-4770 4799; e-mail: john.holmstrom@ajeco.fi).

J. Rajamäki is with the Laurea SID Leppävaara, Laurea University of Applied Sciences, Vanha maantie 9, FI-02650 Espoo, Finland. (e-mail: jyri.rajamaki@laurea.fi).

T. Hult is a student at Business Information Technology, Laurea University of Applied Sciences, Vanha maantie 9, FI-02650 Espoo, Finland. (e-mail: taina.hult@laurea.fi).

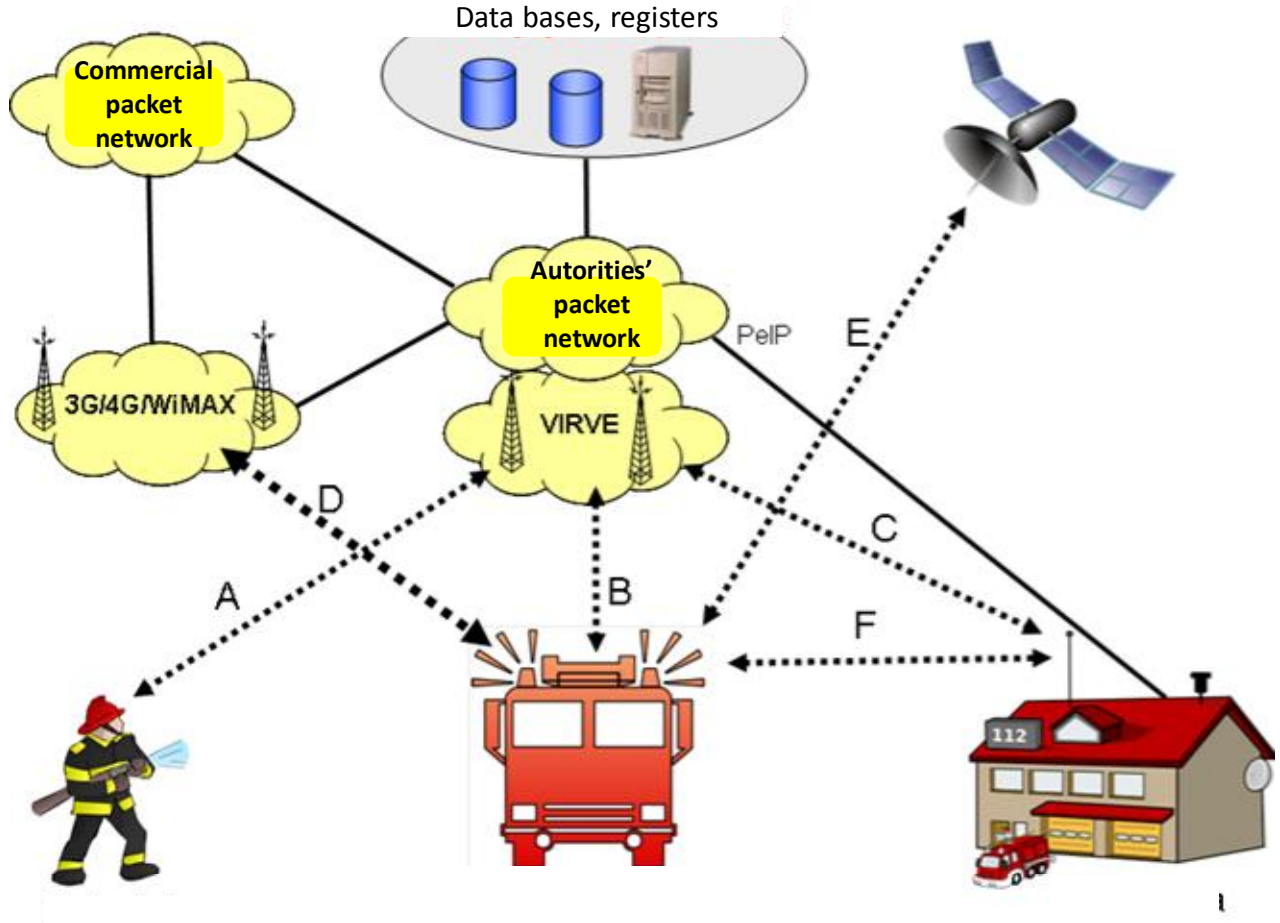
performance, interoperability, integrity, etc. are taken into account.

Integration of information systems is a current trend in all businesses and organizations [3]. The trend is towards larger more mobility and the Web plays a major role in providing critical business data, applications and services for mobile users. In this respect, service-level requirements play an important role in the process. However, service-level requirements are difficult to quantify during the project planning phase. The following intangible values could be used as guide lines for drawing up the operational constraints and goals required: 1) usability, 2) performance, 3) scalability, 4) reliability, 5 availability, 6) extensibility, 7) maintainability, 8) manageability, and 9) trustworthiness and security. Only after deployment, these attributes can be quantified. To meet pertinence requirements, the production (communication) system needs changing and tuning; if not possible, service-level requirements should be readjusted to conform the operational environment. The reason for the existence of any Web system is to support business and organizational needs. A shift of focus may be needed in any new project and Web architecting activities should be given more effort, attention and seriousness. [4]

A. The Communication Needs of Public Safety Authorities

According to [5], the Communication Needs of Public Safety Authorities are: 1) reliable and robust voice communication everywhere, 2) allowing for co-operation and easy communication between all organizations, 3) short messaging for alarming, field task delivery and to secure the validity of the information, 4) file transfer from the place of incident to support sites as the command or 112 centers, and 5) offering of communication from the field for daily office work.

Urban societies need communications to maintain essential services, even during emergencies. Citizens demand safety and security, which can only be delivered by efficient public agencies with access to reliable and secure group (one-to-many) communication. Professionals rely on mission-critical communications to help working together, optimizing



A: TETRA air interface of handheld radio
B: TETRA air interface of vehicle radio/modem
C: TETRA air interface of station radio/modem
D: Air interface for commercial networks
E: SATCOM
F: WLAN Interface between Rescue vehicle and Fire station LAN/Intranet

Fig. 1 Interfaces of wireless communications in the field of fire and rescue services [7]

situational awareness, response time and control when facing challenging situations. Taskforces need the support of secure, uninterrupted voice and data services. Professional mobile radio (PMR) is field radio communications using portable, mobile phones, base stations, and dispatch console radios. Analog PMR systems are regularly not protected against eavesdropping and offer limited voice quality. The operation of digital PMR radio equipment is typically based on standards such as TETRA and TETRAPOL. Key features of professional mobile radio systems can include [6]: 1) point to multi-point communication, 2) push-to-talk, release to listen, 3) large coverage areas, 4) closed user groups, and 5) use of VHF or UHF frequency bands. Fig. 1 shows the interfaces of wireless communications in the field of fire and rescue services.

B. TETRA and TETRAPOL

The Terrestrial Trunked Radio (TETRA) standard has been implemented and developed by the European Telecommunications Standards Institute (ETSI). The TETRA standard can be described as a suite of standards. In practice, these standards cover different technology aspects such as for example air interfaces, network interfaces and services and facilities.

TETRA is a worldwide standard and there exist hundreds of TETRA networks across the world. TETRA systems have many advantages. One advantage is its Interoperability Certification requirement. TETRA can be used and shared by all public safety organizations hence being an economic solution. It offers secure communication channels during emergency situations and disasters. TETRA is a fully digital system, which offers high-quality voice in addition to a wide range of possibilities for data transfer. TETRA also supports voice and circuit switched and packet-switched data transmission with different bit rates and error-correction levels.

A TETRA system is based on virtual private network technology. It offers one physical network which can be shared among different organizations. In practice, each user group is able to utilize a TETRA based network as it would only be available to the group.

The nature of a crisis event affects the usable media. For example in case of a sudden panic event, the public cellular technology is useless. A large crowd (rock concert, hockey game etc.) will load the public cellular net heavily due to the concentration of mobile phones under a limited number of

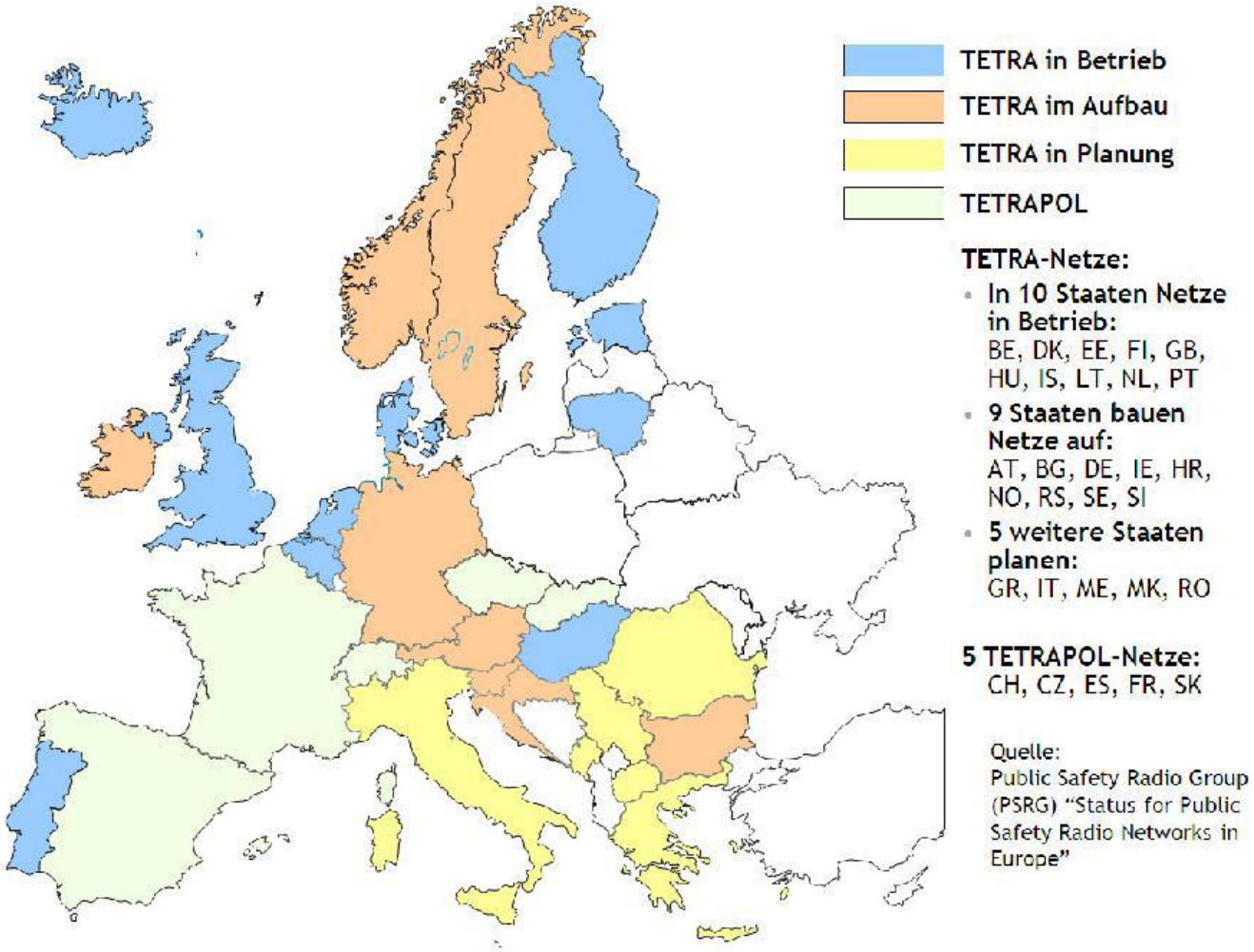


Fig. 2 The nation-wide PMR networks in Europe [8]

base stations - a minor crisis event in this kind of situation may allow for using dispersed public communication channels. And, finally, public cellular technology will most probably remain useful and intact during, for example, an oil disaster due to the large geographic area of the latter.

Regardless of many inevitable advantages in TETRA based networks, being economic and working under all circumstances, it has a disadvantage which is: heavily limited data capacity.

TETRAPOL is another digital PMR technology standard for mission-critical public safety users. The main difference between TETRA and TETRAPOL is that TETRA makes use of the available frequency allocations using Time Division Multiple Access (TDMA) technology with four user channels on one radio carrier with 25 kHz spacing between carriers. TETRAPOL's air interface is based on Frequency Division Multiple Access (FDMA) radio access and Gaussian Minimum Shift Keying (GSMK) modulation.

Fig. 2 shows the nation-wide PMR networks in Europe. TETRA networks are in operational use in Finland, UK, The Netherlands, Belgium, Hungary, Eastland, Lithuanian, Denmark and Portugal.

C. Multichannel Communication

The introduction of the VIRVE network in Finland has enabled a high level of multi-authority co-operation at the (incident) scene. All authority actors have the same basic needs for the system and data communication, but also have own distinct requirements. An intention for finding mutual solutions and operation models, facilitating system integration and enabling coherent system design, exist; improved activities, cost savings, improved multi-authority co-operation at the scene are of desire. [9]

The voice services of the VIRVE network are working well with high reliability, fast connection setup and good coverage. Customers are generally satisfied and in the near future, no major changes in the voice services are foreseen. Furthermore, data services are reliable and the coverage is good. However, the VIRVE data services are of low capacity with customers being unsatisfied with this performance in VIRVE. Improvements to the low data capacity are not visible in the near future that would fulfill the need. The possibility of TETRA Enhanced Data Service (TEDS) upgrade may bring partial solutions to the limited data capacity. [7]

According to [7], the roles of complementary technologies in the future are as follows:

1) Datame (@450/ WiMAX/CDMA,LTE) has good coverage and usability according to tests performed by Police authorities. However, there is uncertainty of the future existence of this radio technology.
2) 2G/EDGE/GPRS technologies are reaching the end of their life cycle.
3) 3G/HSPA technology has good coverage with U900 (better than 2G). However, there are problems on the availability/capacity of commercial networks during major accidents in crowed areas.
4) The first 4G/LTE networks will be at 2.6 GHz, which is not suitable for rural coverage. Future, 800MHz LTE/4G systems are anticipated.
5) WLAN technology has three user cases for data transfer: 1) Vehicle - Fire station at the garage, 2) Local wireless network around fire truck at the scene, and 3) Vehicle - public WLAN:"WLAN fire plug".
6) Satellite technology has a complementary role when there is no terrestrial coverage. This includes long term usage when not available other way, and satellite transmission for temporary site. The telecommunication operator TeliaSonera has announced a start of EutelSat KA-SAT services in june 2011. The service may however be of limited use in Authority communication applications due to the requirement of a relatively large-size satellite dish antenna, limiting the usability of the service in moving vehicles.

In Europe, the present state of public safety communications is that TETRA/TETRAPOL is the best choice for voice communication for authorities having virtually no competitors. On the other hand, the data communication capacity over TETRA does not fulfill growing future needs; however the slow data is robust and works well. Wideband data (=TEDS) is possible to implement in the future but does not solve all problems. The planned TETRA Rel. 3 is not available before 2020 and includes some degree of uncertainty regarding implementation. The aforementioned effectively means that in addition to TETRA, complementary data transfer technologies are needed; choices of today and near future include3G/HSPA, 4G/LTE, WLAN and Satellite Communication.

The 450 MHz band formerly used for cellular NMT technology is today used by Flash OFDM 450 technology in Finland. The 450 MHz bandwidth has a good penetration capability and the cell size of the @450 network is relatively large. There are however concerns about if the Flash OFDM technology will prevail. An alternative technology could be CDMA operating at the 450 MHz band. Regardless of the 450 MHz band with OFDM prevailing or not; there is presently a strong demand for dedicated broadband capacity among authorities. [7]

The solution to ensure quality of critical communication is to use several communication paths provided by several operators. Parallel use of communication channels data links, regardless of technology, solves many problems. The progress of technology is enabling alternative channels for communication.

The big questions are, how much should and could public safety responders rely on commercial broadband services? What is the availability of public networks during major accidents? The aforementioned means that a multichannel router or terminal must intelligently and constantly be aware of usable network resources and coverage (TETRA, 3G, 4G, WiMAX, WLAN, etc.) Furthermore "WLAN - fire plug" availability should also be taken into account.

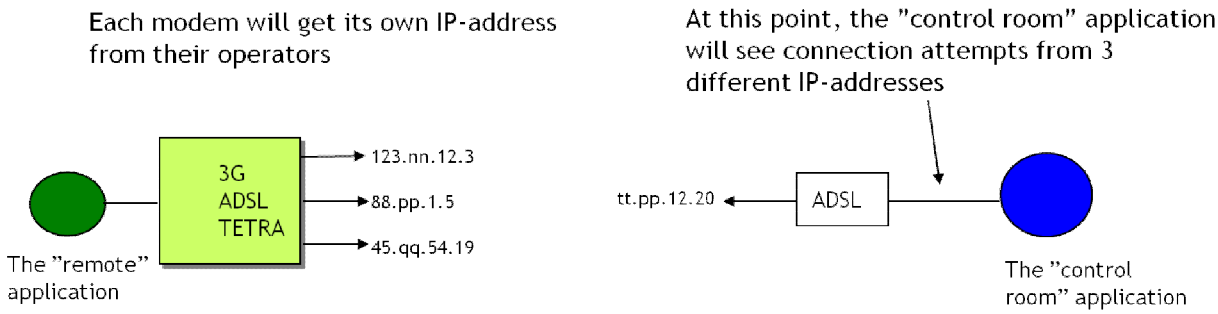


Fig. 3 Typical Multi-modem System

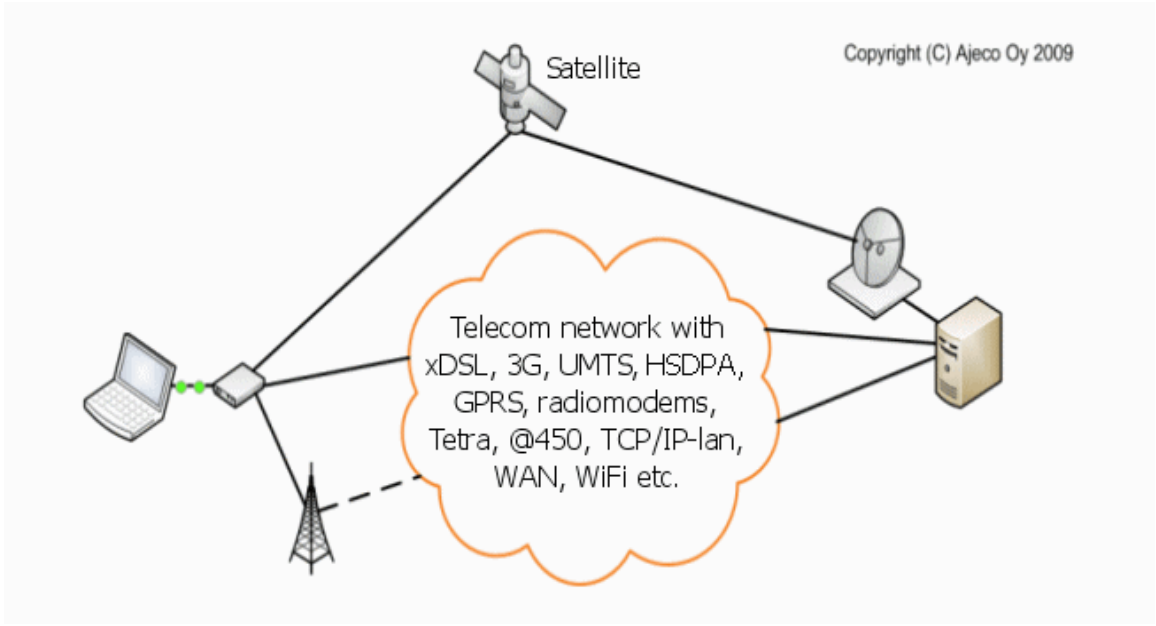


Fig. 4 DSiP Telemetry System

II. Problem Formulation

Fig. 3 shows how a typical multi-modem remote application works. All modems will get their own IP-address from their operators and the control room application(s) will see connection attempts from multiple IP-addresses. This kind of a multi-modem system cannot share communication between different physical media without rewriting the application software to do so, because IP does not support multichannel communications by maintaining simultaneous socket connections over multiple physical media. Rewriting an application software to support multichannel communications is a very challenging task.

A typical security problem many times preventing Virtual Private Networks (VPN) from being used in a multi-modem data communication environment, is that VPN solutions typically allow for creating a secure link over only one physical media at a time. If the media encounters problems, the VPN must be re-established over another media. These limitations are related to IP-addressing issues and how the IP-stack handles socket connections.

A. Research Question

The IP-protocol is a great protocol for transporting data but it is not enough when considering mission critical or highly important systems. For that reason, the research question (RQ) of this study is formulated:

RQ: Is there any solution that allows also regular communication methods to be used in mission critical telemetry systems?

III. Problem Solution

The new multichannel data communication concept provides a uniform way to communicate over virtually any type of communications media in such a way that multiple, sometimes parallel communication paths appear as a single robust, secure and reliable and unbreakable communication link between communicating peers.

Our proposed solution is based on the Distributed Systems intercommunication Protocol® (DSiP) [10] which handles communication channel selection and hides link establishment issues from devices and/or software that wish to communicate with each other using the DSiP solution. DSiP is simultaneously a protocol-level and routing-level traffic engineering software solution for intelligently handling data routing, using all kinds of physical media, including IP and non-IP communication. It increases dramatically the reliability, security and controllability of communication systems being completely independent from operators. DSiP

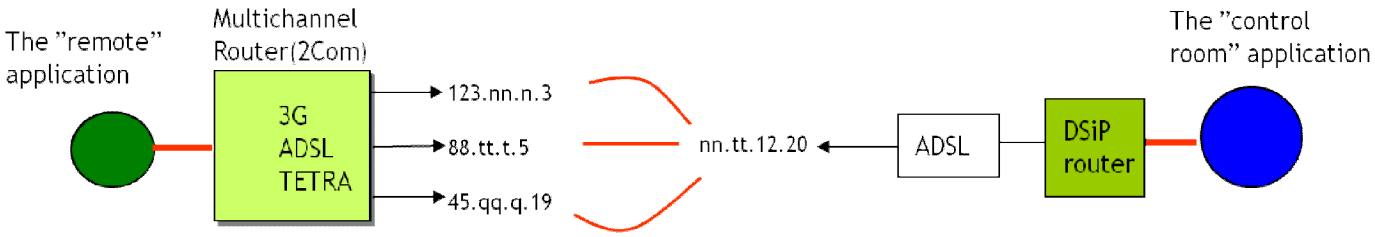


Fig. 5 DSiP Multichannel System

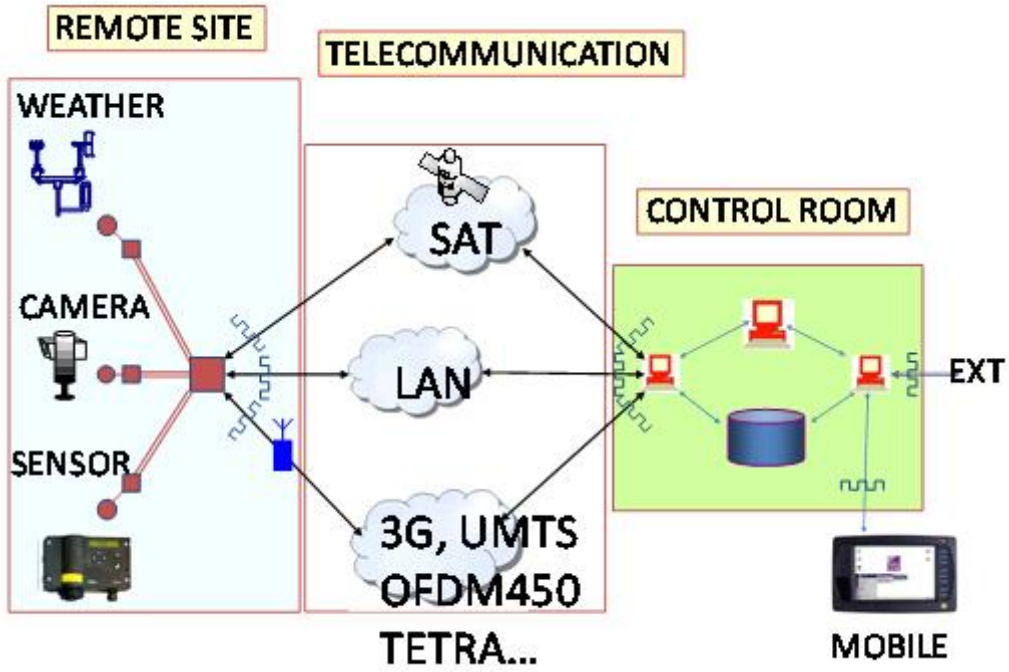


Fig. 6 Modularity of DSiP

can be regarded as a traffic engineering layer above the regular IP-layer – "the missing OSI layer".

DSiP allows for:

1) Combining and using telecommunication methods in parallel so that multiple connections appear like a single reliable and unbreakable connection. DSiP can route data over both IP- and non-IP connections.
2) DSiP is independent from operators. It allows the user to shop and combine telecommunication from any operator.
3) DSiP contains protocol translation methods making equipment, systems and software compatible.
4) DSiP implements security mechanisms as well as reduces risk for DOS attacks and virus-infusion.
5) DSiP has better control over data routing, priorities and services.

A. System Overview

Fig. 4 shows an overview of the DSiP communication system, which is capable of routing data over any kind of connection, IP and non-IP, and works in multi-operator environments applying satellites, 3G, GPRS, UMTS, HDSPA, IP-network, TETRA, serial connections and radio modems.

B. Robust and Secure Data Communications

The DSiP-protocol supports splitting on a VPN tunnel over several physical media simultaneously without the aforementioned constraints, as shown in Fig. 5. In addition, it solves incompatibility issues on both physical and logical levels in addition to providing modularity, data integrity, security and versatility to data communications systems ranging from small to very large size. By following a set of logical rules within the DSiP and by using IP or any bit transferring channel (e.g. radio modems) as means for transport, applications, equipment and software from different vendors may intercommunicate transparently i.e. applications may respond to, and ask for services without needing to know about physical implementations [10]. The DSiP protocol maintains a VPN link regardless of changes in the used physical media i.e. VPN works during channel switches.

C. Modularity

A DSiP telemetry system always consists of three elements: the remote site or LAN segment, the telecommunication system and the command and control room or local LAN segment. If one of these element changes, it does not affect the others, as the DSiP solution is highly modular as Fig. 6 shows.

IV. Applications

A. SCADA Systems

DSiP is applied in the SCADA control of Finland's main power grid. Furthermore, a major part of Vattenfalls power distribution network in Finland is managed and controlled by DSiP, AM08M RTU's and AM06T communication bridges. Power grid breakers are monitored and controlled by a SCADA-system through the DSiP-system. Fig. 7 shows how an operative system works.

B. Coast Guard Surveillance System

The Finnish Frontier & Coast Guard uses coastal surveillance cameras in order to continuously execute control and get telemetry information. The system is an important part of general surveillance and SAR, has an operative status as must remain working on a 365/24/7 basis. The DSiP-system allows for location independent operation i.e. control rooms can be placed at any desired location.

DSiP is also a central communications solution in the Integrated System for Interoperable sensors & Information sources for Common abnormal vessel behaviour detection & Collaborative identification of threat (I2C) - integration project [11] and the Protection of European seas and borders through the intelligent use of surveillance (PERSEUS) demonstration project [12] both funded by EU's FP7 security program.

C. Outdoor Lighting Control

A pilot project has been conducted with Helsingin Energia regarding control of outdoor lighting using Mobile Television Broadcast (DVB-H) as transmission media for DSiP control packets and GPRS as return channel. The DVB-Gate-unit replaces ripple control receiver units in the power distribution network. It contains two communication interfaces: A DVB-T/H interface for receiving broadcasted commands and a GPRS interface for sensor- and energy meter feedback. The GPRS also acts as a backup channel. The DSiP-system provides the data communication infrastructure together with controller tasks and nodes.

V. Discussion

With DSiP, customers can use multiple communication channels in parallel in such a way, that ending peers "think" they are using one channel. DSiP shares communication resources between different hardware equipment and software modules; automatically routes data and uses secondary routes if primary connections are broken. It always knows the correct sender and correct receiver and uses strong encryption and timestamps. DSiP makes communication more robust and improves data security. The DSiP may be regarded as a secure and reliable multi-point to multi-point communication system with VPN characteristics.

IP traffic and its packets have methods for controlling priority, or perhaps better, quality. The IP QoS (Quality of Service) is however either not supported at all, or, supported in non-conforming ways in operator traffic. Customers using DSiP have enhanced controlling possibilities for controlling the data flow i.e. traffic: (1) control priorities – important information is routed first, less important later; (2) control over network timeouts – no undetermined delays or waits; (3) control the usage of communication and bandwidth – DSiP always "knows" the condition of all routes; and (4) have better control over maintenance and configuration; and (5) the DSiP system has in-built congestion control and (6) routing services based on cost-factors enabling certain, less important traffic to be filtered should the used communication be of low capacity for example.

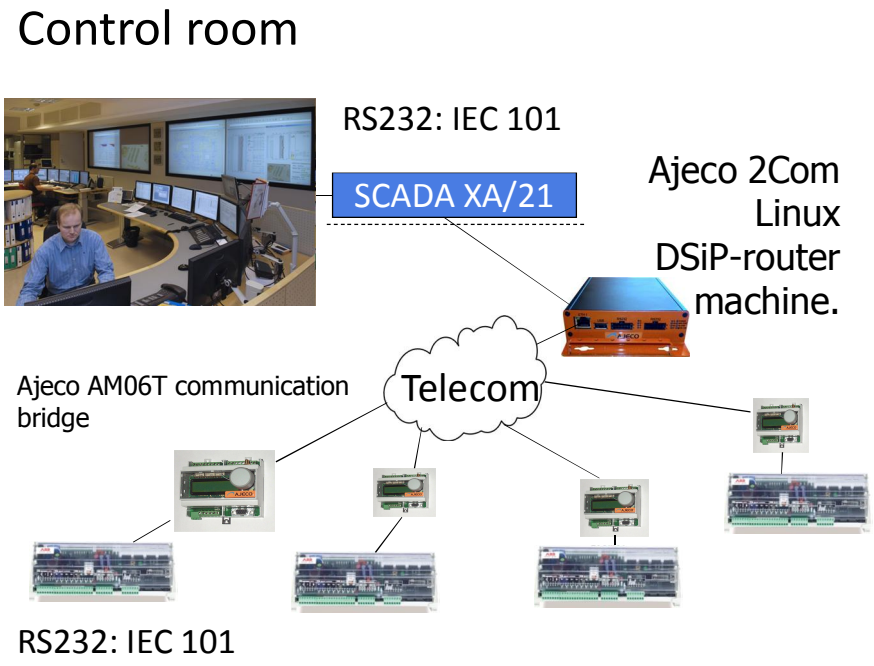


Fig. 7 DSiP-encapsulated IEC-messaging to electrical substations

DSiP can combine and use IP and non-IP communication links and also tunnel IP traffic through non IP connections. DSiP allows for tunneling of other protocols through itself and can make equipment and software compatible via intelligent interface mechanisms.

Being independent from every single telecommunication operator, and virtually any physical method, end-users could distribute the operator risk by using multi-operator network topology.

DSiP is not a heavy or difficult protocol to embed into various equipment and platforms. However, DSiP contains features like:

- Solutions for data-integrity and security and authentication
- Automatic re-routing of information via backup channels – redundancy
- A controllable method for multi & broadcasting – bandwidth control
- A uniform interface to software & equipment – solving incompatibility issues
- Scalability – the system is very flexible – easily add new and old equipment & swr
- Complete independency of physical communication methods – any means for transmitting a bit is good
- Real-time online knowledge of the network topology – NO unwanted connection delays.
- Centralized authentication-, Network management- and Configuration server software – tools for maintaining the system.

A DSiP test environment is set up in Laurea University of Applied Sciences, with the purpose of testing and demonstrating the functions of the multichannel routing solution exploiting multiple communication paths in practice. By creating different problem situations, we are able to test the reliability and robustness of the communication system. So far, the results from the testing environment have been encouraging. Multiple connections over all tested types of media appear like a single ultra-robust communications channel. When one connection fails, DSiP easily finds another working route. The way how the new connections are created can be read from log files. However, this is not very illustrative and for that reason, we are developing new visualizing tools. [13]

VI. Conclusion

With regard to European mission-critical public safety communications, TETRA/TETRAPOL is the best choice for voice communication and in the near future, it has no competitors. Data communication over TETRA is rather slow and does not fulfill future needs even though the low capacity communication can be considered very reliable. Wideband data "enhanced TETRA" (=TEDS) is potentially attractive but does not solve all problems. TERA Rel. 3 is not available before 2020 and has some degree of uncertainty regarding. The conclusion is that in addition to TETRA, complementary technologies are needed and multichannel communications is the answer.

The need for secure multichannel communication is global and exploding. DSiP is a solution allowing also regular communication methods to be used in mission critical communication systems. It also enables a combination of all kinds of telecommunication resources: IP traffic and non-IP traffic over TETRA, radio links, satellite communications, serial connections etc. can all co-exist forming a single uniform and maintainable system.

References

[1] J. Holmstrom, J. Rajamäki and T. Hult, "DSiP Distributed Systems intercommunication Protocol - A Traffic Engineering Solution for Secure Multichannel Communication" in Proc. 9th WSEAS International Conference on Applied Electromagnetics, Wireless and Optical Communications (ELECTROSCIENCE '11), Meloneras, Gran Canaria, Canary Islands Spain, March 24-26, 2011, pp.57-60.

[2] T. Hult and J. Rajamäki, "ICT Integration of Public Protection and Disaster Relief (PPDR): Mobile Object Bus Interaction (MOBI) Research and Development Project", in Proc. 9th WSEAS International Conference on Applied Electromagnetics, Wireless and Optical Communications (ELECTROSCIENCE '11), Meloneras, Gran Canaria, Canary Islands Spain, March 24-26, 2011, pp.143-148.

[3] D. Litan, A.-M. Mocanu, "Information systems integration, a new trend in business", ", in Proc. 9th WSEAS International Conference on Applied Electromagnetics, Wireless and Optical Communications (ELECTROSCIENCE '11), Meloneras, Gran Canaria, Canary Islands Spain, March 24-26, 2011, pp.250-256.

[4] S. Tumin, S. Encheva, "A brief look at Web architecting", in Proc. 9th WSEAS International Conference on Applied Electromagnetics, Wireless and Optical Communications (ELECTROSCIENCE '11), Meloneras, Gran Canaria, Canary Islands Spain, March 24-26, 2011, pp.245-249.

[5] J. Koivukoski, "What are the future solutions and technologies of national security communications?" VIRVE Day -seminar, Helsinki, Finland, March 2011.

[6] Professional mobile radio – Wikipedia, http://en.wikipedia.org/wiki/Professional_Mobile_Radio

[7] M. Rantama, Pelastustoimen langattoman tiedonsiirron tarpeet ja toteutusmahdollisuudet tulevaisuudessa, Pelastusopiston julkaisu, B-sarja: Tutkimusraportit 2/2011. http://www.pelastusopisto.fi/pelastus/images.nsf/files/A1933B8977CDAE26C22578570025B300/$file/Pelti%20loppuraportti%20liitteineen.pdf

[8] Bundesanstalt für den Digitalfunk der Behörden und Organisationen mit Sicherheitsaufgaben, htpp://www.bdbos.bund.de

[9] K. Junttila, "What are the future needs of mission critical communications at rescue services?" VIRVE Day -seminar, Helsinki, Finland, March 2011.

[10] M. Nordman, M. Lehtonen, J. Holmström, K. Ramstedt and P. Hämäläinen, "A TCP/IP communication architecture for distribution network operation and control", in Proc. of the 17th Internal Conference on Electricity Distribution, Barcelona, Spain, May 12-15, 2003.

[11] M. Morel and S. Claisse, "Integrated System for Interoperable sensors & Information sources for Common abnormal vessel behaviour detection & Collaborative identification of threat (I2C)" in Proc. of the Ocean and Coastal Observation: sensors and observing systems, numerical models and information systems, Brest, France, June 21-23, 2010.

[12] Demonstration project on the Surveillance of the EU Sea Borders, by Europolice on 22. January2011, Available: http://euro-police.noblogs.org/2011/01/demonstration-project-on-the-surveillance-of-the-eu-sea-borders/

[13] J. Rajamäki, J. Holmström and J. Knuuttila, Robust Mobile Multichannel Data Communication for Rescue and Law Enforcement Authorities, Proc. of the 17th Symposium on Communications and Vehicular Technology in the Benelux, ,Twente, The Netherlands Nov. 24-25, 2010.