Lääkelaitoksen julkaisusarja 1/2004

Terveydenhuollon laadunhallinta
Lääkintälaitejärjestelmien turvallisuus

Ilpo Pöyhönen
Kaarle Kylmälä

LÄÄKELAITOS
LÄKEMEDELSVERKET
NATIONAL AGENCY
FOR MEDICINES

Julkaisija:
Lääkelaitos
PL 55
00301 Helsinki
Puh. (09) 473 341
Faksi (09) 714 469
www.nam.fi

ISBN 952-5099-74-1
ISSN 1238-8777

Terveydenhuollon laadunhallinta

Lääkintälaitejärjestelmien turvallisuus

Ilpo Pöyhönen
Kaarle Kylmälä

TIIVISTELMÄ

Lääkintälaitteita liitetään yhä useammin yhteen laitejärjestelmiksi. Laitteiden ja järjestelmien suorituskyky kasvaa terveydenhuollon tietojen käsittelyn ja arkistoinnin digitalisoinnin yleistyessä.

Terveydenhuollossa käytettävien laitejärjestelmien turvallisuuteen vaikuttaa useita tekijöitä, mutta niiden tunnistaminen ei ole itsestään selvää. Kokonaisturvallisuuteen vaikuttavat myös laitteita ja järjestelmiä ympäröivät toimintaprosessit. Prosesseja on useita ja ainakin hankinta-, huolto- ja hoitoprosesseilla on välittömiä vaikutuksia turvallisuuden asettumiselle tietylle tasolle. Turvallisuuden määrittämisen ensimmäinen vaihe on tavoitteiden asettaminen. Jokainen organisaatio asettaa omat tavoitteensa ja luo puitteet tavoitteen saavuttamiseksi. Sisäinen yhteistyö eri henkilöstöryhmien ja toimintaprosessien välillä on tällöin tärkeää.

Konkreettisia keinoja tavoitteiden saavuttamisessa ja niiden ylläpitämisessä ovat toimintajärjestelmään kirjatut menettelytavat, toiminnan ohjaaminen prosessiksi tai toimintaketjuksi sekä koulutus. Toimintaketjuilla saavutetaan yhtenäiset toimintatavat koko yksikössä, jolloin kukin voi ymmärtää toiminnan kokonaisuutena. Toiminnan suunnitelmallisuus, hankintavaiheen määrittely, sopimukset, tuotteen elinkaaren hallinta, tarkistuslistojen käyttö sekä systemaattinen johdon hyväksymä riskienhallinta ovat keinoja, joilla käyttäjä voi nostaa toimintansa laatua ja turvallisuutta.

Lääkintälaitejärjestelmien kokonaisturvallisuuden kehittämisessä avainasemassa ovat laitteen elinkaaren hallinta, ohjelmistojen turvallisuus, riskienhallinta ja tietoturvallisuus.

SAMMANDRAG

Det blir allt vanligare att medicinteknisk utrustning sammanlänks till en systemhelhet. Utrustningens prestanda ökar i takt med att hälsovårdens databehandling och arkivering i allt högre grad sker elektroniskt.

Det finns många faktorer som påverkar den medicintekniska utrustningens säkerhet, men det är inte alltid självklara saker. De verksamhetsprocesser som omger utrustningen inverkar på säkerheten som helhet. Det finns flertal olika processer och man kan säga att åtminstone anskaffningen, service och vårdprocesserna har en direkt inverkan på säkerhetsnivån. Då man definierar säkerhet, är det första skedet att bestämma målsättningen. Varje organisation har sin egen målsättning och skapar förutsättningarna för den. Härvid är det interna samarbetet mellan olika personalgrupper och verksamhetsprocesser mycket viktigt.

För att nå och upprätthålla säkerhetsmålsättningen konkret, krävs planering av verksamheten, så att den utgör en systematisk process med bestämda, dokumenterade metoder och ett utbildningsprogram. Verksamheten ges en definition med enhetliga metoder för hela enheten, varmed alla berörda personer får en klarare bild av helheten. Användaren kan begagna sig av planmässighet, definierat anskaffningsförfarande, avtal, kontroll av utrustningens livscykel, checklistor och en av ledningen godkänd, systematisk riskkontroll, för att förbättra verksamhetens kvalitet och säkerhet.

Då man utvecklar säkerheten för medicinteknisk utrustning som helhet, är det avgörande faktorerna kontrollen av utrustningens livscykel, säkra program, riskhantering och informationssäkerhet.

ABSTRACT

Medical electrical equipment is frequently connected as medical electrical systems. The performance of equipment and systems is increasing as the data management and archiving is being digitised in the health care.

The safety of medical electrical systems used in health care is influenced by several factors, but their identification is not self-evident. For example, the processes surrounding the equipment and systems have an influence on the overall safety. From the many processes at least the procurement, maintenance and care processes have a direct effect on a certain safety level to be achieved. The first step in the determination of safety is the setting of targets. Every organisation sets its own targets and establishes the prerequisites for achieving them. Internal co-operation between various personnel groups and processes is then of an utmost importance.

The concrete means for the achievement and maintenance of these safety targets include the planning of the processes, documentation of the methods and education program. By defining the standard operating procedures in each unit everyone is able to understand the operation as a whole. Operational planning, specifications before procurement, contracts, management of the life cycle of equipment, use of checklists and systematic risk management approved by the management are the means, by which the user organisation is able to improve the quality and safety.

When developing the overall safety of the medical electrical equipment the key issue is the management of life cycle of the equipment, the safety of software, risk management and information security.

SISÄLLYSLUETTELO

1. JOHDANTO

Lääkintälaitteiden ja laitejärjestelmien rooli nykyaikaisessa hoitoketjussa on yhä suurempi. Järjestelmiä käytetään potilaan tilan monitorointiin, diagnosointiin tai hoitoon ja järjestelmien keräämää tietoa pyritään hallitsemaan laajojen tietojärjestelmien avulla. Hyvänä esimerkkinä on diagnostiset kuvantamisjärjestelmät, jossa digitaalisessa muodossa olevista kuvista tehdään diagnooseja ja lausuntoja. Tämän jälkeen ne talletetaan laajoihin tietokantoihin mahdollista uudelleen käyttöä varten.

Ohjelmistojen osuus laitejärjestelmissä kasvaa edelleen ja ohjelmistot suorittavat hyvin pitkälle näiden laitteistojen ohjausta ja hallintaa. Tämä kehitys on johtanut siihen, että valvovat viranomaiset joutuvat kehittämään uusia säädöksiä ohjelmistojen riittävän turvallisuuden ja suorituskyvyn toteamiseksi.

Valmistajan osalta muutokset teknologiassa ja uudet lainsäädännön vaatimukset ovat aiheuttaneet suunnittelun siirtymisen ns. tuotekehityksen elinkaarimallin noudattamiseen, jossa tuotteen suunnittelu aloitetaan esitutkimuksella. Tämän jälkeen edetään määrittelyn, suunnittelun, toteutuksen ja testauksen kautta itse tuotteen valmistukseen. Riskienhallinnan mukanaan tuomat vaatimukset ovat aiheuttaneet myös sen, että tuotteen käyttövaiheen aikana mahdollisesti esiintyvät ongelmat on myös otettava huomioon suunnitteluprosesseissa.

Käyttäjän mahdollisuudet vaikuttaa monimutkaisten järjestelmien turvallisuuteen ja luotettavuuteen voivat tuntua rajallisilta, mutta näin ei välttämättä tarvitse olla. Systemaattiset menettelytavat hankinnassa, hoitoprosesseissa, huollossa ja riskienhallinnassa sekä hankintojen tarkka määrittely ovat avainasemassa monimutkaisten laitteiden ja ohjelmistojen turvallisen ja oikean käytön varmistamisessa.

Tällaisen kulttuurin luominen voi vaatia organisaatiolta huomattavia käynnistyspanostuksia, mutta todennäköisesti investoinnit näkyvät hyvinkin nopeasti toimivimpina hoito-, huolto- ja hankintaprosesseina. Toisaalta myös toimintaprosessien eli toimintojen jäljitettävyys ja osoitettavuus paranee ja toimintaprosesseihin tehtävät muutokset ovat hallitumpia ja ne voidaan ottaa käyttöön nopeammin.

Tämä julkaisu perustuu Lääkelaitoksen ja VTT Tuotteet ja tuotannon terveydenhuollon tuotetekniikan tutkimusryhmän yhteistyössä vuosina 2002-2003 laatimaan selvitykseen. Julkaisun tavoitteena on tarjota opas-

tusta terveydenhuollon toimintayksiköissä käytössä olevien lääkintälaitejärjestelmien hallintaan. Julkaisu täydentää Lääkelaitoksen julkaisua 3/1998 ”Sähkökäyttöisten lääkintälaitejärjestelmien turvallisuus”.

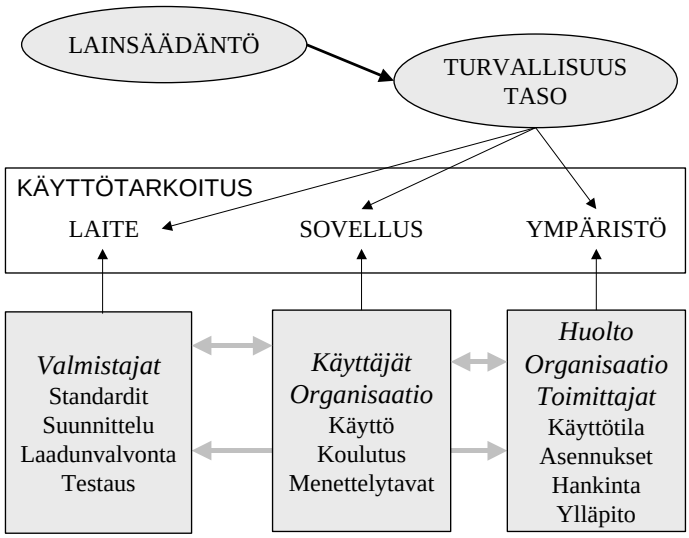
2. LAITEJÄRJESTELMIEN TURVALLISUUS

2.1 Vaatimukset

Terveydenhuollon laitteita ja tarvikkeita koskevan lain (1505/94) ja sen nojalla annettujen säädösten ja määräysten mukaan terveydenhuollon laitteet on suunniteltava ja valmistettava siten, että ne eivät suunnitelluissa olosuhteissa ja käyttötarkoituksen mukaisesti käytettyinä vaaranna potilaan terveydentilaa ja turvallisuutta eikä käyttäjän tai muun henkilön turvallisuutta ja terveyttä. Kaikista ei-toivotuista sivuvaikutuksista aiheutuvien riskien on oltava hyväksyttäviä terveydenhuollon laitteen suunniteltuun suorituskykyyn nähden. (riski-etu -tarkastelu). Näin ollen velvoitteet kohdistuvat ensisijassa valmistajalle. Toimivaltaiset viranomaiset arvioivat tarvittaessa tuotteiden kykyä täyttää asetetut vaatimukset.

Lain mukaan terveydenhuollon laitetta ja tarviketta on käytettävä valmistajan sille määrittämän käyttötarkoituksen mukaisesti. Ammattimaisen käyttäjän eli terveydenhuollon toimintayksikön ja terveydenhuollon ammatinharjoittajan on laitteen toimintakuntoisuuden varmistamiseksi huolehdittava siitä, että laite säädetään, ylläpidetään ja huolletaan asianmukaisesti.

Käyttäjäorganisaation on lisäksi huolehdittava siitä, että käyttöhenkilökunnalla on riittävä koulutus käyttää terveydenhuollon laitteita ja että laitteessa ja sen mukana on riittävät merkinnät ja käyttöohjeet. Lain asettamien vaatimusten täyttyminen voidaan kuvan 1 mukaan saavuttaa laitteen ominaisuuksilla sekä käyttöön ja ympäristöön vaikuttavilla toimintatavoilla ja menetelmäohjeilla. Täten kokonaisturvallisuuteen vaikuttavat useat eri tekijät ja käyttäjällä on merkittävä rooli turvallisuuden pitämisessä tietyllä tasolla.



***Kuva 1**. Turvallisuuteen vaikuttavia tekijöitä*

2.2 Käyttäjän mahdollisuudet varmistaa turvallisuus

Laitejärjestelmien käytön turvallisuuteen vaikuttavien tekijöiden löytäminen ei ole aina itsestään selvää. Kokonaisturvallisuuteen vaikuttaa lisäksi laitetta ja laitejärjestelmää ympäröivät toimintaprosessit. Prosesseista ainakin hankinta-, huolto-, laadunvarmistus- ja hoitoprosesseilla on välittömiä vaikutuksia turvallisuuden asettumisella tietylle tasolle. Turvallisuuden määrittämisen eräs lähtökohta on tavoitteiden asettaminen. Käytännössä jokainen organisaatio asettaa omat tavoitteensa ja luo puitteet tavoitteen saavuttamiselle. Tärkeää näiden tavoitteiden saavuttamisessa on sisäinen yhteistyö eri henkilöryhmien ja toimintaprosessien välillä.

Konkreettisina keinoina turvallisuustavoitteiden saavuttamisessa ja niiden ylläpitämisessä ovat toimintajärjestelmät, menetelmäohjeet sekä koulutus. Näillä toimintaa ohjataan toimintaprosessiksi tai toimintaketjuksi. Määriteltyjen toimintaketjujen avulla yhtenäinen toimintatapa saavutetaan koko yksikössä ja kukin taho voi ymmärtää toiminnan kokonaisuutena. Määriteltyjen toimintaketjujen etuina voidaan nähdä ainakin seuraavat seikat:

- uusimmat työkalut helposti ja keskitetysti löydettävissä,
- tehdään oikeat asiat oikein kerralla,
- selkeä vastuunjako toiminnan kehittämisessä,
- prosessien kehittäminen perustuu asiakkaiden ja henkilöstön tarpeisiin sekä
- organisaatiossa tapahtuvat muutokset siirrettävissä helpommin prosesseihin.

Toiminnan suunnitelmallisuus, hankintavaiheen määrittely, sopimukset, tuotteen elinkaaren hallinta, tarkistuslistojen käyttö sekä systemaattinen johdon hyväksymä riskienhallinta ovat keinoja, joilla käyttäjä voi nostaa toimintansa laatua ja turvallisuutta. Kokonaisturvallisuuteen voidaan vaikuttaa neljällä eri osa-alueella:

1) Riskienhallinta on toimintaa ohjaava ja valvova tukiprosessi, jonka avulla voidaan hallita toimintaa uhkaavia riskitekijöitä. Riskienhallinta käsittää useita eri elementtejä lähtien potentiaalisten vaarojen tunnistamisesta ja näihin liittyvien riskien arvioinnista aina tunnistettujen riskien vähentämisvaihtoehtojen valintaan (luku 3).
2) Järjestelmien ylläpito ja sähköturvallisuus. Järjestelmä käsitteenä on laaja ja välillä hieman epäselvä. Lisäksi kaikkia järjestelmien käyttöön liittyviä turvallisuusvaatimuksia ei kyetä määrittelemään

pelkästään standardin EN 60601-1 avulla. Järjestelmien turvallisuuteen vaikuttaa myös käyttöön, huoltoon ja ylläpitoon liittyvät tekijät (luvut 4 ja 5).

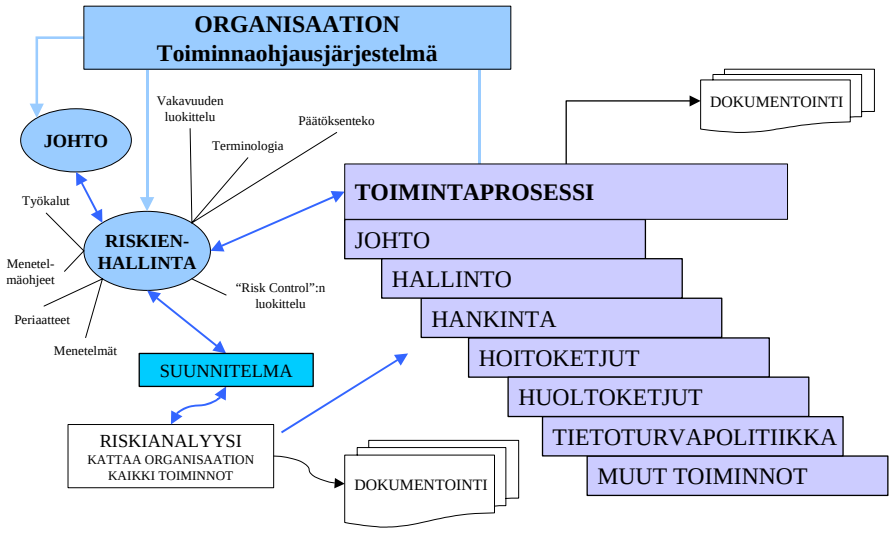
3) Laitteen tai laitejärjestelmän elinkaari. Käyttäjän kannalta elinkaari on riskienhallinnan ohella merkittävä apuväline, jolla monimutkaisten laitejärjestelmien turvallisuutta voidaan ylläpitää systemaattisesti. Elinkaarimallin tärkeitä vaiheita ovat esitutkimus ja määrittely, joilla varmistetaan myöhempien käyttövaiheiden toimivuus. Elinkaarimalli edellyttää myös ns. katselmuskäytäntöjen käyttöönottoa. Kullekin elinkaaren vaiheelle laaditaan selkeät tavoitteet, joiden täyttymistä arvioidaan katselmuskokouksissa (luku 5).
4) Ohjelmistojen turvallisuus. Terveydenhuollon laitteeseen tai laitejärjestelmään liittyviä ohjelmistoja suunniteltaessa ja valmistettaessa tulee kiinnittää huomiota siihen, että ohjelmistotuotannon elinkaarella ja sen vaiheistuksella on merkittävä osuus määriteltäessä tuotteen laatua, turvallisuutta ja luotettavuutta. Käyttäjän kannalta valmista reseptiä ostettavan ohjelmiston turvallisuuden takaamiseksi ei vielä ole olemassa. Luvuissa 6 ja 7 kuvataan joitakin keinoja ohjelmiston turvallisuuden ja suorituskyvyn varmistamiseksi.

3. RISKIENHALLINTA

3.1 Johdanto

Riskienhallinta on suunnitelmallinen, tiukasti toimintaa ohjaava ja valvova tukiprosessi, jonka avulla voidaan hallita toimintaa uhkaavia riskitekijöitä. Riskienhallinta käsittää useita eri elementtejä lähtien potentiaalisten vaarojen tunnistamisesta ja näihin liittyvien riskien arvioinnista aina tunnistettujen riskien vähentämisvaihtoehtojen valintaan. Tähän päästään sopivien riskien valvonta- ja vähentämiskeinojen valinnalla, käyttöönotolla ja valvonnalla. Nämä riskien valvontatoimenpiteet ja vaihtoehtoanalyysit ovat myös osa riskienhallintaa.

Riskienhallinta voi olla integroitu osaksi toimintaprosessia tai se voi olla kokonaan oma prosessinsa. Riskienhallintaprosessilla on oltava kuitenkin tietyt peruselementit, jotta se kykenee löytämään normaalitoiminnan heikkoja lenkkejä ja tätä kautta parantamaan organisaation toiminnan laatua. Kuvassa 2 on esitetty malli riskienhallintaprosessista. Johdon hyväksyntä ja sitoutuminen sanelevat ensisijaisesti riskienhallinnan toimivuuden. Koulutuksen, tiedottamisen ja yhteistyön avulla organisaation eri osastot ja henkilöryhmät saadaan tietoisiksi riskienhallinnasta ja sen tavoitteista. Tällöin riskienhallinnasta on mahdollista muodostaa systemaattinen, suunniteltu ja ohjeistettu prosessi, jolla on selkeät dokumentointivaatimukset. Prosessissa noudatetaan laadittuja periaatteita (hyväksyntä, hylkäys, menetelmät, ohjeet).



Kuva 2. *Malli riskienhallintaprosessille*

Eri organisaatioilla voi olla erilaisia tavoitteita ja vaatimuksia riskienhallinnan suhteen. Kunkin organisaation on pohdittava oman organisaatioon toimintamalliin parhaiten sopivat. Riskienhallinnalla on myös mahdollista parantaa organisaation toimintaa, mikä on riskienhallintamallia pohdittaessa ja suunniteltaessa syytä ottaa huomioon. Mahdollisia etuja voivat olla:

- Toimintaprosesseja voidaan parantaa ja systematisoida (analyysien avulla poistetaan häiriötekijät ja prosessin toistettavuus paranee).
- Vahingolliset tapahtumat eliminoidaan jo ennen niiden syntymistä (keskustelut, analyysit, riskianalyysien avulla päivitetyt rutiinit ja menetelmäohjeet).
- Menetelmän avulla löydetään mahdollisia organisatorisia ongelmia (ongelmat tiedon kulussa eri osastojen ja henkilöiden välillä, erilaiset menetelmät ja käytännöt, analyysitilanteet, puutteellinen menetelmäohjeiden noudattaminen, puutteelliset tietoturvaratkaisut tai tietoturvapolitiikan puuttuminen).
- Ulkoisten vaatimusten hallinta. Esimerkiksi vakuutusyhtiöt voivat edellyttää riskienhallintaprosessin käyttöönottoa korvauskäytäntöjen tai vakuutusmaksujen ehtona.

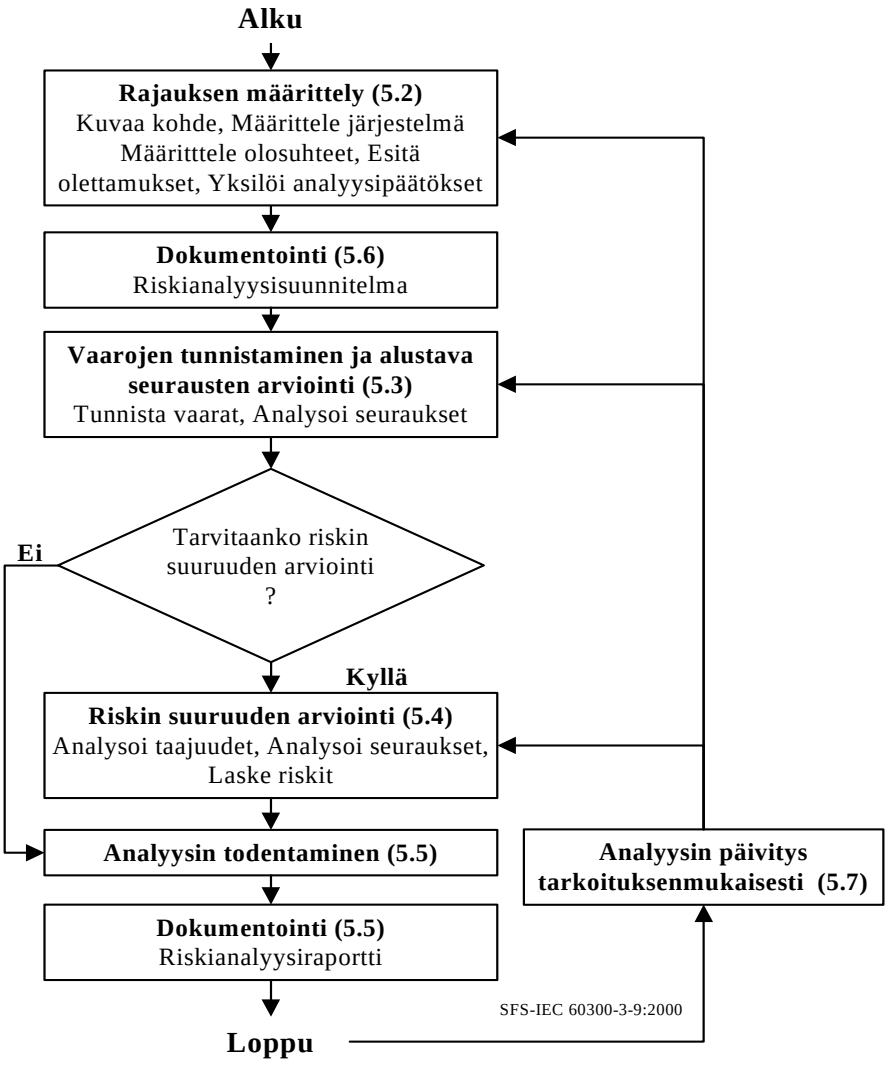
Riskienhallintaa on käsitelty useissa standardeissa. Standardi ISO 14971:2000 on tarkoitettu erityisesti terveydenhuollon laitteiden riskienhallintaan. Lisäksi on syytä tutustua ainakin standardeihin SFS-IEC 60300-3-9:2000 ja IEC 61508 -standardisarjaan (sisältää useampia standardeja). Standardin SFS-IEC 60300-3-9 (2000) mukaan riskienhallintaprosessiin liittyy seuraavat vaiheet:

- ***Riskianalyysi***, johon sisältyy käsittäen tuotteen käytön tai toimintaprosessin rajauksen määrittämisen, siihen liittyvien vaarojen tunnistus ja analysointi sekä riskin suuruuden arviointi.
- ***Riskin merkityksen arviointi*** eli riskin evaluointi, johon sisältyy päätökset riskin siedettävyydestä sekä vaihtoehtojen analysointi. Prosessissa tehdään päätökset riskin siedettävyydestä riskianalyysin perusteella ottamalla huomioon sellaiset tekijät kuten sosioekonomiset ja ympäristölliset näkökohdat.
- ***Riskin pienentäminen ja valvonta***, johon sisältyy päättäminen toteutettavista menetelmistä riskin hallitsemiseksi ja/tai pienentämiseksi, niiden käyttöönotosta, seurannasta sekä uudelleen arviointi aika ajoin, käyttäen riskin arvioinnin tuloksia yhtenä lähtötietona.

Riskianalyysiprosessi on esitetty kuvassa 3. Prosessiin sisältyy myös johdon määrittelemät riskienhallinnan periaatteet, jotka ohjaavat orga-

nisaation linjaa hallita riskejä. Periaatteet näkyvät kaikissa toiminnoissa (taloudelliset riskit, toimintaa uhkaavat riskit, teknologiariskit ja tuotteisiin liittyvät riskit).

Alkuvaiheessa riskienhallinta saattaa tuntua raskaalta ja teoreettiselta. Kunhan prosessi saadaan ohjeistettua riittävästi ja integroitua osaksi jokapäiväisiä toimintoja sekä käytännön kokemuksen hieman karttuessa on sillä varmasti toiminnan laatua parantava vaikutus. Lisäksi täytyy muistaa, että jotkut toiminnot edellyttävät säädösten ja standardien kautta riskianalyyttisiin menetelmiin perustuvaa päätöksentekoa.



Kuva 3. *Riskianalyysiprosessi*

3.2 Toimivan riskienhallinnan osa-alueita

3.2.1 Määritelmiä

Riskienhallintaan liittyvien käsitteiden merkitys tuntuu joskus aiheuttavan sekaannusta tai ainakin samalla sanalla saatetaan eri yhteyksissä tarkoittaa erilaisia asioita. Organisaation yhteisesti hyväksymällä ja käyttämällä terminologialla riskienhallintaan liittyvän koulutuksen ja analyysien ja riski/etu -tarkastelujen suorittamista saadaan helpotettua ja systematisoitua. Taulukkoon 1 on poimittu riskienhallintaan liittyviä määritelmiä.

Taulukko 1. Riskienhallintaan liittyviä määritelmiä [1]

Termi	Lähde	Selitys
VAHINKO *Harm*	ISO 14971:2000	Fyysinen vamma, terveyshaitta tai omaisuus- tai ympäristövahinko [ISO/IEC Guide 51: 1999, 3.1].
VAARA *Hazard*	ISO 14971:2000	Vahingon mahdollinen lähde [ISO/IEC Guide 51, 3.5].
VAARALLINEN TILANNE *Hazardous situation*	ISO 14971:2000	Olosuhteet, joissa ihmiset, omaisuus tai ympäristö ovat alttiina yhdelle tai useammalle vaaralle [ISO/IEC Guide 51, 3.6].
SUURIN SIEDETTÄVÄ RISKI *Maximum tolerable risk*	IEC 60601-1-4:2000	Suurin mahdollinen riskin arvo, joka voidaan sallia
RISKI *Risk*	ISO 14971:2000	Vahingon esiintymisen todennäköisyyden ja vahingon vakavuuden yhdistelmä [ISO/IEC Guide 51, 3.2].
JÄÄNNÖSRISKI *Residual risk*	ISO 14971:2000	Turvallisuustoimenpiteiden toteuttamisen jälkeen jäljelle jäävä riski.
TURVALLISUUS *Safety*	ISO 14971:2000 IEC 60601-1-4:2000	Tila, jossa vahingon riski on hyväksyttävällä tasolla [ISO/IEC Guide 51, 3.1].
RISKIANALYYSI *Risk analysis*	ISO 14971:2000	Saatavilla olevan tiedon systemaattinen käyttö vaarojen tunnistamiseksi ja riskin suuruuden arvioimiseksi.
VAARAN TUNNISTUS *Hazard Identification*	IEC 60300-3-9:2000	Prosessi, joka tunnistaa, että vaara on olemassa, ja määrittelee sen ominaispiirteet.
RISKIN SUURUUDEN ARVIOINTI *Risk estimation*	IEC 60300-3-9:2000	Prosessi, jolla mitataan analysoitavien riskien taso. Riskin suuruuden arviointi koostuu seuraavista vaiheista: taajuusanalyysi, seurausanalyysi ja niiden yhdistäminen.
RISKIN MERKITYKSEN ARVIOINTI *Risk evaluation*	ISO 14971:2000	Riskianalyysiin perustuva päätös, että onko hyväksytty riski saavutettu perustuen yhteiskunnan asettamiin sen hetkisiin arvioihin.

RISKIN ARVIOINTI *Risk assesment*	ISO 14971:2000	Riskianalyysin ja riskin merkityksen arvioinnin kokonaisprosessi. Perustuu harkinnanvaraisiin päätöksiin, joiden tukena on laadullisia ja määrällisiä menetelmiä.
RISKIN VALVONTA *Risk control*	ISO 14971:2000	Prosessi, jolla tehdään päätökset ja toimenpiteet riskin pienentämiseksi määritellylle tasolle tai pitämiseksi riski määritellyllä tasolla.
RISKIN HALLINTA *Risk management*	ISO 14971:2000	Johdon systemaattisesti soveltama menettelytapa, joka sisältää menettelytavat ja käytännöt tehtävien analysoimiseksi, riskin merkityksen arvioimiseksi ja riskin hallitsemiseksi
Turvallisuustoimenpide Safety measure	SFS-EN 1050:1997	Toimenpide, joka poistaa vaaran tai pienentää riskiä
VAKAVUUS *Severity*	ISO 14971:2000	Mitta-asteikko mahdollisen vaaran seurauksille

3.2.2 Riskin luokittelu

Vaaran poistaminen tai siihen liittyvän riskin pienentäminen, kun ne ovat jo toteutuneet, on mahdotonta tai erittäin vaikeaa. Haluttaessa poistaa vaara, tulee tuntea ja pohtia mahdollisen vaaran syntymekanismia ja siihen kytkeytyvää riskiä.

Riskienhallinnan tulee sisältää vaaroihin liittyvien riskien luokittelumenetelmät, jotta riskin suuruutta voidaan arvioida joko määrällisesti tai laadullisesti. Luokittelua tarvitaan, kun analyysissä havaitun riskin suuruutta arvioidaan, tehdään päätöksiä riskin pienentämisestä tai arvioidaan riskin hyväksyttävyyttä.

Riskin suuruus ilmaistaan yleensä kahden erillisen elementin avulla, jotka ovat:

- vaarallisen tapahtuman ***todennäköisyys***
- vaarallisen tapahtuman seurauksen ***vakavuus***.

Luokittelumenetelmät tarkoittavat usein näiden riskin elementtien laadullista arviota. Taulukossa 2 on esitetty esimerkki standardin SFS-IEC 60300-3-9 mukaisesta riskin luokittelusta.

Taulukko 2. Esimerkki riskien luokittelusta. (H = korkea riski, I = keskinkertainen riski, L = matala riski, T = vähäinen riski)

Tapahtumistaajuus	Arvioitu taajuus (vuodessa)	Seurausten vakavuus			
		Katastrofaalinen	Suuronnettomuus	Vakava	Pieni
Hyvin todennäköinen	> 1	H	H	H	I
Todennäköinen	$1 – 10^{-1}$	H	H	I	L
Satunnainen	$10^{-1} – 10^{-2}$	H	H	L	L
Vähäinen	$10^{-2} – 10^{-4}$	H	H	L	L
Epätodennäköinen	$10^{-4} – 10^{-6}$	H	I	L	T
Hyvin epätodennäköinen	$< 10^{-6}$	I	I	T	T

Katastrofaalinen	Käytännössä täydellinen laitoksen tai järjestelmän tuhoutuminen. Useita kuolleita.
Suuronnettomuus	Laaja vaurio laitokselle tai järjestelmälle. Muutamia kuolleita.
Vakava	Vakava vamma, vakava työperäinen sairaus, merkittävä laitoksen tai järjestelmän vaurio.
Pieni	Lievä vamma, lievä työperäinen sairaus tai pieni järjestelmän vaurio.

Huom! Luokkien määrittelyt ja arvot ovat vain suuntaa antavia.

Edellä kuvattu luokittelu ei välttämättä sovellu terveydenhuollon organisaation käytettäväksi sellaisenaan, jossa analysoitavina kohteina voivat olla hankinta-, hoito- ja huoltoketjut sekä erilaisten kuvantamis- tai monitorointijärjestelmien muodostamat laitejärjestelmät. Esimerkkiluokittelu muodostaa kuitenkin perustan, jonka mukaan kukin organisaatio voi laatia itselleen soveltuvan luokittelujärjestelmän.

Riskin toinen elementti on todennäköisyys, jonka määritteleminen saattaa olla hyvinkin vaikeaa. Esimerkiksi ohjelmistoille tyypilliset systemaattiset viat eivät oikein sovi todennäköisyyden käsitteeseen. Todennäköisyyden määrittäminen voidaan tehdä standardin ISO 14971 mukaan käyttämällä seuraavia tietoja tai menetelmiä:

- asiaan kuuluvat historiatiedot,
- todennäköisyyden ennakointi analyyttisillä menetelmillä tai simuloimalla,
- asiantuntija-arviot.

Standardissa SFS-EN 1050 on joitain lisätietoja vaaran esiintymisen todennäköisyyden määrittelemiseen. Osa määrittelyistä on sovellettavissa sellaisenaan terveydenhuollon tuotteen tai hoito- ja huoltoprosessin riskien arviointiin. Edellä mainitussa standardissa todennäköisyys koostuu kolmesta tekijästä (taulukko 3).

Taulukko 3. Vaaran esiintymisen todennäköisyyteen vaikuttavia tekijöitä.

Kohde	Tarkempi jaottelu
1. Altistumisen taajuus ja kesto	Vaaravyöhykkeelle pääsyn tarve Pääsytapa Vaaravyöhykkeellä oloaika Henkilöiden lukumäärä, joiden on päästävä vaaravyöhykkeelle Vaaravyöhykkeelle menemisen taajuus
2. Vaarallisen tapahtuman esiintymisen todennäköisyys	Luotettavuutta koskevat ja muut tilastolliset tiedot Tapaturmatiedot Tiedot terveyshaitoista Riskin vertailu
3. Vahingon vältettävyys ja rajoitettavuus	
a) koneen käyttäjien vaikutuksesta	Ammattitaitoiset henkilöt Ammattitaidottomat henkilöt Kone on miehittämätön
b) vaarallisen tapahtuman ilmaantumisnopeus	Äkillinen Nopea Hidas
c) tietoisuus riskin olemassaolosta	Yleistietoihin perustuen Suoraan havaitsemalla Varoitusmerkintöjen ja merkinantolaitteiden avulla
d) inhimilliset mahdollisuudet välttää tai rajoittaa vahinkoa (esim. refleksit, notkeus, mahdollisuudet pelastautumiseen)	Mahdollisia Mahdollisia tietyissä olosuhteissa Mahdottomia
e) käytännön kokemusten ja tietojen avulla	Kyseisestä koneesta Vastaavasta koneesta ei kokemusta

Täten riski (R) voidaan määritellä vakavuuden (V) ja esiintymistodennäköisyyden (E) avulla seuraavasti:

$R = f[V, E]$

$E = f[a, v, vv]$, jossa

a = altistumisen taajuus ja kesto

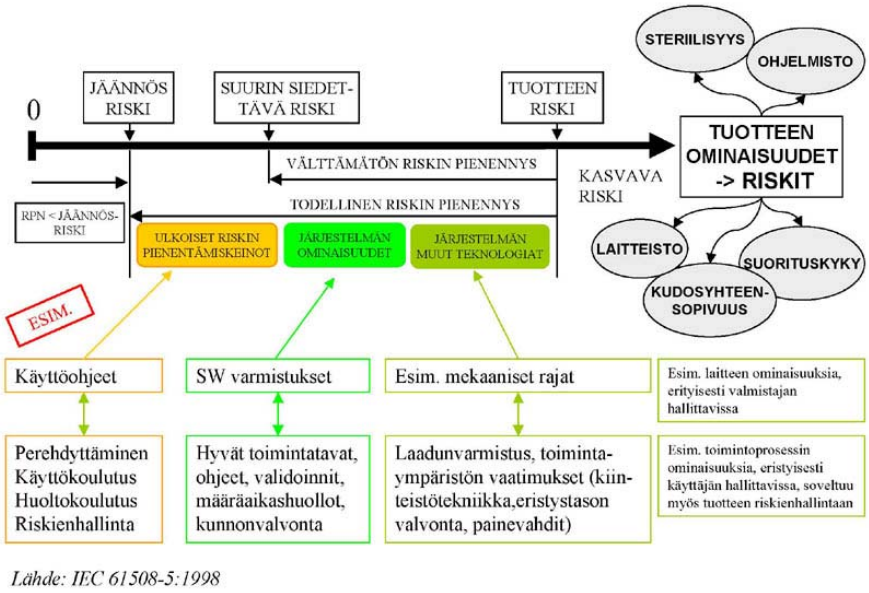
v = vaarallisen tapahtuman esiintymisen todennäköisyys

vv = vahingon vältettävyys ja rajoitettavuus

Näin esiintymistodennäköisyyden määrittelemiseen saadaan lisää aputekijöitä, jotka voivat olla joissain tapauksissa merkittävä apuväline. Ohjelmoitavissa järjestelmissä vahingon vältettävyyteen ja rajoitettavuuteen voidaan katsoa kuuluvan myös havaittavuuden ja vikasietoisuuden, joita huolellisesti harkiten voidaan käyttää riskin valvonnan ja pienennyksen välineinä.

Ilman organisaatiokohtaista riskin luokittelujärjestelmää on mahdotonta tehdä riskin vakavuuden ja todennäköisyyden arviointia. Arvioinnissa on kuitenkin muistettava, että mihin tahansa luokittelujärjestelmään sisältyy tietty määrä epävarmuutta. Esimerkiksi inhimillisten tekijöiden

ja ohjelmistoille luonteeltaan systemaattisten virheiden luokittelussa on aina mukana myös jonkinlainen epävarmuustekijä. Tämän takia jokainen analyysi on oma erillinen tapauksensa ja siihen liittyvien riskien luokittelu on aina tapauskohtaista. Kullakin organisaatiolla on myös omat toisistaan poikkeavat keinot pienentää riskiä. Kuvassa 4 on esimerkkejä, joita voidaan käyttää riskin pienentämiseksi hyväksytylle tasolle. Huomaa kuvassa olevien riskinpienennys-toimenpiteiden erilaisuus, kun analysoitavana kohteena on joko tuote tai toimintaprosessi.

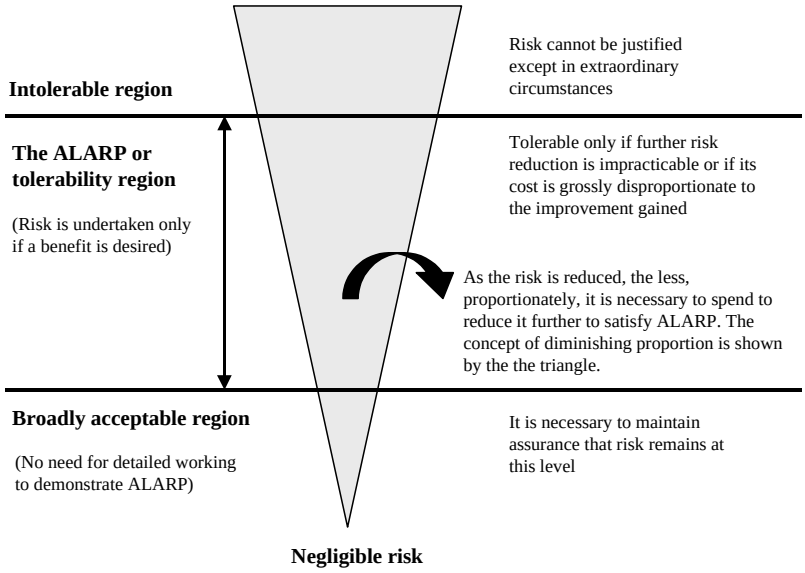


Lähde: IEC 61508-5:1998

***Kuva 4**. Riskin pienennyksen periaatteet*

3.2.3 Riskin siedettävyys

Riskin siedettävyyden määrittelyyn liittyy ns. ALARP–periaate (As Low As Reasonably Possible), joka kuvataan standardeissa IEC 61508-5, IEC 60601-1-4 ja ISO 14971. ALARP–alueella riskit on vähennetty alhaisimmalle kohtuudella toteutettavissa olevalle tasolle, jossa riski on vielä on siedettävä. Erityisesti ALARP-alueella joudutaan pohtimaan jäännösriskin siedettävyyttä. Alue sijaitsee sietämättömän riskialueen ja selvästi käyttökelpoisen riskialueen välissä, missä toimenpiteisiin ryhtyminen on helppoa (kuva 5).



Kuva 5. *Siedettävä riski ja ALARP –periaate.*

Kuvan 5 alueet määritellään standardissa IEC 61508-5 seuraavasti:

- Sietämätön alue (intolerable region). Vaarojen riski on niin vakava, että niitä ei voida hyväksyä. Riskiä tällä alueella voidaan pienentää pienentämällä vakavuutta ja/tai vaaran todennäköisyyttä.
- Siedettävä alue (ALARP region). Aluetta sietämättömän ja selkeästi hyväksyttävän alueen välissä kutsutaan siedettäväksi alueeksi. Tämä on alue, jossa riski on pienennetty niin pieneksi kuin kohtuudella voidaan toteuttaa. Tällä alueella riskit on pienennetty alhaisimmalle mahdolliselle tasolle suhteessa hyväksyttävään riskiin ja riskin lisäpienennysten aiheuttamaan kustannukseen nähden. Mikä tahansa riski voidaan pienentää alueelle, joka on 'siedettävä alue'. Lähellä sietämättömän alueen rajaa riskit on pienennettävä vaikka siitä aiheutuisikin huomattavia lisäkustannuksia.

- Selkeästi hyväksyttävä alue (broadly acceptable region). Vaaran vakavuus ja/tai vaaran mahdollisuus on niin alhainen, että riski on merkityksetön verrattuna muiden hyväksyttyjen vaarojen riskeihin. Näissä vaaroissa riskin pienentämistä ei tarvitse harjoittaa aktiivisesti.

ALARP-periaatetta tulee hyödyntää riskin hyväksyttävyyttä määriteltäessä. Mikäli analyysi osoittaa riskin olevan ALARP–alueella, tulee käynnistää pohdiskelu kyseisen riskin hyväksyttävyydestä tässä analyysissä. Pohdiskelussa tulee välttää ajattelutapaa, että jos edellisessäkin analyysissä riski voitiin hyväksyä, niin se automaattisesti hyväksyttäisiin uudestaan.

Käytännön esimerkkinä voidaan vaikka mainita terveydenhuollon sovellukset, jotka on alunperin tarkoitettu ainoastaan aikuispotilaille. Teknologian kehittyessä sovellus on tarkoitus ulottaa myös lapsipotilaisiin. Tässä tapauksessa lapsipotilaiden fysiologia ja vitaaliparametrin mitta-alueet eivät välttämättä ole vastaavia aikuispotilaiden kanssa. Tämän takia aiemmin tehty riskianalyysi on ehdottomasti uusittava ennen sovelluksen käyttöönottoa.

3.2.4 Analyysimenetelmän valintaan vaikuttavia tekijöitä

Riskianalyysissä haetaan aina syy-vika-seuraus-vaara –ketjuja, joiden tunnistaminen voidaan aloittaa huipputapahtuman tunnistavalla tekniikalla (top-down -tekniikka, esim. vikapuuanalyysi, FTA) tai hieman analyyttisempää, tuotteen rakenteen huomioonottavalla vikamuodon tunnistavalla tekniikalla (bottom-up -tekniikka, esim. vika- ja vaikutusanalyysi, FMEA). Menetelmiä voidaan soveltaa myös siten, että aloitetaan analyysi esim. vikapuu-analyysillä, jonka jälkeen analysoidaan kriittiset löydökset vaikkapa vika- ja vaikutusanalyysillä.

Vaarojen tunnistamisessa haetaan aina vastausta seuraavanlaisiin kysymyksiin:

- Mikä laitteessa/järjestelmässä/prosessissa on sellaista mikä (voi) aiheuttaa vahinkoa ihmisille tai laitteen ympäristölle?
- vikamuodot
- Mikä voisi tehdä laitteesta/järjestelmästä/prosessista sellaisen, että se (voi) aiheuttaa vahinkoa ihmisille tai laitteen ympäristölle?
- alullepanevat syyt

Asetetuissa kysymyksissä on tunnustettava, että erilaisiin tapahtumiin ja järjestelmän tiloihin liittyy epävarmuutta, esimerkiksi:

- osat voivat vikaantua,
- prosessi ei toimi odotetulla tavalla,
- ohjelmat voivat toimia odotetusta poikkeavasti,
- ihmiset voivat toimia odotetusta poikkeavasti (inhimilliset tekijät, tahallinen väärinkäyttö, käyttöliittymien monimutkaisuus).

Valittavien menetelmien tulee olla tunnustettuja ja tieteellisesti päteviä ja niiden pitää soveltua analysoitavaan järjestelmään. Usein kahden tai kolmen analyysinmenetelmän hyvä tuntemus on riittävä. Riskienhallinnassa tutkittava kohde voidaan jakaa useisiin osatekijöihin, jolloin kuhunkin tarkasteltavaan osatehtävään voidaan helpommin valita oikea menetelmä. Menetelmien käyttöön tulee olla riittävä määrä koulutettuja henkilöitä, jotta menetelmää voidaan käyttää työkaluna siten, että analyysi on jäljitettävissä, toistettavissa ja verifioitavissa ja se tuottaa tulokset muodossa, joka auttaa riskin luonteen ymmärtämisessä ja valvonnassa.

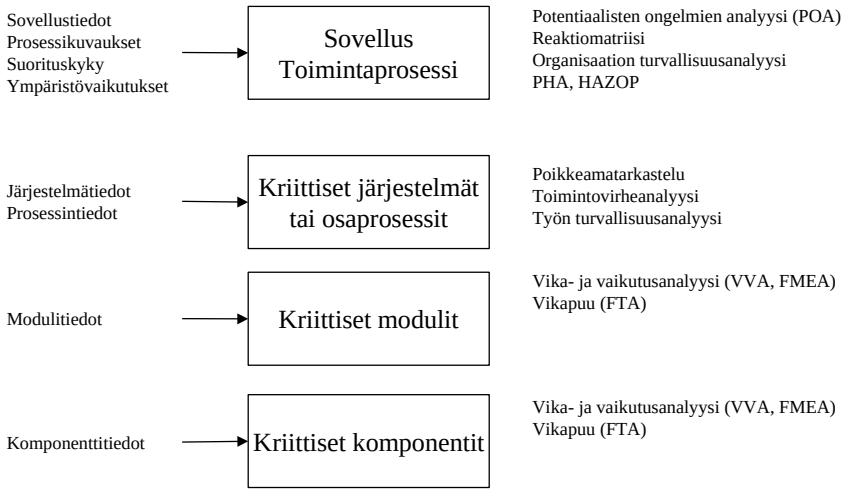
Riskianalyysi edellyttää systemaattista ajattelutapaa ja lähes poikkeuksetta sen suorittaminen vaatii usean ihmisen muodostaman tiimin. Tiimissä on oltava usean eri alan ammattilaisia, joilla on esimerkiksi:

- vahva käytännön kokemus ja vastuu projektin johtamisesta
- hyvä tuntemus sovellusalueesta (esim. riskin hyväksyttävyyden päättäminen edellyttää joissain tapauksissa kliinikoiden päätöstä)
- kyky toteuttaa laadunvarmistusta, katselmuksia sekä prosessien verifiointia ja validointia
- teknologiaosaaminen (elektroniikka, ohjelmistoteknologiat, mekaniikka, käyttäytymistiede inhimillisien tekijöiden arvioinnissa)
- riskienhallintatekniikoiden osaaminen.

Analyysimenetelmien valintaan ja analyysin onnistumiseen vaikuttaa aina useampi tekijä. Seuraavassa on kuvattu muutamia tekijöitä, jotka on otettava huomioon menetelmää valittaessa:

- Saatavilla olevan tiedon määrä ja laatu
- Onko analyysin tai tuotteen kriittiset tekijät tunnistettu (vikamuodot, avainsanat, huipputapahtumat, tutkittava taso jne.)
- Voidaanko tehdä kohteen tarkka rajaus
- Onko vika- ja vaikutusanalyysin käytön tukena kokemusperäisen tiedon avulla laadittuja vikamuoto-tarkastuslistoja (menetelmällä on hankala tunnistaa vikamuotoja)

- top-down -tyyppiset menetelmät hakevat valittuun huipputapahtumaan johtavia syitä, kun taas bottom-up -tyyppiset menetelmät hakevat syistä tai vikamuodoista johtuvia vaikutuksia.



Kuva 6. *Esimerkkejä käytettävistä riskianalyysitekniikoista*

Kvantitatiivisten menetelmien käyttöä voi joissain tapauksissa rajoittaa saatavilla olevan tiedon määrä tai luotettavuus, jolloin on tapauskohtaisesti arvioitava käytetäänkö määrällisiä vai laadullisia menetelmiä. Analyysin aloituksessa on muistettava, että analysoitavaksi kohteeksi valitaan aina sovellus tai toimintaprosessi. Tällöin analyysimenetelmäksi on valittava ihmisten, laitteiden ja sovellusten riskejä ja vaaratekijöitä hyvin tunnistava menetelmä, joka antaa myös hyvää lähtötietoa teknisten järjestelmien analyysimenetelmille. Tämän jälkeen voidaan siirtyä analyysissä alemmas kriittisten osajärjestelmien, komponenttien tai kriittisten vioittumismekanismien tarkasteluun. Kuvassa 6 on esimerkkejä eri analyysimenetelmien soveltuvuudesta eri vaiheisiin ja käyttötarkoituksiin.

3.3 Riskianalyysi ja tulosten kirjaaminen

Riskianalyysista on laadittava kirjallinen selostus, josta on käytävä ilmi riskienhallintasuunnitelman edellyttämät asiat. Selostuksen laajuus riippuu hyvin pitkälti analyysin laajuudesta. Analyysin on katettava standardin SFS-IEC 60300-3-9 mukaan ainakin seuraavat seikat:

a) yhteenveto
b) johtopäätökset
c) tavoitteet ja rajaus
d) rajoitukset, oletukset ja olettamuksien perustelu

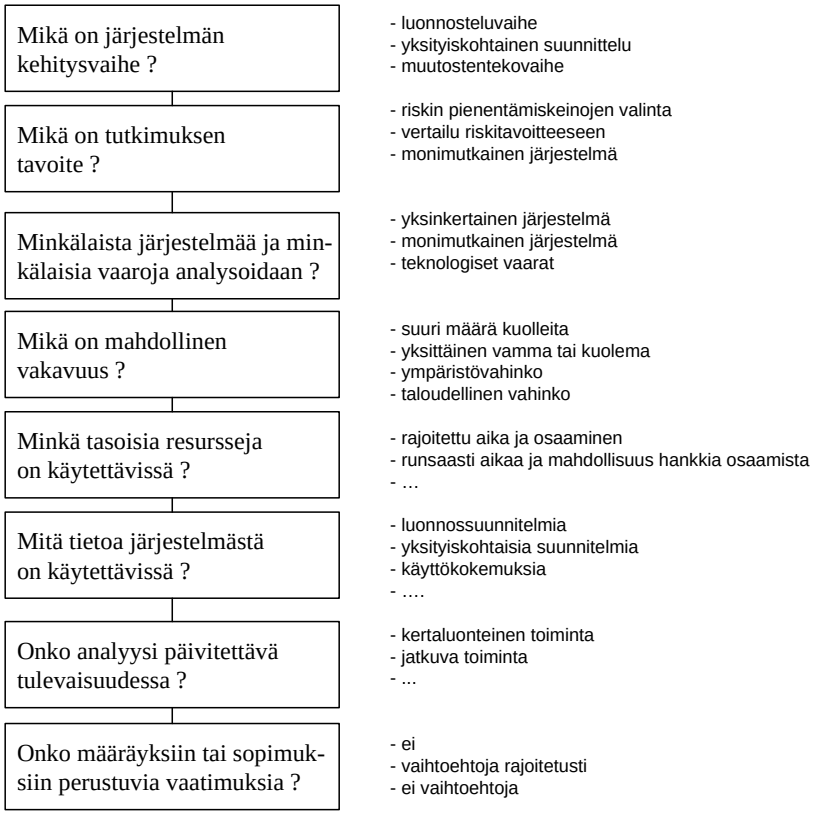
e) järjestelmän asianmukaisten osien kuvaus
f) analyysimenetelmät
g) tulokset vaarojen tunnistamisesta
h) käytetyt mallit, mukaan lukien oletukset ja tarkkuuden/riittävyyden todentaminen
i) lähtötiedot ja niiden lähteet
j) riskin suuruuden arvioinnin tulokset
k) herkkyys- ja epävarmuusanalyysit
l) tulosten tarkastelu (mukaan lukien analysointiongelmien tarkastelu)
m) käytetyt lähteet.

Analyysin kirjaamisen tulee täyttää organisaation dokumentoinnille asettamat vaatimukset. Selostus tulee laatia siten, että sitä voidaan tarvittaessa helposti päivittää.

Riskienhallinta määrittelee periaatteet, politiikan ja käytettävät työkalut suunnitelman ja itse analyysin tekemiselle. Suunnitelma taas määrittelee soveltamisalan, aikataulun, tekijät, tavoitteet, hyväksyntärajat, menetelmät ja tulosten kirjaamisen. Analyysi tehdään riskienhallinnan periaatteita noudattaen suunnitelman edellyttämällä tavalla ja riskienhallinnan määrittelemillä työkaluilla

3.4 Miten aloitan riskianalyysin?

Analyysin suorittamiseksi on pakko tutustua teoriaan, jotta käsitteet riski, riskinpienennys, vikamuodot ja itse analyysitekniikat tulevat tutuiksi. Kuten aiemmin on todettu, analyysiä ei voi suorittaa pelkästään yksi ihminen. Mitä monimutkaisempi on analysoitava kohde sitä useamman eri alan asiantuntijoita joudutaan analyysissä käyttämään. Sama pätee myös analyysin kattavuuteen. Analyysin valmistelussa auttaa standardin SFS-IEC 60300-3-9 päättelypuu (kuva 7).



***Kuva 7**. Analyysin valmistelussa esitettäviä kysymyksiä*

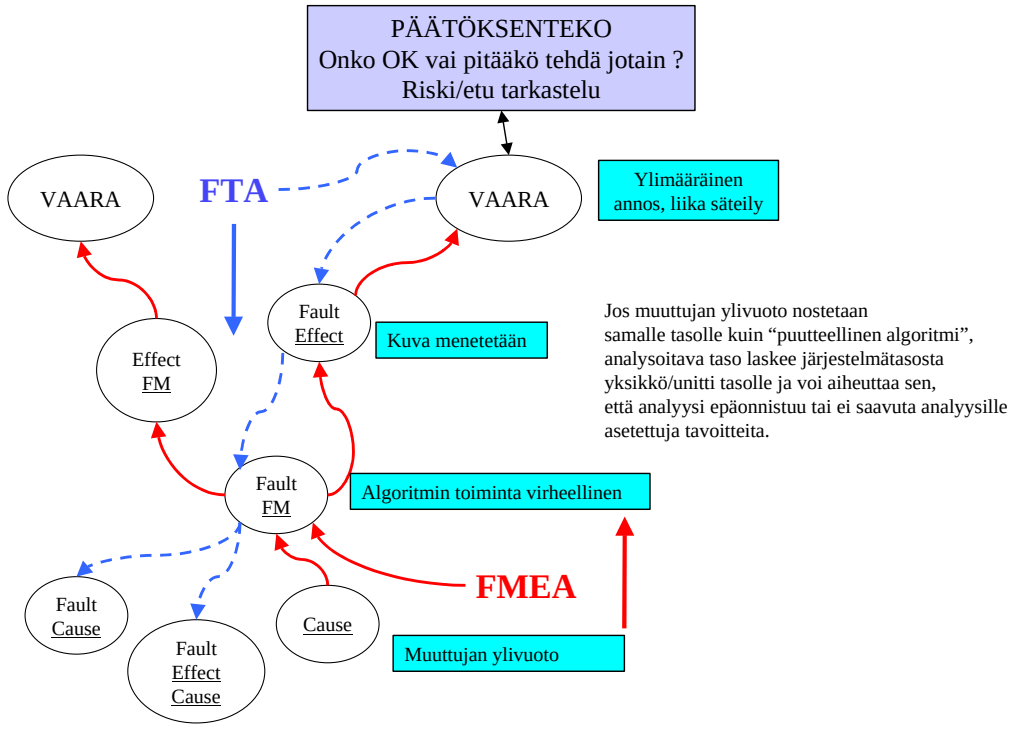
Analyysiä aloitettaessa on laadittava aina suunnitelma, jossa määritellään tavoitteet ja kattavuus sekä määritellään analyysin dokumentointi. Tässä vaiheessa on mietittävä myös mahdolliset rajaukset, joihin vaikuttaa esim.:

- minkälaisia riskityyppejä tarkastellaan (turvallisuus, muut)
- mikä on tarkasteltava käyttöolosuhde (suunniteltu käyttö, väärinkäyttö, maksimi kuormitus, tyhjäkäynti, paljon käyttäjiä, ei lainkaan käyttäjiä jne.)

- Minkälaisia henkilöryhmiä ja toimintaympäristöjä tarkastelussa otetaan huomioon (potilaat, käyttäjät, asentajat ja huolto, sivulliset)
- mikä on tarkasteltava laitekokonaisuus.

Mahdollisia rajauksia tehtäessä on muistettava, että ne sopivat asetettuihin tavoitteisiin. Tämän jälkeen on analysoitavasta kohteesta kerättävä kaikki mahdollinen tieto. Saatu tieto tai lähinnä puuttuva tieto voi vielä vaikuttaa analyysin rajauksiin. Saadun tiedon perusteella voidaan valita analyysimenetelmä analyysiin suorittamiseksi (ks. 3.2.4).

Itse analyysi on tämän jälkeen systemaattista syy-seuraus –ketjujen etsintää. Analyysiä voidaan tukea valmiilla tarkistuslistoilla, joissa on valmiina esimerkiksi järjestelmän vikaantumiseen johtavia syitä tai tunnettuja prosessin häiriötekijöitä. Jokaisen löydetyn ketjun kohdalla tehdään riskin suuruuden arviointi, edellyttääkö löydetty syy-seuraus –ketju riskinpienennystä vai voidaanko se hyväksyä sellaisenaan (kuva 8).



***Kuva 8**. Esimerkki syy-seuraus -ketjusta*

Analyysin lähtökohdaksi on valittava järjestelmätasolla aiheutuva vaara. Tämä täytyy muistaa niissä tapauksissa, kun analysoidaan esimerkiksi

järjestelmän tai toimintoprosessin osatoimintoja tai alijärjestelmiä. Suoritettaessa riskianalyysiä ensimmäisen kerran voidaan analyysin vetäjäksi palkata vaikka ulkopuolinen valitun analyysimenetelmän tunteva henkilö. Tällöin hän ohjaa tehtyä analyysiä (vikamuodot ja syy-seuraus -ketjut ovat oikeita sekä pysytään valitulla tasolla) ja opastaa tiimiä analyysin eri vaiheissa.
Riskianalyysin ”lyhyt oppimäärä”:

1. Tutustu riskienhallinnan teoriaan.
2. Kerää analysoitavasta kohteesta mahdollisimman paljon tietoa.
3. Laadi tarkistuslistoja analyysin tueksi.
4. Harjoittele analyysiä ensiksi yksinkertaisilla ja rajatuilla kohteilla.
5. Käytä tarvittaessa asiantuntijoiden apua.

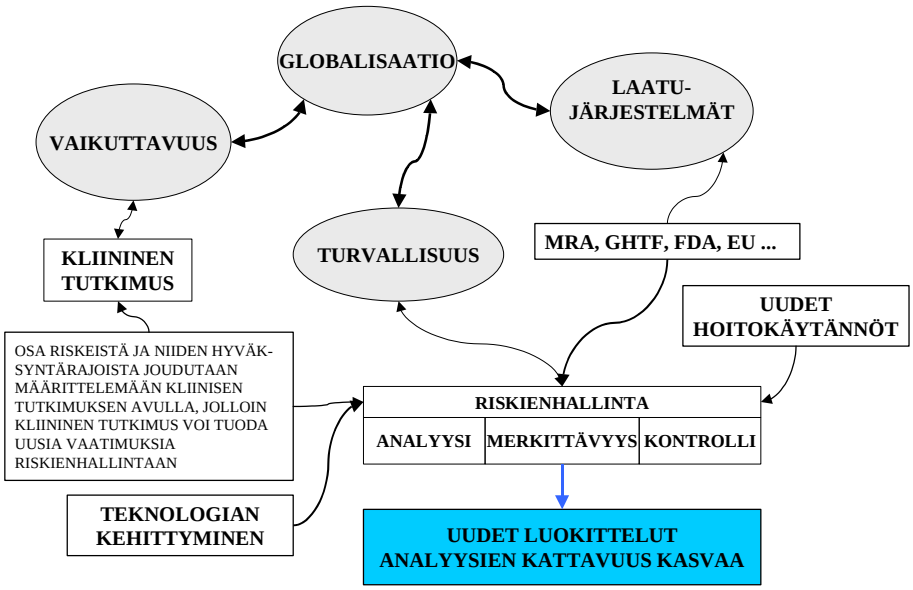
Lisätietoa riskienhallinnasta ja erilaisista menetelmistä löytyy esim. seuraavilta verkkosivuilta:

http://riskianalyysit.vtt.fi/	
http://riskianalyysit.vtt.fi/indexe5b3.html	Ohjeita ’hyvälle riskianalyysille’
http://www.pk-rh.com/	Pk-yrityksen riskienhallinnan aloitussivut

3.5 Vaatimukset riskienhallinnalle muuttuvat

Markkinoiden kansainvälistyessä vaatimuksia yhdenmukaistetaan. Tämä avaa valmistajalle mahdollisuuden viedä tuotteitaan uusille markkinoille. Toisaalta se tuo valmistajalle myös uusia vaatimuksia. Valmistajien on otettava huomioon mahdollisesti väestön ja kulttuurin erilaisuudesta johtuvat erot. Erot näkyvät mahdollisesti erilaisina hoitokäytäntöinä tai laitteiden huoltoina. Nämä kaikki muutokset tuovat uusia vaatimuksia valmistajien riskienhallintaan. Myös hoito- ja tutkimusprosessien kehittyminen asettaa vaikuttavuudelle ja turvallisuudelle uudet puitteet, jolloin prosessien ja teknologian kehittyessä siirrytään laitteen arvioinnista työkalujen arviointiin, tämä unohdetaan usein tuotteen kelpuutusprosessissa (validointi).

Nämä muutokset eivät voi olla vaikuttamatta osaltaan myös käyttäjien tai järjestelmien maahantuojien riskienhallintaprosesseihin. Tärkeää on myös muistaa, että riskienhallinnasta vastaavat tahot koostuvat riittävän laajasta asiantuntijajoukosta. Tulevaisuus voi tuoda myös isojakin muutoksia käyttäjäorganisaatioiden riskienhallintaprosesseihin esimerkiksi analyysien riskiluokitteluissa tai itse analyysien kattavuudessa (kuva 9). Tämä edellyttää organisaatiolta ja sen johdolta kykyä seurata uusiutuvia vaatimuksia ja kytkeä ne omaan riskienhallintaprosessiin mahdollisimman tehokkaalla tavalla.



***Kuva 9**. Riskianalyysiprosessi kehittyy uusien vaatimusten myötä*

4. LAITEJÄRJESTELMÄT

4.1 Mikä on laitejärjestelmä?

Terveydenhuollon laitteiden yhteydessä puhutaan paljon järjestelmistä. Laitejärjestelmä on käsitteenä melko laaja ja välillä hieman epäselvä. Lisäksi turvallisuusvaatimuksia ei kyetä määrittelemään pelkästään standardin EN 60601-1 avulla. Tämän takia lääketieteellisille laitejärjestelmille on laadittu standardi EN 60601-1-1, joka määrittelee laitejärjestelmän seuraavien määritelmien avulla.

Sähkökäyttöinen lääkintälaitejärjestelmä [Medical electrical system]
Yhdistelmä laitteita, joista vähintään yksi laite on lääkintälaite ja jotka on kytketty toisiinsa toiminnallisella yhteydellä tai käyttämällä moninapaista pistorasiaryhmää.
Moninapainen siirrettävä pistorasiaryhmä [Multiple portable socket outlet]
Kahden tai useamman pistorasian yhdistelmä, johon on tarkoitettu kytkettävän taipuisia liitäntäjohtoja, tai joka muodostaa em. liitäntäjohtojen ja pistorasioiden kanssa kiinteän kokonaisuuden, jota voidaan helposti siirtää paikasta toiseen sähköverkkoon kytkettynä.
Toiminnallinen yhteys [Functional connection]
Sähköinen tai muu yhteys, sisältäen kytkennät, joilla signaali ja/tai teho ja/tai materiaali voidaan siirtää.

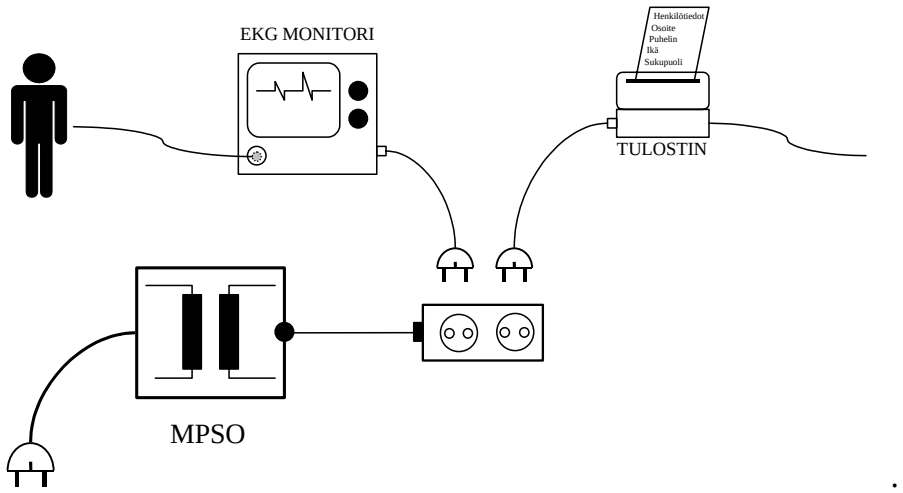
Määritelmien mukaan laitejärjestelmä voidaan muodostaa, joko galvaanisella yhteydellä tai toiminnallisella yhteydellä. Toiminnallinen yhteys voi olla johtava tai johtamaton yhteys. Määritelmä ei pois sulje myöskään mahdollisuutta, että toiminnallinen yhteys voi perustua inhimilliseen päätökseen toiminta. Kuvissa 10 ja 11 on esimerkkejä standardin määritelmän mukaisista laitejärjestelmistä.

Kuvassa 10 on moninapaisen siirrettävän pistorasiaryhmän (MPSO) avulla syötetään EKG-monitoria ja tulostinta. Tulostimelle tulostetaan potilaan henkilötietoja esim. potilashallintajärjestelmästä. Järjestelmä täyttää laitejärjestelmän määritelmän MPSO-kytkennän kautta. Järjestelmässä on toisaalta myös käytössä toiminnallinen yhteys, koska monitoroitavana olevan henkilön tietoja tulostetaan potilaspaikan vieressä olevalle tulostimelle. Määritelmässä tulee muistaa, että toiminnallinen yhteys ei välttämättä ole johtava yhteys

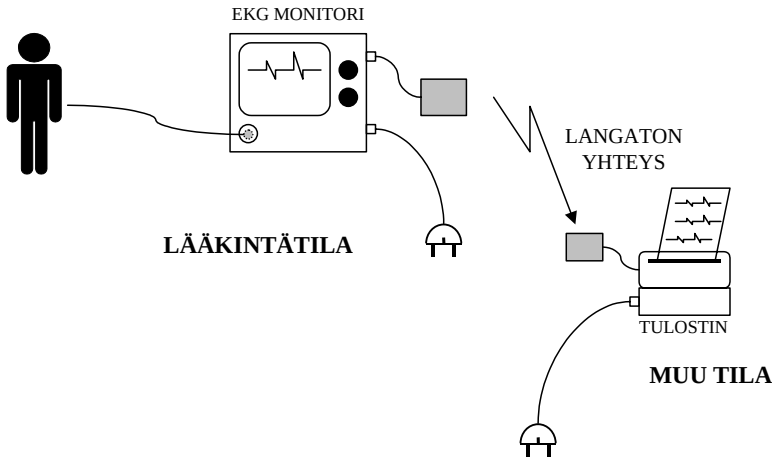
Yllä mainitut esimerkit käsittävät perinteisesti galvaanista tai ns. toiminnallista yhteyttä, jossa laite lähettää tietoa toiselle laitteelle. Laitejärjestelmän määritelmän voi toisaalta täyttää myös epäsuora yhteys, jossa käyttäjä lukee lääkintälaitteelta tietoa ja tallentaa sen osaksi poti-

lastietojärjestelmää. Talletetun tiedon perusteella voidaan tehdä hoitotoimenpiteitä saman työvuoron tai jopa seuraavien työvuorojen aikana.

Toiminnoksi voidaan käsittää myös lääkintälaitteen lähettämä tieto osaksi sairaalan potilastietojärjestelmää, useamman laitteen keräämästä tiedosta jonkin algoritmin avulla laskettu tulos, lääkintälaitteen lähettämän tiedon tulostaminen erillisellä tulostimella, laskentatulos tai lääkintälaitteen potilastiedon ja hälytysten siirtäminen keskusvalvontajärjestelmälle.



***Kuva 10**. Laitejärjestelmä, jota syötetään moninapaisella siirrettävällä pistorasiaryhmällä*



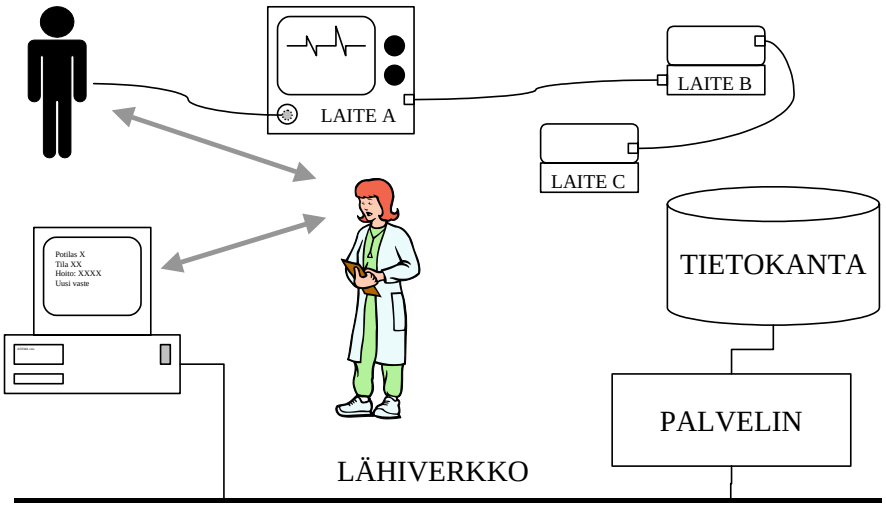
***Kuva 11**. Laitejärjestelmä toiminnallisella yhteydellä*

Kuvan 11 esimerkissä EKG-monitorista lähetetään joko WLAN- tai BlueTooth-yhteyden avulla potilastietoa keskusvalvomon tulostimelle. Laitejärjestelmän määritelmä täyttyy näin ollen toiminnallisen yhteyden

kautta. Järjestelmän sähköturvallisuusvaatimukset täyttyvät toiminnallisen yhteyden osalta. Tämän kaltaisessa kytkennässä ensisijaisiksi vaatimuksiksi muodostuvatkin tietoturvavaatimuksiin liittyvät tiedon luottamuksellisuus, eheys ja saatavuus.

Standardien tehtävänä on määritellä termit, käsitteet ja niitä koskevat vaatimukset mahdollisimman tarkasti ja yksiselitteisesti. Käytännössä tämä on usein mahdotonta, koska vaihtoehtoja ja mahdollisuuksia on liian monta tai tekniikka vain yksinkertaisesti kehittyy standardeihin nähden liian nopeasti. Näin on käynyt myös joiltain osin standardissa EN 60601-1-1. Esimerkiksi standardin määritelmä laitejärjestelmälle antaa käyttäjälle, valmistajalle tai ilmoitetulle laitokselle useita mahdollisuuksia tulkita eri sovelluksia järjestelmäksi.

Kuvan 12 esimerkissä voidaan tietoverkkoon kytketty potilashoidon tietojärjestelmä tulkita omaksi järjestelmäkseen tai osaksi olemassa olevaa järjestelmää, jos potilaan lääkeannostelu ja tilanmuutokset talletetaan tietojärjestelmään ja tietojärjestelmän tiedon perusteella voidaan potilaan lääkeannostelua tai hoitoa muuttaa. Tässä tapauksessa järjestelmän 'toiminnallisen yhteyden' muodostaisi käyttäjä omien toimintojensa kautta. Näin ollen tietojärjestelmälle tulisi asettaa standardin EN 60601-1-1 vaatimukset, mikä saattaisi joissain tapauksissa olla kohtuuton vaatimus.



***Kuva 12**. Mistä alkaa ja mihin loppuu kuvan järjestelmä ?*

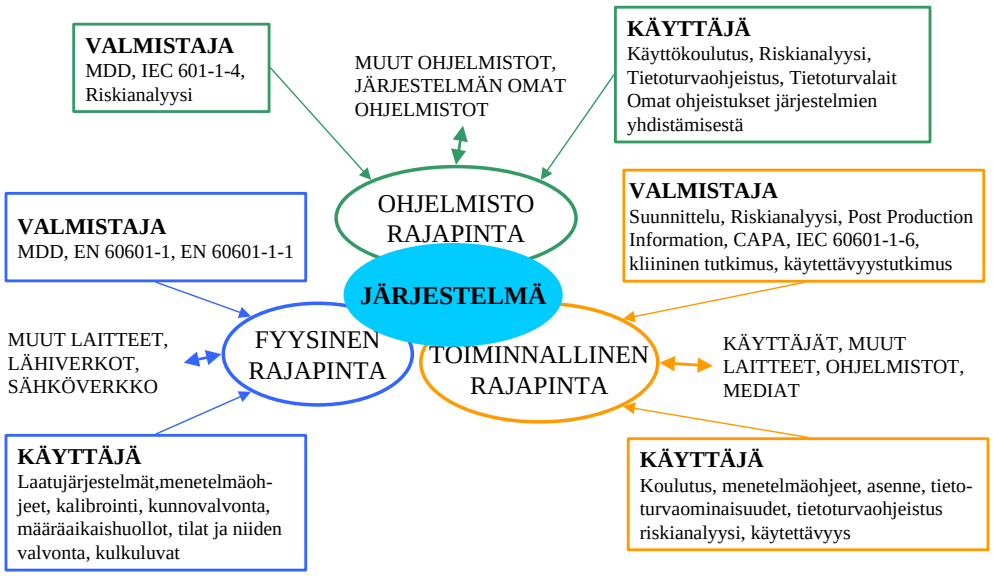
Näin tulkittuna asia voi laajentua vielä siten, että tietojärjestelmään tulee soveltaa terveydenhuollon laitteita koskevien säädösten vaatimuksia. Tällöin tietojärjestelmän ohjelmiston suunnittelussa tulee noudattaa standardin EN 60601-1-4 vaatimuksia ja lisäksi tietojärjestelmälle tulee tehdä säädösten edellyttämä riskianalyysi.

Esimerkkien perusteella voidaan havaita, että luokittelut ja määritelmät ovat välillä melko monimutkaisia ja jokainen tapaus tulee aina käsitellä erikseen. Tärkeää valmistajan ja käyttäjän kannalta on kuitenkin se, että järjestelmästä kyetään tunnistamaan ne kriittiset kohdat, joilla on suurin merkitys järjestelmän turvallisuudelle ja suorituskyvylle.

4.2 Laitejärjestelmän rajapinnat

Laitejärjestelmän rajaaminen on käytännössä joskus hyvinkin vaikeaa. Rajaamisen helpottamiseksi voidaan ottaa käyttöön käsitteet *fyysinen rajapinta, ohjelmistorajapinta ja toiminnallinen rajapinta* (kuva 13). Rajapinnat ovat periaatteessa niitä pisteitä, joissa järjestelmä on vuorovaikutuksessa joko ulkopuolisen tahon tai järjestelmän eri osien kanssa. Näihin rajapintoihin käyttäjä voi kohdistaa erilaisia laadunvarmistustoimintoja varmistaakseen laitejärjestelmän turvallisuuden. Laadunvarmistustoimenpiteet voivat olla mittauksia, menetelmäohjeita tai käyttöön ja huoltoon liittyviä koulutuksia.

Selkeimmin laitejärjestelmän rajaaminen onnistuu silloin, kun kyseessä on lääkintälaitteen ja muun sähkökäyttöisen laitteen yhteen kytkeminen. Vaikeampaa järjestelmän rajaaminen on silloin, kun järjestelmän laitteet kytkeytyvät toisiinsa esimerkiksi sairaalan lähiverkon kautta ja niiden toiminnallisuus perustuu osittain tai kokonaan kaupallisilla tai avoimilla käyttöjärjestelmäalustoilla toimiviin sovellusohjelmistoihin tai kaupallisiin ohjelmistoihin (Commercial Off-The-Shelf, COTS) perustuviin sovelluksiin. Kuvassa 13 on määritelty muutamia keinoja, joilla käyttäjäorganisaatio voi ylläpitää laitejärjestelmien suorituskykyä ja luotettavuutta.



***Kuva 13**. Laitejärjestelmään liittyviä rajapintoja*

4.2.1 Fyysinen rajapinta ja sähköturvallisuus

Fyysinen rajapinta on se laitejärjestelmän rajapinta, johon voidaan asettaa selkeämmin mitattavia ominaisuuksia (esim. vuotovirrat, jännitekoestus, ottoteho ja pinta- ja ilmavälit, mekaaninen turvallisuus). Lääkintälaitteiden ja laitejärjestelmien fyysisen rajapinnan suunnittelulle ja valmistukselle asetettavat vaatimukset annetaan terveydenhuollon laitteita koskevissa säädöksissä. Vaatimustenmukaisuuden osoittamisessa sovelletaan yhdenmukaistettuja standardeja (esimerkiksi EN 60601-1, EN 60601-1-1, EN 60601-1-2 ja EN 60601-2 –sarja).

Standardien valintaan vaikuttaa aina laitteen luokittelu ja käyttötarkoitus. Esimerkiksi tehostetussa valvonnassa käytettävän moniparametrimonitorin suunnittelussa tulee ottaa huomioon seuraavat standardit:

- EN 60601-1 Sähköturvallisuus
- EN 60601-1-1 Laitejärjestelmän turvallisuus (jos laite on osa järjestelmää)
- EN 60601-1-2 Sähkömagneettisten häiriöiden sieto ja tuotto
- EN 60601-1-4 Ohjelmiston sisältävät laitteet (sisältää vaatimukset myös riskienhallinnalle)
- EN 60601-2-27 EKG-monitori
- EN 60601-2-30 Epäsuora verenpaine (NIBP, non-invasive blood pressure)
- EN 60601-2-34 Suora verenpaine (IBP, invasive blood pressure)

Vaatimustenmukaisuuden täyttämiseksi joudutaan vielä tapauskohtaisesti soveltamaan joitain lisävaatimuksia. Eräs selkeä vaatimus on ainakin riskienhallinnan noudattaminen tuotteen suunnittelussa.

Käyttäjäorganisaation on hankinnan yhteydessä varmistettava, että laite täyttää tarvittavat vaatimukset. Vieläkin tärkeämpää on kuitenkin varmistaa laitteen oikea ja turvallinen käyttö sekä huolto sen käyttövaiheen aikana. Tämä voidaan toteuttaa joko huoltosopimusten avulla tai laatimalla menettelyt laitteen määräaikaishuollolle, kunnonvalvonnalle ja kalibroinnille. Vaatimusten ylläpitäminen edellyttää myös jatkuvaa koulutusohjelmaa niin käyttäjille kuin huoltajillekin.

Säädösten velvoitteista johtuen valmistajat ovat ruvenneet määrittämään ne tahot, jotka saavat ylipäätään korjata ja huoltaa laitteita. Käytännössä tämä tarkoittaa erilaisten ohjeiden laatimista, joilla laitetoimittaja määrittelee lääkintälaitteille ja laitejärjestelmille sovellettavat toimitus-, huolto- ja korjausprosessit. Sairaaloiden tulee omissa toimintaohjeissaan ottaa huomioon nämä käyttäjiä, huoltajia ja huollon resursseja koskevat vaatimukset ja ohjeet. Nämä on otettava huomioon hankintavaiheessa.

Liitteessä A kuvataan lyhyesti sähköturvallisuuteen liittyviä suunnitteluvaatimuksia, joiden ylläpitäminen varmistetaan määräaikaishuoltojen, korjausten, kalibrointien ja päivitysten avulla. Kunkin kappaleen loppuun on liitetty maininta, miten kukin kohta liittyy käyttäjäorganisaatiolle ja miten käyttäjäorganisaatio voi ylläpitää ko. kohdan turvallisuutta. Laitejärjestelmän sähköturvallisuuteen liittyviä seikkoja on käsitelty yksityiskohtaisemmin Lääkelaitoksen julkaisussa [2], jossa käsitellään erityisesti eri laitteiden välillä syntyviä vuotovirtoja ja keinoja vuotovirtojen rajoittamiseksi.

4.2.2 Ohjelmistorajapinta ja ohjelmistojen turvallisuus

Lääkintälaitteissa ja laitejärjestelmissä käytettävät ohjelmistot muodostavat entistä merkittävämmän osan koko laitteen tai järjestelmän toiminnasta. Käytännössä ohjelmisto voi muodostaa lähes koko laitteen esimerkkinä sädehoidon annossuunnitteluohjelmistot tai lääketieteellisten kuvien digitaaliset arkistot. Elektronisten vahvistimien ja mittauspiirien toiminnassakin ohjelmiston merkitys voi olla huomattava, jos mittaussignaalia käsitellään erilaisten ohjelmallisten suotimien tai algoritmien avulla.

Ohjelmistorajapinnassa laitejärjestelmän omat ohjelmistot kohtaavat laitteiston, järjestelmän muita ohjelmistoja tai järjestelmän ulkopuolisia ohjelmistoja. Tällä rajapinnalla on merkittävä rooli laitejärjestelmän turvallisuuden, luotettavuuden ja suorituskyvyn varmistamisessa. Ohjelmistorajapinnan määrittely on huomattavasti monimutkaisempaa, kuin esimerkiksi sähköisten suureiden määrittely. Määrittelyssä on muistettava, että rajapinnat arvioinnin kohteena olevasta ohjelmasta muodostavat edelleen useita erillisiä rajapintoja.

Lääkintälaitteiden ja laite järjestelmien ohjelmistorajapinnan vaatimukset annetaan terveydenhuollon laitteita ja tarvikkeita koskevista säädöksistä. Sovellettavat standardit ovat esimerkiksi EN 60601-1-4 ja ISO 14971. Vaatimukset muuttuvat selkeistä mitattavista suureista prosessimaisemmiksi (riskianalyysit, kliininen tutkimus, suunnittelukäytännöt ja kliinisen tutkimuksen avulla osoitettu suorituskyky).

Huolimatta ohjelmistojen merkittävyydestä ja tärkeydestä laitteen turvallisuudessa on niiden testaus perinteisin testausmenetelmin lähes mahdotonta. Siinä missä sähköturvallisuus voidaan varmistaa standardin EN 60601-1 mukaisilla testeillä, joudutaan ohjelmiston testaus siirtämään osittain itse ohjelmiston arvioinnista ohjelmiston tuottavan prosessin arviointiin. Lisäksi vaatimusta riskienhallinnan toiminnoista osana koko tuotekehityksen elinkaarta ei voida osoittaa valmiista ohjelmistosta. Vaatimuksenmukaisuus voidaan arvioida ainoastaan suunnittelu- ja riskienhallintadokumentaatiolla ja niiden keskinäisellä jäljitettävyydellä.
Lääkintälaitteen ja laitejärjestelmän ohjelmistoihin liittyviä vaatimuksia ja käyttäjän mahdollisuuksia lisätä käytössä olevien ohjelmistojen turvallisuutta käsitellään laajemmin luvussa 6.

4.2.3 Toiminnallinen rajapinta

Toiminnallisessa rajapinnassa laitejärjestelmä kommunikoi eri tahojen kanssa. Vastapuoli voi olla joko toinen laite tai ohjelmisto (ks. ohjelmallinen rajapinta), mutta vastapuolena voi olla myös käyttäjä eli ihminen.

Vaatimuksina tällä rajapinnalla ovat edelleen turvallisuus ja luotettavuus, mutta lisätekijöinä mukaan tulee käytettävyys ja järjestelmän kyky kestää virheellistä käyttöä tai ilkivaltaa vastaa ja toisaalta myös niin päin, että järjestelmä ei myöskään heikennä potilaan, käyttäjän tai ym-

päristön turvallisuutta. Vaatimukset perustuvat edelleen terveydenhuollon laitteita koskeviin säädöksiin sekä yhdenmukaistettuihin standardeihin (EN 60601-1, EN 60601-1-1, EN 60601-1-2, EN 60601-1-4 ja riskianalyysit). Lisäksi on otettava huomioon tietoturva- ja tietosuojavaatimukset, henkilörekisterilaki, henkilöstölle asetetut pätevyysvaatimukset (kuka saa tehdä ja mitä saa tehdä) sekä organisaation omat menetelmäohjeet.

Toiminnallinen rajapinta on hyvin vaikea määritellä, koska toiminnallisuus voi ulottua sairaalan yhdestä tutkimushuoneesta toisen terveydenhuollon toimintayksikön toimenpide- tai tutkimushuoneeseen. Keinoja toiminnallisen rajapinnan turvallisuuden varmistamiseksi on mm. käyttökohteen määrittely, tiedon luokittelu, kliininen tutkimus, käytettävyystestit, suorituskykytestaus, riskienhallinta ja koulutus. Toiminnallisen rajapinnan merkittävimpiä tarkistuskohteita ovat laitejärjestelmän suorituskyky, inhimilliset tekijät ja järjestelmän käyttökoulutus.

4.2.3.1 Laitejärjestelmän suorituskyky

Puutteellisen suorituskyvyn aiheuttamat ongelmat voivat aiheuttaa useita erilaisia hoitotapahtuman vaarantavia tilanteita. Pienimmillään ne voivat keskeyttää hoitotapahtuman tilapäisesti. Vakavimmillaan ne voivat vaarantaa potilaan tai käyttäjän terveyden tai tuottaa virheellistä informaatiota potilaan tilasta, jonka seurauksena potilasta hoidetaan väärin. Virheellinen tilainformaatio voi taas aiheuttaa potilaan terveyden vaarantumisen tai turhia lisäkustannuksia.
Käyttäjän tulisi jo hankintavaiheessa määritellä testit ja testitapaukset, joilla laitetoimittaja osoittaa laitejärjestelmän täyttävän sille asetetut suorituskykyvaatimukset. Lähes poikkeuksetta tämä edellyttää, että hankinnasta vastaavassa ryhmässä on myös sovellusalan asiantuntijoita. Laitejärjestelmän päivitysten yhteydessä suorituskykytestit suoritetaan sopimuksen mukaisesti. Päivitysten suoritustapa ja sisältö tulee alustavasti määritellä jo hankintavaiheessa. Testitapausten ja -mittausten raportointi tärkeää, koska kirjattujen tulosten avulla voidaan mahdollisissa ongelmatapauksissa paikantaa vian lähde. Raportit ovat myös eräs kriteeri joiden perusteella hyväksytään toimituksen loppulasku.
Suorituskyvyn seuranta ohjelmistoa sisältävissä laitteissa ja laitejärjestelmissä on tärkeää myös normaalikäytössä. Suorituskykyä voi alentaa levytilan puute, levyjen pirstoutuminen, virheelliset konfiguroinnit tai puutteellinen kapasiteetti (liikaa käyttäjiä, kyselyiden puutteellinen optimointi käyttäjämäärään nähden, keskusmuistia liian vähän käyttäjä-

määrään nähden jne.). Liitteessä E on kuvattu ohjelmistoon liittyviä kohteita, joita voidaan säännöllisin väliajoin tarkastaa.

4.2.3.2 Inhimilliset tekijät

Eräs vaaran lähde voi olla käyttäjän virheellinen toiminta. Inhimillisistä seikoista johtuvia vaaroja voidaan vähentää hyvän suunnittelun ohella koulutuksella ja hyvillä käyttöohjeilla. Toisaalta suunnittelijan perehtyminen sairaalan tai käyttäjän tapaan toimia todellisessa hoitotilanteessa voi auttaa suunnittelijaa välttämään inhimillisten virheiden mahdollistavia suunnitteluratkaisuja. Tällä tavoin laitteen suunnittelussa voidaan huomioida inhimillinen käyttäytyminen ja sen mukanaan tuomat riskitekijät. Hyvä suunnittelukäytäntö on myös sellainen, että laitteen oikea käyttö on loogisempaa kuin virheellinen käyttö, jos virheellistä käyttöä ei voi muutoin kuin ohjeella estää. Terveydenhuollon laitteita koskevat säädökset edellyttävät myös ergonomisten seikkojen huomioonottamista tuotesuunnittelussa. Valmisteilla olevassa standardissa (EN 60601-1-6) tullaan määrittelemään käytettävyyteen liittyviä seikkoja huomattavasti tarkemmin.

4.2.3.3 Koulutuksen merkitys

Tämän päivän laitteet ja laitejärjestelmät ovat ominaisuuksiltaan erittäin monimutkaisia. Tämän vuoksi hoito- ja huoltohenkilökunnan kannalta on tärkeää hankinnan yhteydessä määritellyt ja järjestetyt koulutustilaisuudet. Tätä seikkaa ei välttämättä kaikissa käyttökohteissa tiedosteta riittävän hyvin. Ongelmana on myös se, että käyttäjät vaihtuvat ja käyttökoulutus ei välttämättä tavoita kaikkia. Näin ollen käyttö- ja huoltokoulutukset on uusittava aina tietyin väliajoin. Laitteen oikean huollon kannalta on tärkeää, että laitteen huollosta vastaavat henkilöt osallistuvat myös käyttökoulutuskursseille.

Hankintavaiheessa on määriteltävä myös laitejärjestelmän huoltotarpeet, käyttöpaikan ja teknisen huollon rooli sekä vastuun jako. Tässä yhteydessä voidaan määritellä myös:

- vastuuhenkilöt käyttökohteessa ja lääkintälaitehuollossa (informaation seurattava myös järjestelmän mukana)
- käyttökoulutuksen suunnittelu yhdessä vastaanottotarkastuksesta vastaavan yksikön ja laitteen käyttöpaikan kesken.

Vastuujaon ja vastuuhenkilöiden määrittelyllä nopeutetaan laitteen huoltoa ja varmistetaan, että tarvittavat vikailmoitukset ja muut käyt-

töön vaikuttavat tiedot menevät oikeille henkilöille. Koulutuksen merkitystä ei saa väheksyä. Tärkeää on myös ajan tasalla oleva koulutusrekisteri, jonka avulla voidaan suunnitella tarvittava lisäkoulutus ja täten varmistaa riittävä osaaminen organisaatiossa.

4.3 Langaton tiedonsiirto laitejärjestelmissä

4.3.1 Yleistä

Langattomalla tiedonsiirtotekniikalla (WLAN) tässä yhteydessä tarkoitetaan standardin IEEE 802.11 mukaista tiedonsiirtoa, joka tapahtuu langattomasti joko infrapuna- tai radiotaajuustekniikan avulla. WLAN on langaton radiotaajuustekniikka, joka toimii taajuudella 2,4 Ghz tai 5,0 GHz. Tällä hetkellä yleisimmin tuntuisi olevan käytössä 2,4 GHz alueella toimiva WLAN (IEEE 802.1b). Sen nimellinen tiedonsiirtonopeus on 1 - 11 Mb/s. Standardin IEEE 802.1a mukainen WLAN toimii taajuudella 5 GHz ja sen nimellinen tiedonsiirtokapasiteetti on 6–54 Mb/s. WLAN-tekniikkaa koskevia standardeja kehitetään jatkuvasti. Työn alla on ainakin jo standardi IEEE 802.1g, jossa siirtonopeus olisi jopa 20 Mb/s. Suurimmaksi lähetystehoksi on standardeissa määritelty 100 mW, mutta käytännössä lähetysteho on tätä alhaisempi. Alentuneen lähetystehon ja kasvaneen taajuuden ansiosta on mahdollista, että WLAN-tekniikan käyttö on jopa turvallisempaa ja luotettavampaa, kuin matkapuhelimien avulla tapahtuva liikennöinti sairaaloissa. Lopullinen varmuus voidaan osoittaa ainoastaan riittävillä kenttäkokeilla.

4.3.2 WLAN ja laitejärjestelmät

Langattoman tiedonsiirtotekniikan käyttö laitejärjestelmien osana lisääntyy. Langattomuus tuo useita uusia mahdollisuuksia laitejärjestelmien käytölle; esimerkiksi liikkuvuuden paraneminen, hankalien kiinteiden ja laitteitta rajoittavien kaapelointien väheneminen sekä osittain myös sähköturvallisuuden lisääntymien lääkintälaitteiden ja tiedonsiirtoverkkojen välillä. WLAN- ja mahdollisesti myös Blue Tooth -tekniikoiden voidaan olettaa mahdollistavan ainakin seuraavanlaisien sovelluksien ja ominaisuuksien kehittymisen lyhyellä aikavälillä:

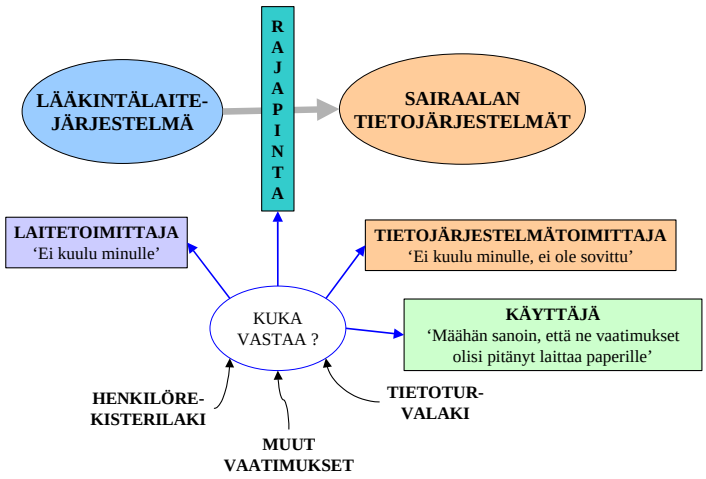
- potilaan terveydentilaa voidaan valvoa reaaliaikaisesti, paikasta riippumatta sekä käsitellä tuloksia vastaanottopisteessä esim. kuljetustilanteiden aikana
- potilas voidaan paikantaa mahdollisen sairauskohtauksen aikana
- potilasmonitoroinnissa syntynyt tieto siirretään reaaliaikaisena potilastietojärjestelmään

- potilastietoja voidaan käsitellä paikasta riippumatta
- etädiagnostiikan mahdollisuus.

On täysin mahdotonta tehdä täydellistä arviota tekniikan kehittymisestä 2-5 vuoden kuluessa. Tekniikka ja laitteet tulevat kuitenkin kehittymään, joten sairaaloiden tulee varmistua siitä, että valittu tekniikka täyttää sairaaloiden tarpeet ja toisaalta myös niin päin, että sairaala organisaationa on valmis (kykenee) käyttämään valittua tekniikkaa. Valitun tekniikan käyttöönotto edellyttää ohjeistuksen laadintaa, koulutusta sekä vanhan tekniikan osittaista soveltamista uuteen tekniikkaan. Tämä edellyttää organisaatioilta tekniikan uudelleen arviointia, suunnittelu- ja koulutuspanostusta, jonka onnistuminen nähdään vasta jonkin ajan kuluttua uusien tekniikoiden käyttöönotosta.

4.3.3 Uusi tekniikka ja uudet vaatimukset

Valmistajan kannalta merkittäviä tuotekehityspanostuksia joudutaan kohdistamaan tekniikan luotettavuuteen ja järjestelmän tietoturvaominaisuuksiin. Ongelman voi myös aiheuttaa se, että WLAN-teknologia toimii hyvin useasti valmiilla kolmannen osapuolen ohjelmistoalustoilla, jolloin lääkintälaitevalmistajan tehtäväksi jää varmistaa ns. COTS -komponenttien ja ohjelmistojen soveltuvuus terveydenhuollon tuotteille asetettuihin vaatimuksiin.



***Kuva 14**. Kuka vastaa rajapintavaatimuksista ?*

Käyttäjän kannalta WLAN-teknologia tuo mukanaan uuden tekniikan yhteensovittamisen jo olemassa oleviin omiin tietojärjestelmiin, mikä jo

sinänsä on iso kertaluonteinen työpanos. Lisäksi käyttäjän eli terveydenhuollon toimintayksikön vastuulla on varmistaa esim. potilastietojärjestelmien ja digitaalisten kuva-arkistojen tietoturva niissä tapauksissa, kun tietojärjestelmiin lähetetään lääkintälaitejärjestelmistä kerättyä tietoa. Tässä kohtaa lainsäädännön vaatimukset eivät välttämättä ole aivan aukottomia ja yksiselitteisiä. Vastuut määräytyvät viime kädessä järjestelmien käyttötarkoituksesta. Kuvan 14 esimerkissä valmistajan ja käyttäjän kannalta paras ratkaisu olisi mahdollisimman tarkat yhteistyössä laitetoimittajan kanssa tehdyt määrittelyt tietojärjestelmien rajapinnoista. Määrittelyillä voidaan varmistaa järjestelmien keskinäinen yhteensopivuus ja luotettava toiminta.

Mikäli hankintaprosessin alkuvaiheessa on useita laitetoimittajaehdokkaita, voidaan määrittely tehdä kahdessa eri vaiheessa. Ensimmäinen määrittely on alustava, jossa voidaan vertailla eri laitetoimittajien ratkaisuja. Lopullinen määrittely tehdään ennen virallista tilausta yhteistyössä tarjouspyynnön voittaneen laitetoimittajan kanssa. Määrittelyissä on huomioitava mm. mobiilitekniikan erityispiirteet, kuten esimerkiksi WebPadin käyttö, sovellusten käyttäjien tunnistus, käyttäjien luokittelu ja tiedon keruu, tietoturva ja yhteydet suljettuihin tietoverkkoihin (VPN). Lisäksi uusi tekniikka tuo tullessaan laajan koulutustarpeen sekä ylläpidosta vastaaville että käyttäjille.

Voidaan tietysti esittää kysymys, että onko välttämättä aina otettava viimeisin tekniikka käyttöön. Tähän voi vastata ainoastaan käyttäjäorganisaatio itse. Varmaa on vain se, että järjestelmien suorituskyky ja monimutkaisuus kasvaa jatkuvasti, tuoden mukanaan muutoksia ja niistä aiheutuvia etuja ja haittoja. WLAN on kuitenkin mahdollisuus, jota kannattaa vakavasti harkita.

4.4 Näkökohtia laitejärjestelmän tarkastuksesta

Käyttäjäorganisaation kannalta laitejärjestelmän vastaanottotarkastuksen yhteydessä tehtävät laajat täydellisen tyyppitarkastuksen kaltaiset testit ovat tarpeettomia. Vastaanottotarkastuksella ei myöskään voida korjata esitutkimuksen ja määrittelyvaiheen aikana tapahtuneita puutteita tai laiminlyöntejä.

Vastaanottotarkastus tuleekin ennemmin kohdistaa toimituksen yhdenmukaisuuden, suorituskyvyn ja laitteiden hyväksyntöjen varmistamiseen. Olisi myös suotavaa, että hiemankin isommalla laitteistotoimituksella olisi yksi toimituksesta vastaava henkilö, jonka kautta kaikki tieto kul-

kisi ja jolla viime kädessä olisi kokonaisvastuu järjestelmän toimituksesta ja kokoonpanosta. Liitteessä B on esimerkkejä asioista, joita vastaanottotarkastuksessa on syytä ottaa huomioon.

Käytännössä on usein havaittu, että laitteet yksittäin täyttävät niille asetettavat vaatimukset, mutta koko laitejärjestelmän vaatimustenmukaisuutta ei ole osoitettu. Tähän vastaanottotarkastuksessa on erityisesti kiinnitettävä huomiota.

5. LAITEJÄRJESTELMÄN ELINKAARI JA YLLÄPITO

5.1 Elinkaari valmistajan kannalta

Valmistajat ovat jo jonkin aikaa hallinneet laitteen suunnittelua, valmistusta ja ylläpitoa ns. elinkaarimallin avulla. Valmistajan kannalta laitteen tai laitejärjestelmän elinkaari jakaantuu kahteen vaiheeseen. Ensimmäisen vaiheen muodostaa tuotekehityksen elinkaari, jossa alustavien kartoitusten, analyysien ja vaatimusmäärittelyjen jälkeen laite suunnitellaan, toteutetaan ja vapautetaan tuotantoon. Valmistuksen jälkeen alkaa varsinainen laitteen käytön aikainen elinkaari, johon sisältyvät asennus, koulutus, käyttö, ylläpito ja käytöstä poisto.

Lainsäädännön vaatimukset velvoittavat valmistajia sisällyttämään terveydenhuollon laitteiden elinkaareen myös aktiivisen riskienhallinnan, joka kattaa tuotteen suunnittelun ja valmistuksen. Käytön aikaisen riskienhallinnan kattaa tuotannon jälkeisen informaation keruuvaihe, jonka avulla valmistaja kerää laitteen käytön aikaista tietoa ja tekee tarvittavia toimenpiteitä saadun tiedon perusteella. Toimenpiteinä voi olla esim. tuotteen poistaminen markkinoilta, muutokset tuotannossa, tuotteen komponentin vaihto, päivitykset tai käyttäjätiedotteet.

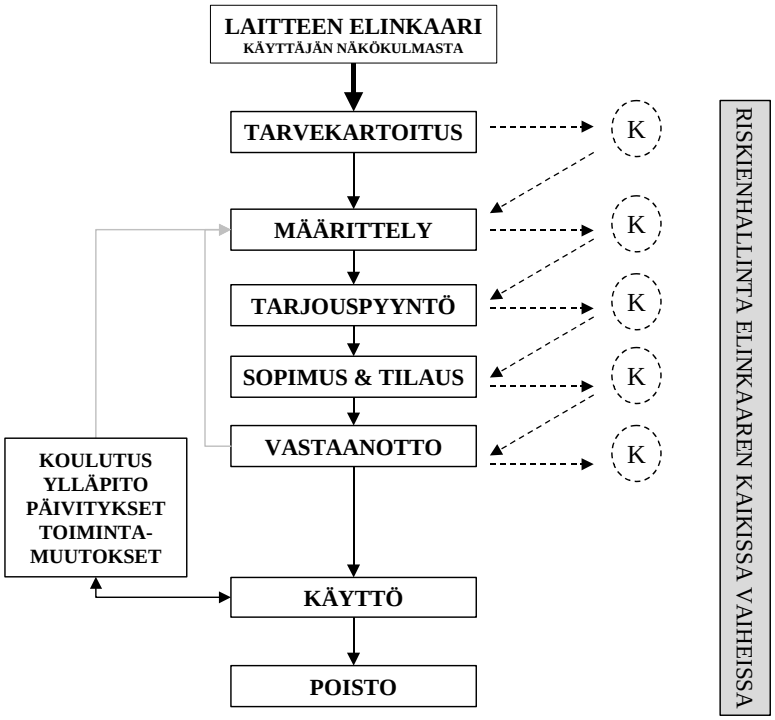
5.2 Elinkaari käyttäjän kannalta

Käyttäjän kannalta elinkaari on hieman erilainen kuin valmistajan ns. tuotekehityksen elinkaari. Käytön elinkaari alkaa myös tarvekartoituksella ja määrittelyllä lähes samoin kuin tuotekehityksen elinkaarikin. Tämän jälkeen elinkaaren seuraavat vaiheet poikkeavat suunnittelun elinkaaresta. Tosin näissäkin vaiheissa on yhteneväisiä piirteitä.

Käyttäjän kannalta tärkeimmät vaiheet ovat esitutkimus, määrittely, tarjouspyyntö ja tilaus. Näiden vaiheiden sisältöön voi vaikuttaa myös käyttövaihetta tukevista toiminnoista saatu palaute. Tässä vaiheessa käyttäjällä on kaikki mahdollisuudet vaikuttaa hankinnan onnistumiseen. Näin ollen hankinta kannattaa suunnitella ja valmistella huolella, koska sillä on vaikutusta toiminnan laatuun ja pidemmällä aikavälillä myös kustannuksiin.

Käyttäjä voi ottaa käyttöön elinkaaren eri vaiheita tukemaan ns. katselmukset (kuva 15). Katselmuksissa varmistetaan, että kaikki vaiheen tehtävät on suoritettu hyväksytysti ja vaiheille asetetut tavoitteet on saavu-

tettu. Katselmuskäytäntö edellyttää eri vaiheille asetettujen tavoitteiden selkeää kirjausta. Tämä edellyttää myös toimintaohjeiden laatimista, jossa ohjeistetaan suunnittelukatselmusten tavoitteet ja toteutus.



Kuva 15. *Laitejärjestelmän elinkaari käyttäjän kannalta.*

Hankintavaiheessa on erittäin tärkeää määritellä myös järjestelmien ohjelmistot, kattaen sovellusohjelmat, käyttöjärjestelmät, ohjaustiedostot (ajuri) sekä em. ohjelmistoille sovellettavat tietoturvaratkaisut. Mikäli laite tai laitejärjestelmä kytketään jo olemassa olevaan järjestelmään tai tietoverkkoon tulee myös liitynnän rajapintavaatimukset määritellä sisältäen vaatimukset toiminnallisuudelle, sähköturvallisuudelle, tietoturvallisuudelle ja ohjelmistoille. Tietoverkon määrittelyssä tulee ottaa huomioon kaapelointien ja verkon aktiivisten laitteiden asettamat vaatimukset. Toteutetut ratkaisut vaikuttavat tietoturvateknologiaan ja fyysiseen tietoturvaan (laitteiden ja kaapelointien sijoittelu). Ratkaisujen on noudatettava organisaation tietoturvapolitiikkaa.

Hankintavaihetta voidaan tukea erilaisilla tarkistuslistoilla, joissa voidaan ottaa huomioon myös asennuksen, teknologian, huollon, koulutuk-

sen ja käytön aiheuttamia kustannuksia. Liitteessä C on esimerkkejä asioista, joiden avulla voidaan varmistaa hankinnan aikaisen määrittelyn onnistumista. Onnistuneella määrittelyllä voidaan selkiyttää myös muiden vaiheiden toimintaa. Avainkysymyksiä käyttäjän kannalta ovat, kuinka turvallisuusvaatimukset ja riskienhallinta saadaan integroitua laitteen tai järjestelmän käytönaikaiseen elinkaareen ja toisaalta kuinka kuvatut keinot saadaan muutettua käytännön ratkaisuiksi.

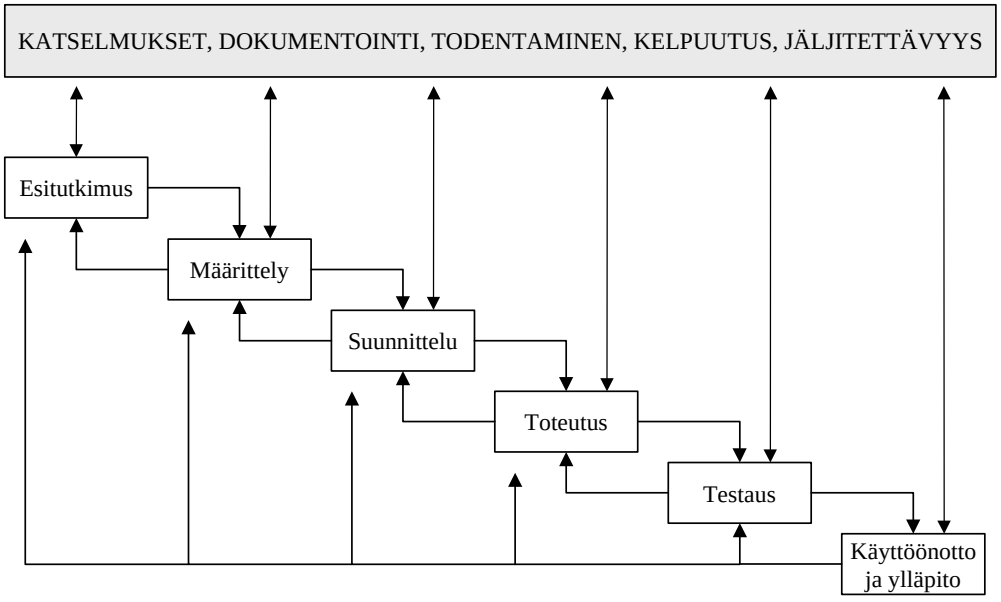
6. OHJELMISTOJEN TURVALLISUUS

6.1 Yleinen ohjelmistotuotantomalli

Valmiin ohjelmiston turvallisuutta ei käytännössä voida täydellisesti varmistaa. Periaatteessa testauksien (Black-Box- ja Glass-Box) avulla voidaan varmistaa ohjelmiston turvallisuus ja suorituskyky täydellisesti. Tämä on kuitenkin mahdollista vain 'periaatteessa', koska hiemankin laajemman ohjelmiston kaikkien ominaisuuksien, toimintojen ja muuttujien käsittely kaikissa eri tilanteissa vaatii liian paljon aikaa. Tämän takia ohjelmistojen turvallisuuden arviointi ulotetaankin valmiista ohjelmistosta sitä tuottavan prosessin arviointiin.

Ohjelmiston tuotantoprosessin tyypillisimpiä tunnusmerkkejä ovat määrittely, vaiheistus, tavoitteet ja dokumentointi. Parhaiten näiden vaatimusten toteutuminen on voitu toteuttaa ohjelmistotuotannon elinkaarimallilla.

Ohjelmiston elinkaarimalleja on lyhyen ohjelmistokehityksen historian aikana kehitetty useita (esimerkiksi vesiputous-, spiraali- tai inkrementaalimalli). Perinteistä ja laajalti käytettyä elinkaarimallia edustaa ideaalinen vesiputousmalli, jossa tuotanto etenee hyvin määritellyissä perättäisissä vaiheissa. Kullekin vaiheelle on määritelty tavoitteet, joiden täyttymistä valvotaan vaiheen päättävissä katselmuksissa (kuva 16). Elinkaarimallin onnistumista voidaan punnita määrittelyn ja toteutuksen välisellä jäljitettävyydellä, jossa mistä tahansa valmiin ohjelmiston vaihedokumentista voidaan siirtyä eteen tai taaksepäin.



***Kuva 16**. Tyypillinen ohjelmistotuotannon elinkaari*

Tyypillisesti vaihejakomallista on löydettävissä vähintään seuraavat toiminnot:

- Hallinta. Projektin tavoitteita valvotaan ja varmistetaan käytettyjen riskianalyysitekniikoiden soveltuvuus projektiin, resurssien riittävyys, teknologiaosaaminen, aikataulut, kustannukset sekä verifiointien ja validointien riittävyys.
- Esitutkimusvaihe. Hankkeen järkevyys ja mahdollisuudet arvioidaan.
- Vaatimusten määrittely. Esitutkimusvaiheen tieto jalostetaan analyysien ja pohdintojen jälkeen järjestelmän vaatimuksiksi.
- Suunnitteluvaihe. Järjestelmä suunnittelu voidaan jakaa useisiin eri tasoihin. Tässä vaiheessa jo tulevat mukaan mahdolliset alihankinnat tai COTS-komponenttien ostot. Mikäli ostotoiminta tapahtuu erillisen osto-osaston kautta, tulee suunnittelutiimin määritellä vaatimukset ostoille ja ns. vastaanottotarkastuksen spesifikaatiot ostotiimille.
- Toteutusvaihe (implementointi). Määriteltyjen vaatimusten ja suunnitteludokumentaation mukaisesti laaditaan ensimmäinen 'toimiva ohjelmakoodi', joka voi tarkoittaa ensimmäistä virheetöntä käännöstä tai ensimmäistä toimivaa kokeiluversiota. Ohjelmiston mukana seuraavan dokumentaation tuottaminen tulisi aloittaa viimeistään tässä vaiheessa.
- Testaus. Ohjelmistosta haetaan virheitä ennalta laaditun suunnitelman mukaisesti. Testaus kattaa kaikki ohjelmamoduulit, ohjelmamoduulien keskinäisen kommunikoinnin sekä järjestelmätestauksen.
- Käyttöönotto ja ylläpito. Ohjelmisto asennetaan, otetaan käyttöön ja annetaan käyttökoulutus. Tässä vaiheessa ohjelmistoon voidaan asentaa myös uusia ominaisuuksia ja korjataan käytön aikana havaittuja virheitä.

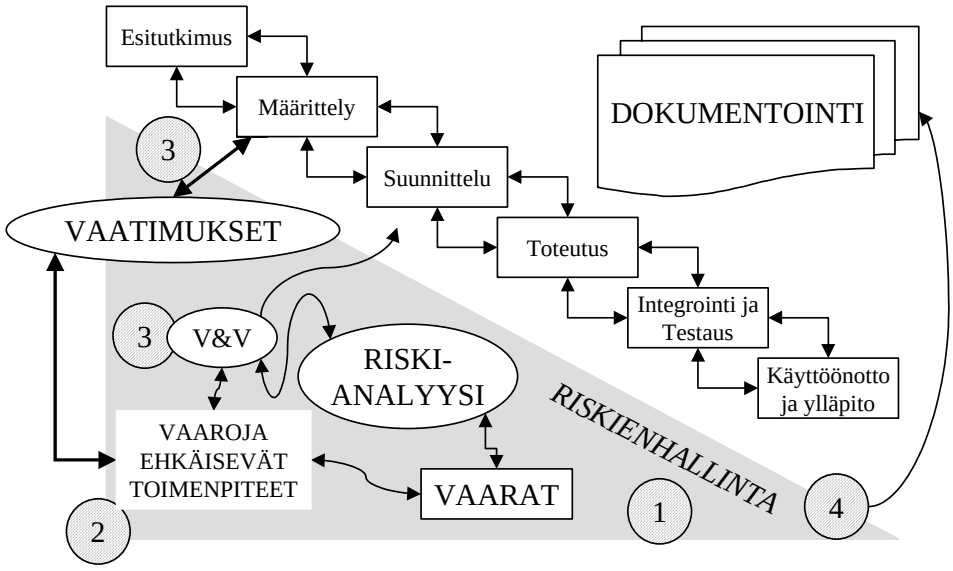
Tarkempaa tietoa ohjelmistotuotannon elinkaarimalleista, jäljitettävyydestä, todentamisesta ja kelpuutuksesta sekä jäljitettävyyden mahdollistavista vaihedokumenteista ja niiden sisältövaatimuksista löytyy esimerkiksi Haikalan ja Märijärven kirjoittamasta kirjasta 'Ohjelmistotuotanto' [3].

Ohjelmistotuotantoa sekä vaatimuksia sen eri vaiheille käsitellään laajasti IEEE:n standardisarjassa (http://standards.ieee.org/catalog/olis/se.html).

Ohjelmistotuotannon vaihejakomalleja käsitellään standardeissa IEEE 1074:1997 'Standard for Developing Software Life Cycle Processes (Software)' ja ISO/IEC 12207:1995 Information technology - Software life cycle processes. Standardit kuvaavat erittäin laajasti ohjelmistotuotannon eri vaiheita ja toimintoja. Näitä standardeja tulisikin lisätä soveltuvin osin osaksi suunnittelun lähtötietovaatimuksia. Esimerkkinä IEEE-standardien soveltamisesta terveydenhuollossa voisi mainita standardin IEEE 829:1998 'Standard for Software Test Documentation'. Standardia voi soveltaa siten, että jo hankintavaiheessa määritellään laitteistojen ohjelmistopäivityksien suoritustapa ja ohjelmistopäivityksien testitapaukset ja testaus raportoidaan ko. standardin mukaan.

6.2 Terveydenhuollon laitteen ohjelmistotuotanto

Terveydenhuollon laitteiden ohjelmistosuunnittelussa voidaan käyttää yleisiä hyväksi havaittuja ohjelmiston suunnittelu- ja tuotantomenetelmiä. Säädösten vaatimuksista johtuen (olennaiset vaatimukset, kohta 2 ja 12.1) terveydenhuollon laitteiden ohjelmistosuunnittelulle asetetaan lisävaatimuksia lähinnä riskienhallinalle, jäljitettävyydelle, raportoinnille ja käytetyille riskienhallintakeinoille (kuva 17).



***Kuva 17**. Terveydenhuollon laitteen ohjelmistotuotannon eroja*

Merkittävimmät erot terveydenhuollon tuotteen ohjelmistosuunnittelussa voidaan kiteyttää neljään kohtaan (vrt. kuva 17):

1. Riskienhallinnan tulee kattaa koko tuotekehityksen elinkaari aina ohjelmistotuotteen vapautuksesta tuotantoon. Riskienhallintaprosessiin kuuluu myös tuotannon jälkeinen informaatio. Tämä edellyttää valmistajaa keräämään tietoa asiakkaille toimitetuista ole-

vista tuotteista (korjaavat ja ennaltaehkäisevät toimet, ilmoitukset vaaratilanteista). Mikäli käytössä olevissa tuotteissa havaitaan ongelmia, tulee valmistajan käynnistää tarpeelliset riskienhallintatoimenpiteet, joilla havaitut vaarat poistetaan ja ongelmat korjataan. Riskienhallintaprosessi sisältää suunnittelussa aina tuotekohtaisen riskienhallintasuunnitelman, verifiointi- ja validointisuunnitelmat sekä kulloinkin käytetyn tai sovelletun tuotekehityksen elinkaaren. Tarvittaessa valvontaviranomainen voi tutkia näitä asioita valmistajan riskienhallintatiedostosta (RMF) ja riskienhallintaselostuksesta (RMS).

2. Riskianalyysissä havaittuja vaaroja poistavat tai niiden riskiä pienentävät keinot tulee saada tuotteen toiminnallisiksi vaatimuksiksi. Vaatimusten täyttyminen edellyttää useampaa kierrosta alustavan riskianalyysin – vaatimusten määrittelyn - riskianalyysin ja vaatimusten määrittelyn välillä. Tämä edellyttää myös jäljitettävyyttä vaatimuksista analyysiin ja päinvastoin.
3. Verifiointi- ja validointisuunnitelmien tulee kattaa erityisesti turvallisuusvaatimukset. Validoinnin riippumattomuus on myös kyettävä osoittamaan. Tarkempaa tietoa vaatimuksista löytyy standardista EN 60601-1-4 sekä IEEE-standardisarjasta.
4. Terveydenhuollon laitteen viranomaisvaatimusten toteutuminen osoitetaan käytännössä suunnittelun dokumentaatiolla. Dokumentoinnilla osoitetaan esimerkiksi suunnittelun lähtötietojen oikeellisuus, riskianalyysissä tehdyt päätökset ja riskin hyväksyttävyys, jäännösriskien kuvaus, käytetyt suunnittelumenetelmät, tuotteen suorituskyky sekä virhemarginaalit että laitteen valmistuksessa käytetyt materiaalit. Esitetyssä dokumentaatiossa on tärkeää myös dokumenttien keskinäinen jäljitettävyys.

Suunnitteludokumentaatio muodostaa myös osan riskienhallintatiedostoa (RMF) sekä riskienhallintaselostusta (RMS), jota vaatimusta ei välttämättä muilla tuoteryhmillä ole. Tästä syystä dokumentointi on avainasemassa vaatimusten mukaisuuden osoittamisessa. Vaatimuksissa korostuvat erityisesti vaikuttavuus- ja turvallisuusnäkökohdat.

6.3 Käyttäjän keinoja varmistua ohjelmistojen turvallisuudesta

Tällä hetkellä valmiita laatumittareita ohjelmistotuotannon ja ohjelmistojen laadun mittaamiseksi on jo olemassa. Valitettavasti useat niistä toimivat parhaiten tuotekehityksen aikana (jäljitettävyys, testattavuus, virheettömyys, vaatimusten ristiriidattomuus jne.). Miten käyttäjät eli terveydenhuollon toimintayksiköt sitten voivat varmistua toimitettavien ohjelmistojen turvallisuudesta, suorituskyvystä tai vaatimustenmukaisuudesta.

Käyttäjän tarvitsemaa helppokäyttöistä 'yleismittaria', joka käytännössä tarkoittaa selkeitä ohjeita ja oppaita ei ohjelmistojen laadun määrittämiseksi vielä ole kehitetty. Ohjeidenkin ongelmana voi olla niiden teknologiariippuvaisuus. Toisin sanoen www-sovellusten tarkastusohje ei välttämättä sovellu C++ -sovellukselle. Alkuvaiheessa käyttäjä voi kuitenkin pohtia ainakin seuraavien keinojen käyttöä:

- Terveydenhuollon laitteen ohjelmistoja suunniteltaessa ja valmistettaessa tulee kiinnittää huomiota siihen, että ohjelmistotuotannon elinkaarella ja sen vaiheistuksilla on merkittävä osuus tuotteen laadun, turvallisuuden ja luotettavuuden suhteen. Tästä syystä käyttäjä voi kysyä laitetoimittajalta, että onko tuotteen suunnittelu toteutettu jonkin elinkaarimallin mukaisesti. Osoitus ohjelmistotuotannon vaihejakomallin soveltamisesta voisi olla eräs vaatimus hankintavaiheen määrittelyssä.
- Terveydenhuollon yksiköt voisivat yhteistyössä laatia yhtenäisiä ns. de facto -standardeja, jotka avoimesti esitetään laitetoimittajille uushankinnan, muutosten ja päivitysten yhteydessä. Tehokkaaksi tämän keinon tekee ainoastaan yhteistyö eli kaikilla terveydenhuollon yksiköillä on samanlainen käytäntö ja samanlaiset ohjeet hankintaprosessissa.

Ohjeistuksia laadittaessa on huomioitava, että ne soveltuvat kaikille tahoille ja etteivät ne olisi teknologiariippuvaisia ohjeita. Kukin sairaala voi lisätä näiden ylätason ohjeiden tueksi omia, tietyn teknologian tai sovelluksen huomioivia tarkistuslistoja. Ohjeiden laadinnassa tulee myös huomioida, että ne ovat yhdenmukaisia organisaation muiden laadunvarmistusohjeistuksen kanssa. Liitteessä C on kuvattu esimerkkejä, joita voi lisätä osaksi hankintaa tukevia tarkistuslistoja.

6.4 Ohjelmiston päivitykset ja muutokset

Muutokset laitteessa sen elinkaaren aikana ovat hyvin normaaleja ilmiöitä, joilla valmistaja pyrkii esimerkiksi parantamaan laitteen suorituskykyä, lisäämään tuotantomääriä, alentamaan tuotantokustannuksia, parantamaan laitteensa kestävyyttä tai lisäämään siihen uusia ominaisuuksia markkinoiden vaatimuksesta.

Muutokset kohdistuvat yleensä ohjelmiston, rakenteen, materiaalien, tuotannon tai itse laitteen ominaisuuksien muutokseen. Valmistajan tulee huolehtia laitteen vaatimustenmukaisuudesta myös muutoksen jälkeen. Yleensä muutos edellyttää vähintään riskianalyysin päivittämistä, mutta muutoksen laajuuden mukaan voidaan joutua uusimaan myös sähköturvallisuustestejä, mekaanisia testejä, ohjelmiston turvallisuuden arviointia, kliinisiä kokeita ja suorituskykymittauksia, joko osittain tai kokonaan. Muutokset laitteessa, tuotannossa ja suorituskyvyssä sekä vaatimustenmukaisuuden täyttyminen tulee dokumentoida. Laitteen mukana seuraavien asiakirjojen päivitystä ei saa unohtaa.

Käyttäjän kannalta muutosta ei voi hyväksyä käyttöön ilman perusteluja ja riittävän kattavaa testisuunnitelmaa. Käyttäjää voi helpottaa tieto siitä, että säädökset edellyttävät valmistajaa ilmoittamaan kaikki merkittävät muutokset ilmoitetulle laitokselle uudelleen arviointia varten (ainoastaan korkeamman riskiluokan tuotteet ja ne tuotteet, joiden markkinoille saattaminen on toteutettu yhteistyössä ilmoitetun laitoksen kanssa). Näin ollen käyttäjä voi tiedustella valmistajalta tai maahantuojalta tätä muutosilmoitusta, josta pitäisi ilmetä seuraavat seikat:

- muutosselvitys (mitä, miksi ja kuka on muuttanut ja arvio muutoksen merkittävyydestä)
- miksi tietoa muutoksesta ei ole toimitettu ao. ilmoitetulle laitokselle
- aiheuttaako tehty muutos uusia vaaroja, joita aiemmin ei ole käsitelty (päivitetty tai kokonaan uusi riskianalyysi)
- onko laitteen suorituskyky, käyttötarkoitus tai käyttötapa muuttunut (järjestelmätestaus, suorituskykymittaukset)
- riittävätkö olemassa olevat kliiniset tiedot uusiin ominaisuuksiin
- onko ohjelmiston edellisen version asiakaskohtaiset sovitukset otettu huomioon muutoksessa tai päivityksessä
- vastaavatko kieliversiot ja päivämääräasetukset aiempaa ohjelmaversiota
- onko muutoksesta tai päivityksestä toimitettu riittävät testaus-, verifiointi- ja validointiraportit

- onko laitteen tai laitejärjestelmän mukana seuraavat asiakirjat päivitetty (käyttöohjeet, kytkentäkaaviot ja huolto-ohjeet).

Ohjelmistomuutosten osalta (pätee osittain myös muihin ominaisuuksiin) käyttäjäorganisaatio voi edellyttää laitetoimittajalta tietyn ohjelmiston muutoshistoriaa. Muutoshistoriassa kuvataan ohjelmistolle tehdyt muutokset, arvioidaan muutosten vaikutusta ohjelmiston suorituskykyyn ja luotettavuuteen ja määritellään menetelmät muutosten kelpuuttamiseksi tuotantoon (validointi). Täten muutoshistorian avulla saadaan selvitettyä, miten ohjelmistomuutos on toteutettu, dokumentoitu ja hyväksytty.

Tapauskohtaisesti muutos voi tuottaa seuraavanlaisia dokumentteja:

- riskienhallintasuunnitelma ja päivitetty riskianalyysi sisältäen uusien riskien tunnistuksen
- verifiointisuunnitelmat ja raportit yksikkö- ja järjestelmätasolla sisältäen hyväksyntä kriteerit, testiraportit, yhteenvedon ja testi tulokset
- validointisuunnitelmat ja raportit.

6.5 Ohjelmiston testaus

Testauksen tarkoituksena on varmistua ohjelmiston suorituskyvystä ja luotettavasta toiminnasta. Periaatteessa riittävän kattavalla testauksella voidaan osoittaa ohjelmiston täydellinen virheettömyys (edellyttää tietysti välillä löydettyjen virheiden korjausta). Käytännössä tämä on kuitenkin mahdotonta, koska yleensä tuotekehitysprojektilla on tietyt etukäteen sovitut aikataulu- ja kustannusvaatimukset, joita ei voida ylittää. Tästä syystä voidaan väittää, että ohjelmistoissa on aina joitain virheitä. Väittämää tukevat useat esimerkit, joissa ohjelmiston käytön yhteydessä on havaittu, että hankittu ohjelmisto ei toimikaan odotetulla tavalla.

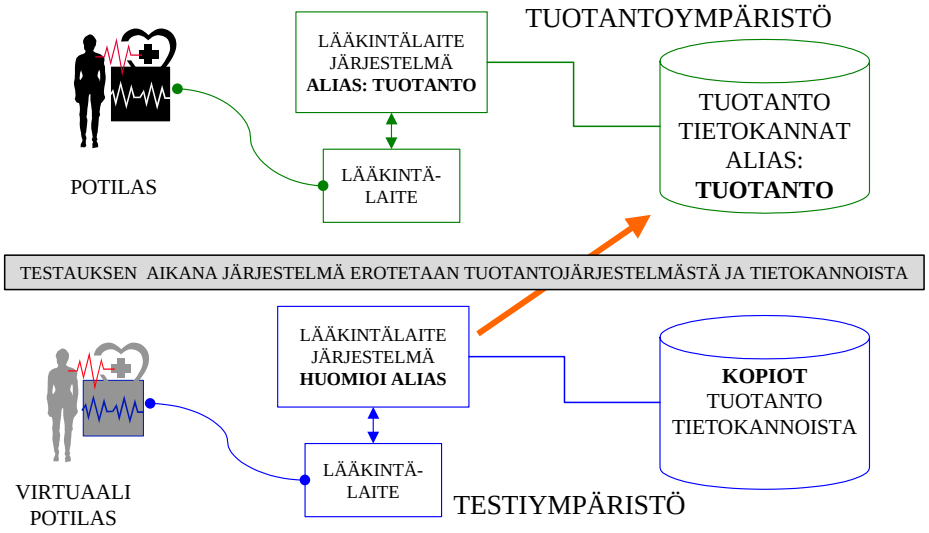
Valmistaja testaa ohjelmiston hieman eri tavalla ja eri lähtökohdista kuin käyttäjä. Valmistajalla on täydelliset mahdollisuudet hyvin yksityiskohtaisiin ja laajoihin testeihin, kun taas käyttäjä hankkii usein valmiin ohjelmiston, jolloin mahdollisuudet täydelliseen testaukseen ovat erittäin huonot. Tästä huolimatta molempien osapuolien suorittaman testauksen tulisi olla toisiaan tukevaa ja riittävän kattavaa. Mikäli hankinnan määrittelyvaiheessa on sovittu vastaanottovaiheessa suoritettavista testeistä, on käyttäjällä ohjelmiston testaukseen hieman paremmat mahdollisuudet.

Käyttäjät voisivat ruveta edellyttämään hankintojen yhteydessä toimitettavia ohjelmistojen virhelistoja (’bugilistaukset’), joissa valmistajat avoimesti listaavat ohjelmistossa olevia virheitä tai toimimattomuuksia. Lopullisessa käyttöönoton yhteydessä tapahtuvassa testauksessa testataan myös ilmoitettujen virheiden vaikutus sovellukseen ja sen luotettavuuteen. Tällaiset viralliset virhelistat voivat tuntua järjettömiltä, mutta todellisuudessa niiden julkistamiselle löytyy aivan selkeät vaatimuksetkin (ks. [4] kohta 3.11 ja standardi EN 60601-1-4, kohdat 6.8 ja 52.203.6).

Virhelistojen julkistaminen käyttäjille voi olla mahdotonta, mikäli sitä pyytää vain yksi käyttäjä. Tässä tapauksessa käyttäjät voisivat tiivistää yhteistyötä ja laatia suosituksen, jota noudatettaisiin kaikissa hankinnoissa. Yhtenä kohtana suosituksessa voisi olla virhelistojen julkistaminen. Ajatusta voisi kehitellä ja siitä olisi syytä keskustella yhdessä käyttäjien, valmistajien ja maahantuojien kesken.

Liitteessä D on kuvattu kohteita, joita käyttäjän suorittamassa testauksessa voidaan tarkastaa. Testeissä on erittäin tärkeää määritellä testidata, jolla testaus suoritetaan. Testidatan on vastattava järjestelmän käyttämää tuotantodataa. Ohjelmistotestauksessa on tärkeää huomioida myös ääripäiden testaus. Testitapausten tulee siis sisältää testit myös ensimmäiselle tietueelle, viimeiselle tietueelle, minimikuormitukselle, sekä tilanteille, joissa kaikki tiedostot suljettuna sekä kaikki tiedostot avoinna (määriteltävä avoimien tiedostojen tai tietokantojen maksimimäärä) ja kaikki käyttäjät kirjautuneina järjestelmään (määriteltävä maksimikäyttäjämäärä) maksimikäyttäjillä. Testien tulee kattaa kaikki normaalikäytön aikana suoritettavat toiminnot (esimerkiksi alusta, etsi, lisää, korvaa, poista ja muuta). Testien aikana monitoroidaan prosessorin ja käyttöjärjestelmäprosessien kuormitusta ja käyttäytymistä ja tulokset kirjataan testauspöytäkirjoihin.

Muutosten ja päivitysten testaus suoritetaan omassa ympäristössään erotettuna tuotantoympäristöstä. Testauksen valmistelussa tulee muistaa, että sovellus voi osoittaa tiettyyn polkumäärittelyyn tai tietokannat on määritelty ns. alias-nimillä. Vaikka testausta varten otetaan kopiot tietokannoista sekä sovelluksesta ja siirretään ne omaan testiympäristöön, voi sovellus edelleen käyttää todellista tuotantotietokantaa (kuva 18). Tässä tapauksessa testaus voi aiheuttaa häiriöitä tuotantojärjestelmässä tai se voi peräti tuhota tai muuttaa tuotantojärjestelmän tietoja.



***Kuva 18**. Testattava kohde erotetaan tuotantoympäristöstä*

Testauksen valmistelussa on huomioitava sen suunnitelmallisuus ja suunnitelmien noudattamien sekä mahdolliset vaikutukset järjestelmien kuntoon. Laitetta rikkovat testit jäävät testisuunnitelmien ulkopuolelle tai niistä on sovittava etukäteen laitetoimittajan kanssa. Mikäli haluaa lisätietoa testauksesta, niin kannattaa tutustua Edward Kitin kirjoittamaan kirjaan nimeltä 'Software Testing in the real world, improving the process' (ISBN:0-201-87756-2). Kirjassa on selitetty erittäin hyvin ohjelmiston testauksen perusteita ja mahdollisuuksia. Lisäksi kirjassa on valmiita tarkistuslistoja, joita voidaan soveltaa omaan käyttöön.

Muista, että hyvä testaus perustuu aina suunnitelmallisuuteen. Ilman suunnitelmaa et tiedä mitä ja miten pitää testata, kuka tekee ja mitkä ovat hyväksyntäkriteerit. Testauksen hyväksyntäkriteereitä ei voida laatia ilman järjestelmävaatimuksia.

6.6 Ylläpito ja määräaikaishuollot

Laitteiden ja laitejärjestelmien luotettavan toiminnan kannalta merkittävässä asemassa ovat säännöllisin välein suoritettu kunnonvalvonta tai määräaikaishuollot. Huollot ja tarkastukset tulee tehdä aina hankintaprosessin tai vastaanottotarkastuksen yhteydessä laaditun suunnitelman mukaisesti. Tarkastusten tulee kattaa laitteen toiminnan ja käytön kannalta tärkeät huollot, kalibroinnit ja määräaikaishuollot, joilla varmistetaan laitejärjestelmän suorituskyky, sähköturvallisuus ja muu turvallisuus sekä jossain määrin myös käytettävyys. Tarkastuksista ja tehdyistä mittauksista tulee laatia pöytäkirja, joka talletetaan laitteen huoltotietoihin. Liitteessä E on kuvattu esimerkkejä määräaikaishuollossa tarkastettavista kohteista.

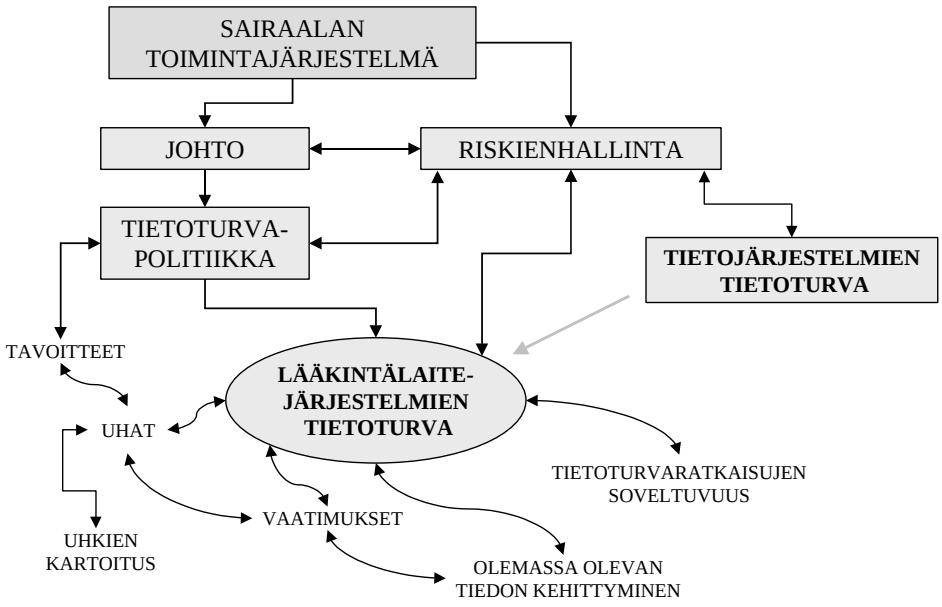
7. TIETOTURVA

7.1 Laitejärjestelmän tietoturva

Lääkintälaitejärjestelmän tietoturva merkitsee potilaaseen liittyvien tietojen suojaamista väärältä käyttötarkoitukselta sekä tiedon saatavuuden ja oikeellisuuden varmistamista. Laajemmin ajateltuna tietoturva ei saa vaarantaa niitä toimintoja ja tarkoituksia, joilla järjestelmän on aiottu toimivan. Tietoturvallisuusjärjestelyiden ensisijaisena tavoitteena on standardin BS 7799-1 mukaan suojata tiedon:

- luottamuksellisuus: tietoa pääsevät käsittelemään vain ne, joilla on siihen käyttöoikeus
- eheys: tieto ja sen käsittelytavat ovat täydellisiä ja virheettömiä
- käytettävyys: tieto ja sen käsittelytavat ovat aina tarvittaessa valtuutettujen käyttäjien saatavilla.

Jotta yllämainitut tavoitteet voidaan saavuttaa on organisaation ennen tietoturvapolitiikkansa julistamista tehtävä riskianalyysi käyttämistään ja tarvitsemistaan järjestelmistä sekä niiden käyttäjistä. Riskianalyysin on katettava kaikki organisaation käytössä olevat tietoturvaan välittömästi tai välillisesti vaikuttavat toiminnot tai järjestelmät mukaan lukien lääkintälaitejärjestelmät (kuva 19).



***Kuva 19**. Riskienhallinnan ja analyysien on katettava myös tietoturva*

Analyysin tuloksena määritellään organisaation tietojärjestelmille ja laitejärjestelmille soveltuvat tietoturvaratkaisut. Tietoturvaratkaisuissa huomioidaan myös tietojärjestelmien ja laitejärjestelmien välinen rajapinta. Laitejärjestelmien tietoturva on osa organisaation riskienhallintaa ja sen ylläpito edellyttää jatkuvaa tietoturvatapahtumien seurantaa. Tietoturvan tehokas toteutus edellyttää käyttäjäorganisaation ja toimittajan välistä yhteistyötä, joka kattaa järjestelmän koko käyttöiän.

7.2 Taustaa tietoturvavaatimuksille

Terveydenhuollon organisaatioiden toiminta on vankasti erilaisten tietojärjestelmien varassa. Tietojärjestelmät sisältävät esimerkiksi ajanvarauksen, hoidonvarauksen, maksuliikenteen, hoitokertomukseen ja digitaalisten kuva-arkistojen hallintaan liittyviä ohjelmistoja. Tavoitteena on ohjelmistojen avulla toteuttaa laadukasta ja kustannustehokasta toimintaa. Sairaaloiden käytössä on jo leikkaussaleissa tai teho-osastoilla lääkintälaitejärjestelmiä, joihin on kytketyillä tietokoneilla tai ns. Web-Pad-laitteilla hoidon aikana esiintyneitä tapahtumia tai hoitosuunnitelmia syötetään sairaalan muihin tietojärjestelmiin.

Laitejärjestelmien tietoturva poikkeaa esimerkiksi terveydenhuollon muista tietojärjestelmistä siten, että potilaaseen kytketyille laitteille tai laitejärjestelmille on asetettu säädöksissä ja harmonisoiduissa standardeissa tiukkoja turvallisuus-, suorituskyky- ja luotettavuusvaatimuksia. Vaatimusten toteutumista valvovat toimivaltaiset viranomaiset.

Terveydenhuollon toimintayksiköiden tietojärjestelmille asetetaan tietoturvavaatimuksia henkilörekisterilaissa sekä standardeissa BS 7799-1 ja BS 7799-2. Laitejärjestelmille vaatimuksia asetetaan terveydenhuollon laitteita koskevissa säädöksissä sekä EN 60601-standardisarjassa , jotka välillisesti kattavat myös tietoturvan. Ongelmana on se, että lääkintälaitteille asetetut vaatimukset eivät suoranaisesti sisällä sanaa 'tietoturva' ja useat valmistajat eivät täten suunnittelussaan huomioi riittävästi laitejärjestelmien tietoturvaan vaikuttavia tekijöitä.

Standardi EN 60601-1-4 sisältää ainakin kolme kohtaa (standardin kohta suluissa), joiden katsotaan kattavan myös tietoturvan[1]:

- Vaara-analyysissä on tunnistettava [tietoturvan puutteellisuudesta johtuvat] vaarat, kun vaaran syyt ovat inhimillisiä ja tahallisia tai tahattomia (52.204.3.1.6).

[1] Hakasulkeet ovat kirjoittajien lisäämiä [1]. Kirjoittajien mielestä vaatimuksien katsotaan implisiittisesti tarkoittavan myös tietoturvaa.

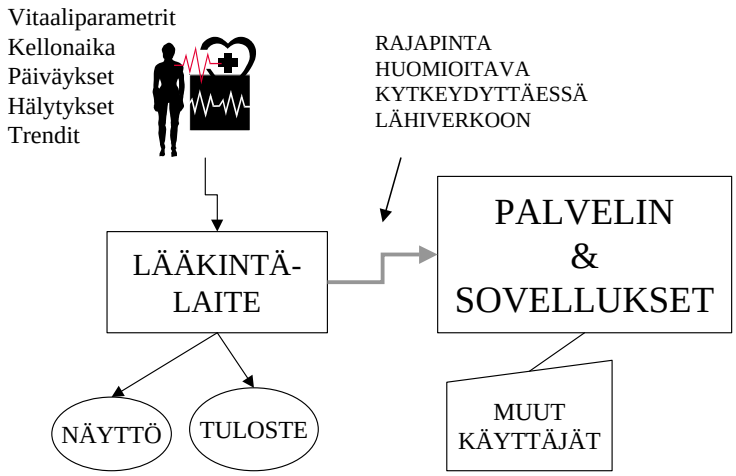
- Vaatimusmäärittelyn tulee eritellä toiminnot, joihin liittyy riski, ja riskejä valvovat toiminnot. Virhetoiminnon vaikutus [tietoturvaan] on tunnistettava. (52.206.2).
- Arkkitehtuurin vaatimusmäärittelyn on sisällettävä suojautumiskeinot inhimillisiltä ja tahattomilta syiltä [, jotka uhkaavat tietoturvaa] (52.207.3).

Kytkettäessä järjestelmiä yhteen on rajapinnan tai itse lääkintälaitejärjestelmän täytettävä asetetut vaatimukset. Näin ollen tehdyn riskianalyysin on katettava myös tietoturvaominaisuudet ja rajapinnan ominaisuudet. Tämä on tärkeää huomioida määrittelyvaiheessa. Tietoturvan toteutus eri järjestelmissä voidaan useinkin toteuttaa normaaleilla IT-järjestelmien tietoturvaratkaisuilla. Lääkintälaitejärjestelmissä edellytetään kuitenkin osoitusta käytettyjen menetelmien tehokkuudesta ja toimivuudesta. Tämä aiheuttaa hieman laajempaa arviointia käytettyjen ratkaisujen soveltuvuudesta. Lisäksi toteutettujen ratkaisujen dokumentointi on tehtävä huolella.

Perinteisesti yksittäinen lääkintälaite antaa äänihälytyksen, näytöllä näkyvän käyrän ja tarvittaessa paperitulosteen. Tällaisen toiminnan tietoturvavaatimukset on melko helposti hoidettu henkilökunnan vaitiolovelvollisuudella ja asiakirjojen asiallisella säilytyksellä. Prosessori- ja ohjelmistopohjaisten lääkintälaitteiden keräämää tietoa on haluttu siirtää osaksi terveydenhuollon organisaation muita tietojärjestelmiä. Tästä seuraa väistämättä lääkintälaitteiden verkottamistarve muihin tietojärjestelmiin, joko langallisia tai langattomia verkkoja hyväksikäyttäen.

Kytkettäessä lääkintälaite verkkoon altistetaan sen toiminta useille erilaisille riskeille (kuva 20). Verkkoon kytketyssä lääkintälaitteessa on huomioitava lisäksi muut tietoturvavaatimukset (tiedon luottamuksellisuus, eheys, käytettävyys), joten lääkintälaitejärjestelmien nykyiset tietoturvavaatimukset joko laajenevat tai muuttuvat oleellisesti.

Lääkintälaitteiden tai lääkintälaitejärjestelmien tietoturvavaatimukset ja ratkaisut tulisi määritellä osana koko organisaation tietojärjestelmiä koskevia tietoturvaratkaisuja ja toteutuksen tulisi olla yhteensopivia myös olemassa olevien ratkaisujen kanssa. Määrittelyssä tulee aina ottaa huomioon käyttäjän ja järjestelmän valmistajan tarpeet ja vaatimukset. Määrittelyissä on tärkeää tuntea sovellusalue, tietoverkon käytön tarve ja mahdolliset lääkintälaitejärjestelmien etähuoltoreitit, jotka mahdollistavat pääsyn tietoverkkoon ns. takaoven kautta.



***Kuva 20**. Lääkintälaitteen liittyessä verkkoon sen tietoturvavaatimukset muuttuvat*

Ratkaisujen onnistuminen edellyttää tiivistä yhteistyötä tietojärjestelmävastaavien, lääkintälaitejärjestelmien valmistajan ja toimittajan, käyttöhenkilökunnan sekä huoltohenkilökunnan välillä. Tiiviillä yhteistyöllä saadaan tietoturvaratkaisut kohdennettua kriittisiin ja käytön kannalta merkittäviin kohtiin.

7.3 Hallinnollinen tietoturva

Tietoturvapolitiikka on organisaation julistus, jolla se suojelee omistamaansa eri muodoissa olevaa tietoa. Hallinnolliseen tietoturvaan liittyy keskeisenä osana johdon sitoutuminen julistamansa tietoturvapolitiikan noudattamiseen. Hallinnollisen tietoturvan tulee määritellä organisaation tietoturvapolitiikka. Sen tulee kattaa tietoturvan tavoitteet, johdon sitoutumisen, ohjeistukset ja vastuut. Standardissa BS 7799-1 määritellään tietoturvallisuuspolitiikan edellyttämät asiat. Tietoturvapolitiikkaan vaikuttavat organisatoriset, ulkoiset ja teknologiasta johtuvat tekijät (kuva 21). Hallinnollisen tietoturvan on otettava kantaa näihin tekijöihin.

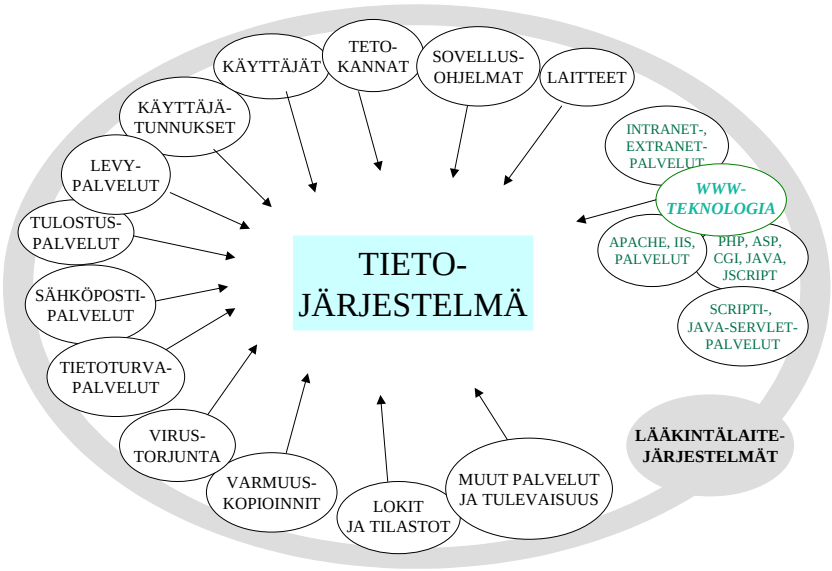
Hallinnollisen tietoturvan on määriteltävä erityisesti sellaiset seikat, joilla voi olla turvallisuutta alentavia tai muita haitallisia vaikutuksia organisaation toimintaan, kuten:

- elektroniset sopimukset (pelisäännöt, toteutus, salassapito)
- sähköisen materiaalin käyttö (omistusoikeus epäselvä, luottamuksellisuus, saatavuus)
- henkilörekisterilain tai muiden viranomaisvaatimusten noudattamatta jättäminen (esim. lääkintälaitejärjestelmissä)

- tietojen vuotaminen ei-sallituille käyttäjille (esim. hakkerointi tai inhimilliset seikat)
- tietojen salaamattomuus (esim. lääkintälaitejärjestelmissä)
- sähköisen tunnistuksen tai salauksen puute (esim. lääkintälaitejärjestelmissä tai verkkoon kytketyissä kotihoidon laitteissa).

***Kuva 21**. Tietoturvaan vaikuttavat tekijät*

Standardin BS 7799-1 mukaan kunkin organisaation on kartoitettava ja analysoitava käytössään olevat ohjelmistot. Kuvassa 22 on esimerkki joistakin tietojärjestelmien ohjelmakomponenteista. Standardin mukaan jokaisen ohjelmiston turvallisuusvaikutus tulisi analysoida. Analyysin jälkeen voidaan laatia tarvittavat ohjeistukset tietojärjestelmien käytölle, huollolle ja koulutukselle sekä toteuttaa käytännön ratkaisut. Analyysi on uusittava aina isoissa muutostilanteissa tai päivitettävä otettaessa käyttöön uusia ohjelmistoja, tekniikoita tai laitteistoja.



***Kuva 22**. Tietoturvan on katettava kaikki käytössä olevat ohjelmistot*

Hallinnollisen tietoturvan (organisaation johto) vastuulle kuuluu huolehtia siitä, että tietoturvan eri osa-alueista laaditaan riittävän selkeät ja kattavat menetelmäohjeet. Taulukossa 4 on esimerkki ohjeiden laadinnasta ja ohjeen sisällöstä. Esimerkki ei ole läheskään kaiken kattava, mutta luultavasti se kuitenkin on tarpeeksi laaja kuvaamaan sitä ohjeistuksen laajuutta, jota tietojärjestelmien oikea ja turvallinen käyttö edellyttää.
Vaikka tietoturvan tärkeä elementti on teknologia, jolla tietoturvaa ylläpidetään, toteutetaan ja käytetään, niin koulutuksen tarpeellisuutta tai inhimillisten tekijöiden merkitystä ei voi unohtaa tai väheksyä. Erään tutkimuksen mukaan tietoturvaongelmista 55 % aiheutuu itse käyttäjistä (lähde: Computer Security Institute).

Hallinnollinen tietoturva on organisaation yksi tärkeimmistä peruspilareista. Mikäli sitä ei määritellä ja johto ei seuraa sen noudattamista, on yksilötasolla hyvin rajalliset mahdollisuudet tietoturvan ylläpitoon. Hallinnollisen tietoturvan avaintehtäviä on määritellä organisaation tietoturva, kattaen ainakin pelisäännöt ja tavoitteet tietoturvalle, käytetyt tekniikat, sallitut tekniikat ja riskienhallinnan menetelmät sekä taata riittävät resurssit tietoturvan toteuttamiseksi.

Taulukko 4. Esimerkki tietoturvaan liittyvästä ohjeistuksesta

OHJE	TARKOITUS	LAATIJA	VASTUUHENKILÖ ja VERSIONUMERO
Käytössä oleva tieto	Minkälaista tietoa organisaatiolla on käytössä, mihin tietoa käytetään, mikä tiedosta on julkista, luottamuksellista, salaista tai erittäin salaista tietoa.	Johto + muut asiaankuuluvat tahot	Henkilö N.N Ver.01 pp.kk.vuosi
Käyttäjät	Määritellään kuka voi lukea, luoda, muuttaa tai poistaa tietoa, kuka vastaa tietoturvasta jne..	Johto, System manager	Henkilö N.N Ver.01 pp.kk.vuosi
Käyttäjätunnukset	Määrittelee ja luokittelee käyttäjätunnukset ohjeen 'käyttäjät' perusteella	Johto, System manager	Henkilö N.N Ver.01 pp.kk.vuosi
Selaimet	Määrittelee organisaatio käytössä olevat selaimet ja niiden tietoturva asetukset.	Johto, System Manager, Tietoturvasta vastaava	Henkilö N.N Ver.01 pp.kk.vuosi
Tietoverkko	Määrittelee tietoverkon, verkon turvallisuuden, mahdolliset intrat ja extrat, sekä palomuuriratkaisut ja portit joista voidaan kytkeytyä	Johto, System Manager, Tietoturvasta vastaava, Tietoverkosta vastaava	Henkilö N.N Ver.01 pp.kk.vuosi
Sähköposti	Määrittelee sähköpostiohjelmat ja niiden tietoturva-asetukset sekä ohjeistus tiedostojen lähetykselle, avaukselle ja tuntemattomien lähettäjien sähköpostin käsittelylle	Johto, System Manager, Tietoturvasta vastaava	Henkilö N.N Ver.01 pp.kk.vuosi
Tietokannat	Määrittelee organisaation käyttämät tietokannat ja tietokantojen hallintajärjestelmät sekä niitä käyttävät sovellukset	Johto, System Manager, Järjestelmä asiantuntija, Tietoturvasta vastaava	Henkilö N.N Ver.01 pp.kk.vuosi
Virus-torjunta	Määrittelee organisaation käyttämät virustorjunta välineet ja tavoitteet virustorjunnalle, mitä kaikki suojataan, määrittelee tietokoneen käynnistykset ja levykkeiden käytöt jne..	Johto, System Manager, Sovellusasiantuntija Tietoturvasta vastaava Virusohjelmistojen toimittaja	Henkilö N.N Ver.01 pp.kk.vuosi
Tulostus	Määrittelee verkkotulostus palvelut, määrittelee arkaluonteisten tulosteiden mahdolliset tulostuspalvelut	System Manager, Sovellusasiantuntija Tietoturvasta vastaava	Henkilö N.N Ver.01 pp.kk.vuosi
Sovellusohjelmat	Mitä kaikkia ohjelmistoja organisaatio käyttää, sisältää myös lisenssisopimusten määrittelyn	Johto, System Manager, Tietoturvasta vastaava	Henkilö N.N Ver.01 pp.kk.vuosi
Tietoturvapalvelut	Määrittelee palomuurit, salaustekniikat, www-palvelimien portti-	Johto, System Manager, Sovellusasiantuntija Tieto-	Henkilö N.N

	määritykset jne..	turvasta vastaava	Ver.01 pp.kk.vuosi
Tietoturva-koulutus	Määrittelee mitä kukakin saa tehdä, minkälaista koulutusta kukin saa/tarvitsee ja esittelee yrityksen tietoturvapolitiikan	Johto, System Manager, Sovellusasiantuntija Tietoturvasta vastaava, Henkilöstön edustaja	Henkilö N.N Ver.01 pp.kk.vuosi
Lääkintälaitejärjestelmät	Määrittelee organisaation käytössä olevat lääkintälaitejärjestelmät, niiden kytkeytymisen tietojärjestelmiin, niille sovellettavat tietoturvavaatimukset sekä hankinta-ohjeistuksen. Määrittelee myös suoritettavat ohjelmistopäivitykset	Johto, System Manager, Sovellusasiantuntija Tietoturvasta vastaava, Hoitohenkilökunta, huollosta vastaavat, järjestelmätoimittaja Jne..	Henkilö N.N Ver.01 pp.kk.vuosi
Uusien laitteiden hankinta ja poisto (voi olla järkevää tehdä kaksi erillistä ohjetta)	Määrittelee uusien laitteiden hankinnan, suoristuskyvyn, laitekokoonpanon, mitä on asennettu valmiiksi ja mitä asennetaan yrityksen omasta toimesta Määrittelee laitteistojen poistojen ja tietojen hävityksen [korput, lerput, romput, nauhat, zippilevyt, winsut]	Johto, System Manager, Sovellusasiantuntija Tietoturvasta vastaava, Jne..	Henkilö N.N Ver.01 pp.kk.vuosi

7.4 Tekninen tietoturva

Tekninen tietoturva toteutetaan organisaation tietoturvapolitiikan mukaisesti siihen määrätyillä resursseilla ja välineillä. Tietoturvaan liittyvät toimenpiteet ja suojauskeinot kohdistetaan tietoturvapolitiikassa määriteltyihin kohteisiin ja ohjelmistoihin.

Tietoturvan ylläpito edellyttää jatkuvaa raportoitujen tietoturvaongelmien seurantaa. Organisaatiossa käytössä olevat ohjelmat tulee kartoittaa. Näiden ohjelmien tietoturvakehitystä tulee aktiivisesti seurata ohjelmistovalmistajien kotisivuilta ja erilaisista uutisryhmistä. Tiedot merkittävistä muutoksista tai tapahtumista tulee toimittaa hallinnollisesta tietoturvasta vastaaville henkilöille.

Tekninen tietoturva voidaan jakaa useampaan eri osa-alueeseen, jossa toiminnalliseen tietoturvaan sisältyy teknologia, ohjelmistot sekä niiden käyttö ja fyysiseen tietoturvaan taas sisältyy perinteisesti tilat, laitteistot, lukitukset ja kulunvalvonta sekä mahdolliselta ilkivallalta suojautuminen. Liitteessä C on kuvattu tietoturvaan liittyviä seikkoja. Liitteen

sisältö voidaan muuttaa tarvittaessa tarkastuslistan muotoon, jolloin sitä voidaan käyttää normaalin toiminnan tukena.

Mikäli organisaation laatima tietoturvapolitiikka ja tätä kautta asetetut tavoitteet ovat epäselviä, ei käytännön tietoturva voi toimivuudeltaan, tehokkuudeltaan ja käytettävyydeltään olla paras mahdollinen.

Useissa käyttöorganisaatioissa on kustannussyistä tietojärjestelmien ylläpito ja tätä kautta myös tietoturvaratkaisut annettu organisaation ulkopuolisille tahoille hoidettavaksi. Ulkoistamisesta on laadittava osapuolten kesken sopimus, jossa standardin BS 7799-1 mukaan tulee määritellä säädösten vaatimukset, vastuujako, suojausmenetelmät tiedon eheyden ja luottamuksellisuuden varmistamiseksi, fyysiset ja loogiset turvamekanismit, palvelujen saatavuuden ylläpito, turvallisuuden taso ja tarkastusoikeudet.

7.5 Miten hallitsen tietoturvan?

Laaditun tietoturvapolitiikan ja toteutetun tietoturvaratkaisun tulee perustua riskianalyysin avulla saatuihin tuloksiin ja päätöksiin. Analyysi on uusittava tietyin väliajoin, koska tietoturvaan liittyvät ongelmat, vaatimukset ja ratkaisut muuttuvat koko ajan. Vaiheistus tietoturvaongelmien selvittämiseksi ja ratkaisemiseksi kulkee pääpiirteissään seuraavasti:

- Kartoita käytössä olevat tietojärjestelmät ja selvitä lainsäädäntö.
- Tutki käytössä olevan teknologian soveltuvuus tämän päivän ja tulevaisuuden tarpeisiin.
- Tee riskianalyysi, aseta tavoitteet ja korjaa ongelmat.
- Laadi tietoturvapolitiikka.
- Toteuta hallinnollinen tietoturva.
- Tee se käytännössä eli toteuta tekninen tietoturva.
- Seuraa kehitystä.

Määrittele organisaatiolle tietoturvapolitiikka, aseta tavoitteet, määrittele resurssit, seuraa tietoturvakehitystä, pidä lokeja, raportoi, tee tarvittaessa muutoksia, hyväksytä muutokset, testaa ja toteuta ne ja uusi tarvittaessa riskianalyysi Tietoturvaan ei ole tänä päivänä vielä löydetty täydellistä ratkaisua; yritä siis tulla toimeen tämän tosiasian kanssa. Hyvä tietoturvaratkaisu on kompromissi, jolla toimintatapojen, käytettävyyden, teknologian ja kustannustekijöiden yhteisvaikutuksella ratkotaan toiminnan kannalta pahimmat tai kriittisimmät ongelmat ja puutteet. Laadittaessa organisaation tietoturva-asioita kannattaa tutustua

valtiovarainministeriön julkaisemiin tietoturvallisuusohjeisiin (taulukko 5). Tietoturvallista matkaa tiedon valtatiellä.

Taulukko 5. Valtionvarainministeriön julkaisemia tietototurvallisuusohjeita

Tietoturvallisuus ja tulosohjaus	VAHTI 2/2004
Valtionhallinnon tietoturvallisuuden kehitysohjelma 2004-2006	VAHTI 1/2004
Ohje riskien arvioinnista tietoturvallisuuden edistämiseksi valtionhallinnossa	VAHTI 7/2003
Opas julkishallinnon tietoturvakoulutuksen järjestämisestä	VAHTI 6/2003
Käyttäjän tietoturvaohje	VAHTI 5/2003
Valtionhallinnon tietoturvakäsitteistö	VAHTI 4/2003
Tietoturvallisuuden hallintajärjestelmän arviointisuositus	VAHTI 3/2003
Turvallinen etäkäyttö turvattomista verkoista	VAHTI 2/2003
Valtion tietohallinnon Internet-tietoturvallisuusohje	VAHTI 1/2003
Arkaluonteiset kansainväliset tietoaineistot	VAHTI 4/2002
Valtionhallinnon etätyön tietoturvallisuusohje	VAHTI 3/2002
Tietoteknisten laitetilojen turvallisuussuositus	VAHTI 1/2002
Toimet tietoturvaloukkaustilanteissa	VAHTI 7/2001
Valtion tietotekniikkahankintojen tietoturvallisuuden tarkistuslista	VAHTI 6/2001
Valtionhallinnon sähköpostien ja lokitietojen käsittelyohje	VAHTI 5/2001
Sähköisten palveluiden ja asioinnin tietoturvallisuuden yleisohje	VAHTI 4/2001
Salauskäytäntöjä koskeva valtionhallinnon tietoturvallisuussuositus	VAHTI 3/2001
Valtionhallinnon lähiverkkojen tietoturvallisuussuositus	VAHTI 2/2001
Valtion viranomaisen tietoturvallisuustyön yleisohje	VAHTI 1/2001
Tietokoneviruksilta ja muilta haittaohjelmilta suojautumisen yleisohje	VAHTI 4/2000
Valtionhallinnon tietojärjestelmäkehityksen tietoturvallisuussuositus	VAHTI 3/2000
Valtionhallinnon tietoaineistojen käsittelyn tietoturvallisuusohje	VAHTI 2/2000
Tietojärjestelmäselosteen laadintasuositus	VM 17.2.2000
Salassa pidettävien tietojen ja asiakirjojen turvaluokittelu- ja merkintäohje	VM 19.1.2000
Valtion tietohallintotoimintojen ulkoistamisen tietoturvallisuussuositus	VAHTI 2/1999
Tietoturvallisuuden tulosohjaus ja kehittämisvälineet	VAHTI 2/1997
Valtiovarainministeriö (VM) ohjaa ja yhteen sovittaa valtionhallinnon tietoturvallisuutta ja sen kehittämistä. Ohjeita kehittää valtionhallinnon tietoturvallisuuden johtoryhmä (VAHTI), joka on VM:n asettama, tietoturvallisuuden asiantuntemusta laajapohjaisesti edustava ryhmä	

8. TEKNOLOGIAKURKISTUS

Terveydenhuolto on jatkuvan muutoksen ja uudelleenorganisoinnin kohteena. Valitettavan usein muutoksissa pyritään hakemaan kustannustehokkuutta erilaisilla säästöillä tai supistamalla toimintaa. Pitkällä aikavälillä ainoastaan näillä keinoilla on todennäköisesti vaikeaa parantaa toiminnan laatua ja samalla pyrkiä vastaamaan tulevaisuuden yhä koveneviin haasteisiin.

Osa muutoksista johtuu myös hoitoprosessien ja toimintojen systematisoinnista ja olemassa olevan tiedon paremmasta hyödyntämisestä. Yritykset parantaa hoidon vaikuttavuutta ja toisaalta vähentää paperien käyttöä sairaalassa on johtanut laitteiden suorituskyvyn kasvamiseen, digitalisoimiseen ja digitaalisten arkistointijärjestelmien lisääntyneeseen käyttöön. Muutosten syyt eivät välttämättä aina ole selviä. Joskus tuntuu ainakin siltä, että käyttäjien tarpeita yritetään muokata uudella teknologialla. Tässä luvussa on kuvattu kohteita, joissa teknologiamuutoksiin on syytä varautua.

8.1 Kotihoidon laitteet

Perinteisten kotihoidon laitteiden (respiraattorit, imulaitteet, dialyysilaitteet, pyörätuolit ja muut apulaitteet) saavat rinnalleen tietokonepohjaisia laitteita, kuten kuvapuhelimia, verensokerimittareita tai muita vitaaliparametrien monitorointilaitteita. Näissä uusissa sovelluksissa laitteen pääasiallisen toiminnon suorittaa ohjelmisto, joka välittää tiedot reaaliajassa joko valvontakeskukselle tai sairaalan tietojärjestelmiin.

Näissä sovelluksissa tulee luotettavuus- ja käytettävyysvaatimuksien lisäksi ottaa huomioon tietoturvavaatimukset. Keskeisiä kysymyksiä onkin, että tarvitaanko sovelluksissa salausta, sähköistä tunnistusta, biometriikkaan perustuvaa tunnistusta tai suljettuja tietoverkkoyhteyksiä (VPN).

Kotihoidon laitteiden yhteydessä täytyy muistaa myös perinteisten laitteiden erityisvaatimukset. Usein hoitoalueella käytettäväksi tarkoitettuja laitteita käytetään kotona, jossa tilojen sähköasennukset yleensä poikkeavat sairaaloiden sähköasennuksista. Tällöin on tärkeää määritellä muutostyöt, joilla laitteet soveltuvat käytettäväksi kotona.

Tärkeää on myös riittävä käyttökoulutus. Käyttökoulutuksen on katettava kaikki oikean käytön ja huollon kannalta tärkeät seikat. Käyttökoulutuksessa on huolehdittava siitä, että kaikille hoitoon osallistuville annetaan riittävästi koulutusta. Koulutuksessa ja mukana seuraavissa dokumenteissa on määriteltävä myös yhteystiedot, joista mahdollisissa ongelmatapauksissa voidaan pyytää apua.

8.2 Mobiilitekniikka

Mobiilitekniikan tulo lääkintälaitejärjestelmiin erilaisten kommunikaattoreiden, tasku- ja käsitietureiden muodossa lisääntyy. Tekniikka mahdollistaa esim. liikkuvan hoitokertomuksen tai potilaan reaaliaikaisen monitoroinnin. Mahdollisuudet tuntuvat rajattomilta tässä suhteessa.

Teknologian soveltuvuus terveydenhuollon sovelluksille asetettuihin vaatimuksiin on pohdittava huolella. Käynnissä on useita erilaisia pilottihankkeita. Keskeisiä vaatimuksia teknologian soveltuvuudelle ovat luotettavuus, suorituskyky, tietoturvavaatimukset (tietosuoja, tiedon luottamuksellisuus, henkilörekisterilaki) sekä liikuteltavuudesta johtuvat mekaaniset vaatimukset.

8.3 Inhimilliset tekijät mukaan määrittelyyn

Teknologian ja laitteistojen monimutkaistuessa inhimilliset tekijät ja käytettävyys on keskeinen osa suunnittelun lähtötiedoista. Vaikka inhimilliset tekijät ja käytettävyys ovatkin vaikeita ominaisuuksia mitata on nämä asiat ainakin riskienhallinnan kautta liitettävä osaksi suunnittelua. Myös terveydenhuollon toimintayksiköiden tulisi tiedostaa nämä vaatimukset osana hankinta-, huolto- tai hoitoprosessia.

Inhimillisille tekijöille on valmisteilla standardi EN 60601-1-6, jonka kehittymistä on terveydenhuollon yksiköidenkin syytä seurata. Standardin vaatimuksia voidaan soveltuvin osin lisätä hankintaprosessiin.

8.4 Hajauttaminen

Ohjelmistosovellusten monimutkaistuessa ja sovellusten suorituskykyvaatimusten kasvaessa voidaan HTTP-protokollan ja CORBA-standardien mukaisilla sovelluksilla jakaa kuormitusta useammalle eri palvelimelle. Käyttäjälle ei välttämättä näy mistä tietoa milloinkin haetaan tai minne sitä viedään. Tällöin ylläpito voi helpottua, kun yksi palvelin hoitaa tietyn osakokonaisuuden, toisaalta se myös monimutkaistaa

helposti ylläpitoa. Näissä tapauksissa määrittely ja testaus on tärkeää. Pelisäännöt on oltava selvillä. Myös tietoturvavaatimuksien uudelleen arviointi ja mahdolliset alihankinta- ja ylläpitosopimukset on pohdittava uudestaan.

8.5 Etähuollot ja -päivitykset

Valmistajan näkökulmasta ylläpitoa, muutoksia ja asennuksia pyritään siirtämään enenevässä määrin tietoverkkojen kautta tapahtuvaksi toiminnoksi. Myös osa terveydenhuollon sovelluksien käyttöliittymistä pohjautuu jo tänä päivänä www-selaimien ja www-palvelimien hyväksikäytölle.

Käyttäjän kannalta tällainen esimerkiksi internetin kautta tapahtuva huolto helpottaa ja nopeuttaa mahdollisesti asennuksien ja muutoksien tekemistä. Vastaavasti se edellyttää käyttäjää laatimaan oman tietoturvapolitiikkansa tällaisen mahdollisuuden toteuttamiseksi.

Lisäksi on syytä laatia tarkat pelisäännöt valmistajan, maahantuojan ja käyttäjän kesken siitä, että kenen on vastuu, jos käyttäjä asentaa uusia softa-ajureita internetin kautta vaikka keskusvalvontamonitorin valvontaohjelmistoon ja jokin meneekin pieleen.

8.6 Uudet sovellusalustat

Avoimeen lähdekoodiin perustuvat sovellukset voivat tuoda uusia mahdollisuuksia terveydenhuollon sovelluksissa. Tässä vaiheessa eniten palstatilaa saanut Linux perustuu avoimeen lähdekoodiin ja voi tarjota terveydenhuollon sovellusten alustaksi mielenkiintoisen ja varteenotettavan vaihtoehdon. Ennen Linuxiin siirtymistä on syytä käynnistää pilottihanke, jossa ennakkoluulottomasti testataan sovellusten ja alustan soveltuvuutta ja vakautta aiotussa käyttötarkoituksessa.

Linuxiin siirtymisessä on kartoitettava hyvin tarkkaan nykyisten sovellusten määrä, tarve, käyttö, tietokannat, tietoturvaratkaisut ja käyttäjämäärät sekä olemassa olevan tiedon ja käyttäjien luokittelu. Tärkeää on selvittää myös tietojärjestelmien rajapinnat erityisesti ulkoisten tietojärjestelmien osalta. Tämän jälkeen on selvittävä vielä, että löydetäänkö vastaavia sovelluksia myös Linux-ympäristöstä tai saadaanko rajapinta määriteltyä siten, että sovellukset voivat keskustella keskenään erilaisista alustoista huolimatta. Linuxin soveltuvuudesta on tehty jo joitain selvityksiä ('Loppuraportti OpenOffice -työasemaohjelmiston ja Linux-

käyttöjärjestelmän soveltuvuudesta Turun kaupungin työasemastandardiksi'[2])

Linux-käyttöjärjestelmän etuja ovat:

- pienemmät välittömät kustannukset,
- paljon käytössä hyväksi havaittuja ilmaisohjelmia (tietokanta-ajureita, kääntäjiä, grafiikkaohjelmia jne.),
- avoin lähdekoodi mahdollistaa 'periaatteessa' paremman osoitettavuuden, luotettavuuden ja vaatimustenmukaisuuden osalta (edellyttää arvioijilta hyvää osaamista),
- tarjoaa vakaan alustan www-palvelimille,
- vähemmän viruksia (tosin Linux-ympäristössäkin on jo löydetty viruksia),
- korjauspäivitykset nopeasti saatavissa.

Linux-käyttöjärjestelmän haittoja ovat:

- edellyttää enemmän koulutusta alkuvaiheessa,
- alkuvaiheen ylläpito voi olla tiedon puutteesta johtuen hankalaa,
- ohjelmistotarjonta vähäisempää,
- tietojen yhteensopivuus Windows-maailman kanssa aiheuttaa ongelmia.

Päätöksenteko siirtymisestä uuteen sovellusalustaan on jokaisen organisaation oma asia. Päätöksenteossa on kuitenkin otettava huomioon sovelluksen kriittisyys, sitoumukset ulkopuolisten tahojen kanssa, yhteensopivuus, muunneltavuus ja kustannustekijät.

8.7 Ohjelmistoarkkitehtuurit

Ohjelmistoarkkitehtuurit ja ohjelmointitekniikat kehittyvät huimaa vauhtia. Tämän hetken kuuma uutuus on Microsoftin .NET-arkkitehtuuri, jolle on keskeistä verkkopalveluiden ja XML-kielen käyttö. Tällä arkkitehtuurilla toteutettavat verkkopalvelut tarkoittavat sovelluksia, jotka keskustelevat keskenään hajautetussa ympäristössä (esim. internetissä). Käyttäjän kannalta uudet ohjelmistoarkkitehtuurit edellyttävät tietoturvamäärittelyiden ja tarvittaessa omien testausohjeistuksien päivittämistä.

[2] http://www.turku.fi/suomi/asukas/hallinto/kanslia/tietotekniikkaosasto/Loppuraportti17122001.rtf

9. YHTEENVETO

Tämän julkaisun pääasiallinen sisältö on turvallisuus, jonka varmistamista käsitellään neljän teeman avulla. Laitteen elinkaaren hallinta, ohjelmistojen turvallisuus, tietoturva ja riskienhallinta ovat avainasemassa parannettaessa laitejärjestelmien kokonaisturvallisuutta. Terveydenhuollon yksiköille turvallisuuden hallinta on suuri haaste, johon voidaan varustautua yhteistyössä laadittujen toimintaohjeiden avulla. Seuraavassa on esitetty terveydenhuollon yksiköille avainkysymyksiä, joita olisi syytä pohtia:

- Teknisillä osastoilla on edessään merkittävä muutos. Laitteiden korjaajista ja ensiavun tarjoajista on jouduttu muuntautumaan nykyajan hankintojen ja pilottijärjestelmien suunnittelijoiksi. Muutos edellyttää toimintojen elinkaariajattelua, jossa tehtävä pilkotaan osakokonaisuuksiin ja kullekin kokonaisuudelle selkeä tavoite. Tällainen toiminta edellyttää ohjeistettua projektinhallintaa, jonka tukena on laadukkaat katselmuskäytännöt.
- Useissa hankinnoissa tietotekniikan merkitys korostuu. Perinteisten elektroniikka- ja vahvavirtatekniikan aiheuttamien ongelmien lisäksi mukaan astuu myös tietotekniikan aiheuttamat ongelmat (prosessoritekniikka, ohjelmistotuotanto, sisällöntuotanto, käyttöjärjestelmäalustat ja ohjelmistoarkkitehtuurit ja -komponentit). Mikäli organisaatio haluaa itse hallita tietotekniikkaan liittyviä ongelmia, joudutaan väistämättä investoimaan myös ohjelmistojen ja tietokoneiden testausvälineisiin. Tämä edellyttää laitteistoja, erillistä testausympäristöä, testausohjelmistoja sekä ammattitaitoa.
- Riskienhallinprosessin kyky hallita potilaaseen, käyttäjään, huoltohenkilöstöön ja ympäristöön kohdistuvia vaaroja tuo uusia mahdollisuuksia sairaaloiden käyttöön. Riskienhallintaprosessi edellyttää lähes poikkeuksetta eri tahojen yhteistyötä. Tämä edellyttää sairaaloissa uutta ajattelutapaa, jossa eri osastojen välillä on saumaton yhteistyö ja eri osastot keskustelevat ja vaihtavat mielipiteitä säännöllisesti keskenään. Toimiakseen optimaalisesti riskienhallintaprosessi edellyttää myös johdon sitoutumisen asiaan sekä laajan menetelmäohjeistuksen ja välineiden käyttöönottoa. Tämä voi kyllä olla osa sitä arvokeskustelua, jossa pohditaan nykyisten lääkintälaitejärjestelmien monimutkaistumisen tarvetta tai järkevyyttä.

Avainkysymys onkin ehkä siinä, että mikä on työntävä voima nykyisessä terveydenhuollossa. Hoitoketjut ovat niin monimutkaisia, että tarvitaan

lisää tietojärjestelmiä vai onko ylimääräisiä tietojärjestelmiä niin paljon, että hoitoketjujen on ruvettava käyttämään niitä? Monimutkaisiin ja kalliisiin järjestelmiin tehtyjen investointien on vähitellen ruvettava maksamaan itsensä takaisin tehostuneina tutkimuksina, vaivattomimpina huoltoina ja päivityksinä.

- Terveydenhuollon toimintayksiköiden tulisi lisätä säädösten vaatimuksia hankinnan lähtötietovaatimuksiin. Esimerkiksi tietoturva- ja henkilörekisterilaki sekä potilaan oikeuksia ja asemaa käsittelevät lait voivat asettaa vaatimuksia laitejärjestelmien tietoturvaratkaisuille. Osa vaatimuksista voi olla jo sellaisia, että ne asettavat vaatimuksia jo mahdollisille toteutustavoille. Säädösten ja harmonisoitujen standardien soveltaminen määrittelyvaiheessa helpottaa mahdollisten ongelmatilanteiden ratkaisua.
- Terveydenhuollon toimintayksiköiden useat toiminnot (hankinta, hoito, huolto jne.) muodostavat isoja toimintakokonaisuuksia. Näissä toiminnoissa tulisi siirtyä prosessiajatteluun ja sen mukaiseen toimintaan (tunnistetaanko aina ko. prosessin erityispiirteet, esim. tiedon kulku, suhteet, prosessin haltija, määritellyt inputit/outputit ja suorituskyvyn mittarit).
- Terveydenhuollon toimintayksiköiden asenteet ja käytännöt toteutetuissa tietoturvaratkaisuissa ovat erittäin vaihtelevia. Yhteistyöllä voitaisiin saada aikaan parhaat käytännöt. Yhteistyössä voitaisiin laatia myös tietoturvaratkaisut, joita kukin sairaala voisi sitten modifioida haluamakseen. Tässä on muistettava, että ennen käytännön tietoturvaratkaisua on laadittava tietoturvapolitiikka ja asetettava tavoitteet tietoturvalle.
- Laitejärjestelmiin tehtävät muutokset ja päivitykset tulisi ohjeistaa. Ohjeiden on katettava ainakin testisuunnitelma, testiympäristö, käyttöönotto, hyväksyntäkriteerit sekä dokumentointi. Hankintavaiheessa voidaan viitata myös ko. ohjeisiin. Muutosten ja päivitysten hallinta on helpompaa, kun useammalla terveydenhuollon toimintayksiköllä on yhtenäiset otteet ja ohjeistukset laitetoimittajan suorittamiin muutoksiin. Mikäli useammat terveydenhuollon toimintayksiköt noudattaisivat samankaltaista ohjeistusta on laitetoimittajien pidemmällä aikavälillä vaikeaa olla noudattamatta myös tätä ohjeistusta.

SYMBOLILUETTELO

COTS	Commercial Of The Shelf
DHR	Design History Record, tuotantohistoria
EN	European Norm, eurooppalainen standardi
FMEA	Failure Mode and Effects Analysis (system), vika- ja vaikutusanalyysi
FMECA	Failure Mode, Effects, and Criticality Analysis (system), vika-, vaikutus- ja kriittisyysanalyysi
FTA	Fault Tree Analysis, vikapuuanalyysi
IEC	International Electrotechnical Commission
IEEE	The Institute of Electrical and Electronics Engineers, Inc.
ISO	International Organization for Standardization
NB	Notified Body, ilmoitettu laitos
PEMS	Programmable Electrical Medical System, ohjelmoitava sähkökäyttöinen lääkintälaitejärjestelmä
RMF	Risk Management File, riskienhallintatiedosto
RMS	Risk Management Summary. riskienhallintaselostus
SFMECA	Software Failure Mode, Effects, and Criticality Analysis. ohjelmiston vika-, vaikutus- ja kriittisyysanalyysi
SRS	Software Requirement Specification. ohjelmiston vaatimusspesifikaatio
VPN	Virtual Private Network
WLAN	Wireless Local Area Network
XML	Extensible Markup Language

LÄHDELUETTELO

[1] Pöyhönen Ilpo, Kylmälä Kaarle, Harju Hannu, Kemppainen-Kajola Pia, Kuhakoski Kalle, Spankie Greig, Ventä Olli: Vaatimukset ohjelmistoa sisältäville lääkintälaitteille. Hallinta ja menetelmät vaatimustenmukaisuuden osoittamiseksi, 2002. VTT Tuotteet ja tuotanto, Espoo. 135 s. + liitt. 40 s. VTT Tiedotteita - Research Notes : 2150 ISBN 951-38-6060-4; 951-38-6061-2

[2] Pöyhönen Ilpo, Kylmälä Kaarle. Terveydenhuollon laadunhallinta. Sähkökäyttöisten lääkintälaitejärjestelmien turvallisuus. Lääkelaitoksen julkaisusarja 3/1998. ISBN 952-5099-21-0.

[3] Haikala, I & Märijärvi, J. Ohjelmistotuotanto, 1998, Suomen Atk-kustannus

[4] Guidance for FDA Reviewers and Industry, Guidance for the Content of Premarket Submissions for Software Contained in Medical Devices

Terveydenhuollon laitteita ja tarvikkeita koskevat säädökset ja määräykset

Laki terveydenhuollon laitteista ja tarvikkeista (1505/94)

Asetus terveydenhuollon laitteista ja tarvikkeista (1506/94)

Sosiaali- ja terveysministeriön päätös terveydenhuollon laitteista ja tarvikkeista 66:1994

Säädösten ja määräysten ajantasaistetut versiot löytyvät Lääkelaitoksen verkkosivuilta http://www.laakelaitos.fi

Standardeja

SFS 4372	Lääkintätilojen sähköasennukset.
SFS-EN 1050	Koneturvallisuus, Riskin arvioinnin periaatteet.
SFS-EN 60601-1	Sähkökäyttöisten lääkintälaitteiden turvallisuus. Osa 1: Yleiset vaatimukset
SFS-EN 60601-1-1	Medical electrical equipment. Part 1-1: General requirements for safety – Collateral standard: Safety requirements for medical electrical systems

SFS-EN 60601-1-4	Medical electrical equipment - Part 1-4: General requirements for safety. Collateral standard: Programmable electrical medical systems.
SFS-EN 60601-1-6	Medical electrical equipment - Part 1-6: General requirements for safety - Collateral standard: Usability: Analysis, test and validation of human factors compatibility'.
SFS-EN 60950	Safety of information technology equipment including electrical business equipment.
SFS-EN ISO 14971	Medical devices – Application of risk management to medical devices.
SFS-EN ISO 9001	Laatujärjestelmät. Suunnittelun, tuotekehityksen, tuotannon, asennuksen ja huollon laadunvarmistusmalli
SFS-EN ISO 9002	Laatujärjestelmät. Tuotannon, asennuksen ja huollon laadunvarmistusmalli
SFS-EN ISO 9003	Laatujärjestelmät. Lopputarkastuksen ja -testauksen laadunvarmistusmalli.
SFS-IEC 60300-3-9	Luotettavuusjohtaminen osa 3: Käyttöopas. Luku 9: Teknisten järjestelmien riskianalyysi.
IEC 61508-5:1998	Examples of methods for the determination of safety integrity levels
ISO/IEC 12207:1995	Information technology - Software life cycle processes.
IEEE 1074:1997	Standard for Developing Software Life Cycle Processes (Software).
BS 7799-1:fi	Tietoturvallisuuden hallinta. Osa 1. Tietoturvallisuuden hallintajärjestelmiä koskeva menettelyohje.
BS 7799-2:fi	Tietoturvallisuuden hallinta. Osa 2. Tietoturvallisuuden hallintajärjestelmiä koskevat vaatimukset.

LIITE A LYHYESTI SÄHKÖTURVALLISUUSVAATIMUKSISTA

A.1 Sähköturvallisuus

Sähkökäyttöisen lääkintälaitteen sähköturvallisuudelle asetetut vaatimukset esitetään SFS-EN 60601 -standardisarjassa . Perusstandardi SFS-EN 60601-1 määrittelee sähkökäyttöisen lääkintälaitteen perusturvallisuuden ja SFS-EN 60601-2 -standardisarja määrittelee lisävaatimukset eri laitetyypeille. Laitteen täyttäessä nämä vaatimukset, katsotaan laitteen täyttävän myös terveydenhuollon laitteita ja tarvikkeita koskevien säädösten vaatimukset näiltä osin.

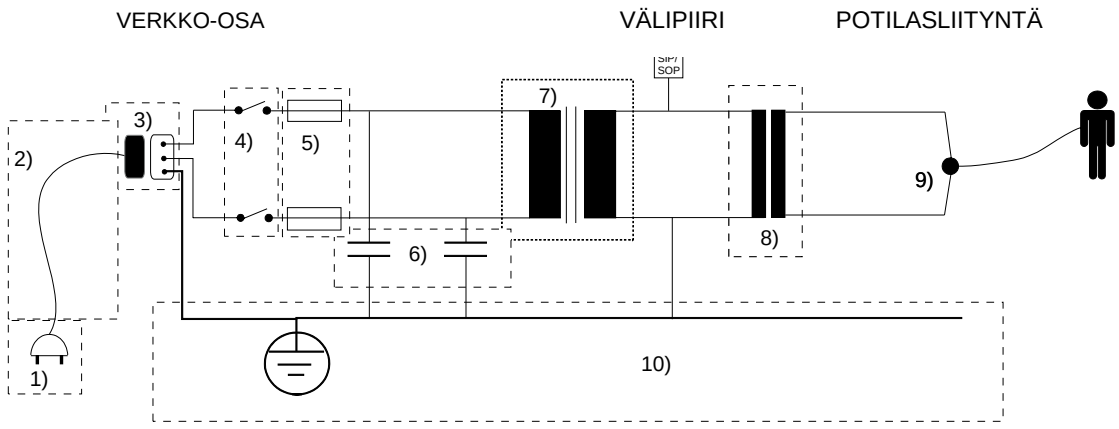
Yleisimmät vaatimusten vastaisuudet lääkintälaitteiden sähköturvallisuudessa aiheutuvat väärin valituista komponenteista, puutteellisista pinta- ja ilmaväleistä, liian suurista vuotovirroista tai puutteellisista maadoituksista. Lisäksi laitteen mukana seuraavissa dokumenteissa on usein ollut merkittäviä puutteita. Seuraavassa esitetään muutama esimerkki komponenteille, pinta- ja ilmaväleille, vuotovirroille sekä maadoitukselle asetettavista vaatimuksista. Esimerkkitapauksen laite on luokkaa I ja siinä on kelluva liityntäosa. Esimerkissä määritellään laitteelle asetettavat vaatimukset. Tämän jälkeen kuvataan käyttäjälle sopivia keinoja, joilla laitteen turvallisuus voidaan varmistaa.

A.1.1 Komponentit

Laitteen suunnittelussa merkittävä osuus on komponenttien valinta. Erityisesti tämä korostuu ns. kriittisten komponenttien kohdalla. Komponenttien on sovelluttava suunniteltuun käyttötarkoitukseensa ja täytettävä tarvittavien standardien vaatimukset. Kuvassa A1 numeroitujen alueiden komponentit ovat pääasiallisesti ns. kriittisiä komponentteja, joille asetettavat vaatimukset on selvitettävä jo suunnittelun alkuvaiheessa. Lisäksi on huomioitava, että eri markkina-alueilla on toisistaan poikkeavia vaatimuksia. Esimerkiksi UL[3]-vaatimukset komponenttien hyväksyntöjen, virran- ja lämmönkeston suhteen ovat joiltain osin huomattavasti tiukemmat kuin vastaavat IEC[4]-vaatimukset.

[3] Underwriters Laboratories

[4] International Electrotechnical Commission



Kuva A1. *Tuotteen suunnittelussa erityisesti huomioitavia komponentteja*

Seuraavassa on käsitelty kuvan A1 komponenttien (kohdat 1-10) vaatimuksia ja käyttäjän keinoja varmistua niiden vaatimusten mukaisuudesta.

1 Pistotulpalle asetettavat vaatimukset ovat ensisijaisesti riittävä virrankesto, pinta- ja ilmavälit, mekaaninen kestävyys ja tarvittaessa nesteiden sisäänpääsy.

Käyttäjän keinoja: Määräaikaishuolloissa voidaan tarkastaa visuaalisten tarkastusten avulla mekaaninen kunto ja nesteiden sisäänpääsy (infuusionesteet, veri ja virtsa) sekä eristysvastusmittauksien avulla mahdolliset eristysviat verkko-osan ja laitteen rungon välillä.

2 Verkkojohdon vaatimukset poikkeavat, jos verkkojohto on irrotettava tai uudelleen johdotettava. Ensisijaisina vaatimuksina ovat materiaali, lämmönkesto, poikkipinta-ala ja mekaaninen kestävyys.

Käyttäjän keinoja: Määräaikaishuolloissa voidaan tarkastaa visuaalisten tarkastusten avulla mekaaninen kunto (säikeiden kunto, eristeiden kunto, vedonpoistot jne.), eristysvastusmittauksien avulla mahdolliset eristysviat verkko-osan ja laitteen rungon välillä ja suojamaadoitusmittauksen avulla maadoituksen jatkuvuus ja riittävyys.

3 Kojepistokkeiden ja kojevastakkeiden vaatimuksina ovat pinta- ja ilmavälit, virrankesto, kosketussuojaus, mekaaninen kestävyys ja tarvittaessa nesteiden sisäänpääsy sekä kojevastakkeilla laitteen sisäisten johdotusten jatkaminen.

Käyttäjän keinoja: Määräaikaishuolloissa voidaan tarkastaa visuaalisten tarkastusten avulla mekaaninen kunto ja nesteiden sisäänpääsy (infuusionesteet, veri ja virtsa) sekä eristysvastusmittauksien avulla mahdolliset eristysviat verkko-osan ja laitteen rungon välillä.

4 Verkkokytkimen vaatimuksina ovat pinta- ja ilmavälit, virrankesto, kosketussuojaus ja tarvittaessa nesteiden sisäänpääsy sekä merkinnät.

5 Verkkosulakkeiden ja sulakepesien vaatimuksina ovat pinta- ja ilmavälit, virrankesto, virrankatkaisukyky, kosketussuojaus ja tarvittaessa nesteiden sisäänpääsy (ulkoiset sulakepesät).

Käyttäjän keinoja: Määräaikaishuollossa ei välttämättä tarvitse tarkastaa sulakkeita. Mutta

on ehdottoman tärkeää sulakkeita vaihdettaessa, että se korvataan aivan samanlaisella sulakkeella. Huomioi sulakkeissa T ja F merkinnät sekä High Break -ominaisuus. Muista myös, että eri valmistajien vastaavan kokoluokan sulakkeiden palokäyrät voivat poiketa toisistaan. Huom! Käytä vain ja ainoastaan samanlaisia sulakkeita.

6 Häiriönpoistokondensaattorien vaatimuksina on erillinen komponenttihyväksyntä X-kondensaattoreille (X1 tai X2) ja Y-kondensaattoreille (Y1 tai Y2).

Käyttäjän keinoja: Määräaikaishuolloissa voidaan kapasitanssi- ja vuotovirtamittauksin tutkia X- ja Y-kondensaattorien kunto.

7 Verkkomuuntajan vaatimuksina on pinta- ja ilmavälit, materiaalit, materiaalien riittävä lämpötilankesto, oikea sulakesuojaus, riittävä eristys- ja dielektrinen lujuus.

Käyttäjän keinoja: Määräaikaishuolloissa voidaan käyttökokein ja vuotovirtamittauksin tutkia verkkomuuntajien kunto. Laajempia kokeita voi olla eristysvastusmittaukset ja rakenteellinen tutkiminen, joka edellyttää laitteen purkua (harkittava toimenpiteen tarpeellisuutta).

8 Isolointimuuntaja tai optoisolaattorit: Vaatimuksina pinta- ja ilmavälit, materiaalit, riittävä eristyslujuus sekä tarvittaessa defibrilloinnin kesto.

Käyttäjän keinoja: Määräaikaishuolloissa voidaan eristysvastusmittauksin ja vuotovirtamittauksin tutkia komponentin kunto. Laajempia kokeita voi olla eristysvastusmittaukset ja rakenteellinen tutkiminen, joka edellyttää laitteen purkua (harkittava toimenpiteen tarpeellisuutta).

9 Vaatimuksina potilasliitynnän liittimille on mekaaninen kestävyys, pinta- ja ilmavälit, materiaalit, riittävä eristyslujuus ja liittimien vaihdettavuus ei saa aiheuttaa vaaratilannetta.

Käyttäjän keinoja: Määräaikaishuolloissa voidaan tarkastaa visuaalisten tarkastusten avulla mekaaninen kunto sekä eristysvastus- ja vuotovirtamittausten avulla mahdolliset eristysviat potilasliitynnässä (Huomioi B-, BF- ja CF-liityntöjen erot).

10 Maadoituksen vaatimuksina ovat riittävän pieni resistanssi, tarvittavien osien maadoitus, riittävä virrankesto maadoituksen osilla, kaapelien värit ja pinta-ala.

Käyttäjän keinoja: Määräaikaishuolloissa voidaan tarkastaa visuaalisesti maadoitusliittimien mekaaninen kunto sekä suojamaatiemittausten avulla maadoituksen hyvyys. Tarkasta myös mahdolliset lisäsuojamaadoitukset ja potentiaalintasausten liittimet ja johtimet.

Komponenttien valinnassa tulee kiinnittää erityisesti huomiota seuraaviin ominaisuuksiin:

Erillishyväksyntä	Komponentista löytyy erillishyväksynnän osoittava leima. Usein suunnittelu edellyttää komponentin toimittajalta kolmannen osapuolen todistusta. Nämä todistukset muodostavat osan tuotteen teknisestä tiedostosta. *HUOM! Erillishyväksyntä ei aina takaa sitä, että ko. komponentti soveltuisi lääkintälaitteen osaksi.*

Soveltuu käyttöön	Komponentit ovat virrankestoltaan, pinta- ja ilmaväleiltään sekä suorituskyvyltään riittäviä ja täyttää tarvittavat turvallisuusvaatimukset.
Riittävät EMC -ominaisuudet	Komponentilta voidaan edellyttää erillisiä EMC–raportteja. Lopulliset EMC–hyväksynnät voidaan tehdä ainoastaan valmiille laitteelle
Riittävät mekaaniset ominaisuudet	Lääkintälaitteen suunnittelu edellyttää sovelluksesta riippuen riittävien turvakertoimien käyttöä.
Kestävät käytettyjä puhdistusaineita	Erityisesti muovimateriaalien ja merkintöjen on kestettävä lääkintätiloissa käytetyt puhdistusaineet (vesi, denaturoitu sprii ja isopropanoli). Esimerkiksi tietokoneet eivät välttämättä täytä näitä vaatimuksia.

Käyttäjäorganisaation suorittaessa laitteessa sellaisia korjauksia tai muutoksia, jotka edellyttävät komponenttien vaihtoja on varmistuttava ensinnäkin siitä, että salliiko laitetoimittaja käyttäjätahon suorittaa korjauksia sekä täyttääkö laite korjausten jälkeen säädösten ja standardien vaatimukset. Vaatimus pätee myös laitetoimittajan suorittamiin korjauksiin, joista käyttäjätahon tulisi saada luotettava todistus. Todistuksesta tulisi käydä ilmi, että mitä laitteesta on korjattu ja täyttääkö laite korjausten jälkeen sille asetetut turvallisuus- ja suorituskykyvaatimukset.

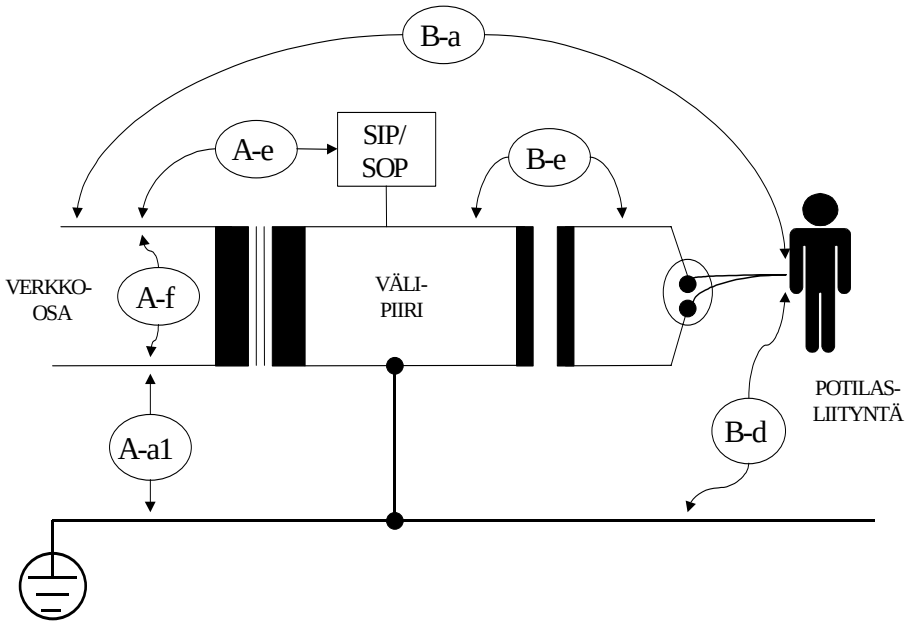
A.1.2 Eristysvälit

Pinta- ja ilmavälien suunnittelussa tulee huomioida standardin SFS-EN 60601-1 asettamat vaatimukset eristysväleille. Laitekohtaiset standardit asettavat joitain lisävaatimuksia lähinnä B-d ja B-e eristysväleille. Standardi SFS-EN 60601-1 määrittelee kyseisen eristysvälin eristysvaatimuksen. Eristyksen yli vaikuttava jännite määrittelee tapauskohtaisesti ko. eristykselle sovellettavan testijännitteen jännitekokeen suorittamista varten sekä lopulliset millimetrivaatimukset pinta- ja ilmaväleille. Pinta- ja ilmavälien vaatimustenvastaisuudet aiheuttavat yleensä huomattavia muutoksia piirilevyjen suunnitteluun ja toteutukseen, mikä taas aiheuttaa huomattavia aikatauluviiveitä laitteen suunnittelussa. Tämän vuoksi tuotekehityksessä tulee pinta- ja ilmavälien suunnittelu tehdä huolellisesti. Suunnittelun tueksi olisi hyvä tehdä alustavia tarkastuksia jo suunnittelun alkuvaiheessa. Pinta- ja ilmavälien esitarkastuksen lisäksi olisi syytä tehdä kyseisille väleille myös vastaavat jännitekokeet.

Kuvassa A2 on määritelty lääkintälaitteiden yleisimmät eristysvälit. Eristysvälien määrittämiseen vaikuttaa laitteen luokittelu, referenssijännitteet eristysten yli, käytettävät materiaalit, käytettävät komponentit sekä laitteen käyttöolosuhteet lähinnä laitteen likaantumisen ja mekaanisen liikkeen ja rasituksen kautta. Eristysvälien vaatimukset määritellään taulukossa A1.

Käyttäjäorganisaation kannalta pinta- ja ilmavälien tarkastus tulisi määritellä osaksi määräaikaistarkastuksia. Huoltotoimenpiteissä on huomioitava valmistajan suunnittelemien eristysvälien säilyminen. Esimerkiksi ruuvien pituuksien tai materiaalin muuttaminen voi vaikuttaa heikentävästi eristysväleihin.

Tarkastuksia voidaan tehdä joko jännitetestein tai vuotovirtamittauksin. Jännitekokeita määriteltäessä on huomioitava, että liian korkeat testijännitteet vanhentavat laitteen eristeitä. Pinta- ja ilmavälien tarkastuksessa voidaan tehdä myös ns. silmämääräinen tarkastus, jossa etsitään laitteesta mahdollisia mekaanisia vaurioita tai lian ja nesteiden aiheuttamia pinta- ja ilmavälien huononemisia. Tarkastuksessa tulisi huomioida myös korroosiovaikutukset.



Kuva A2. *Lääkintälaitteen yleisimmät eristysvälit.*

Taulukko A1. Eristysvälien vaatimukset

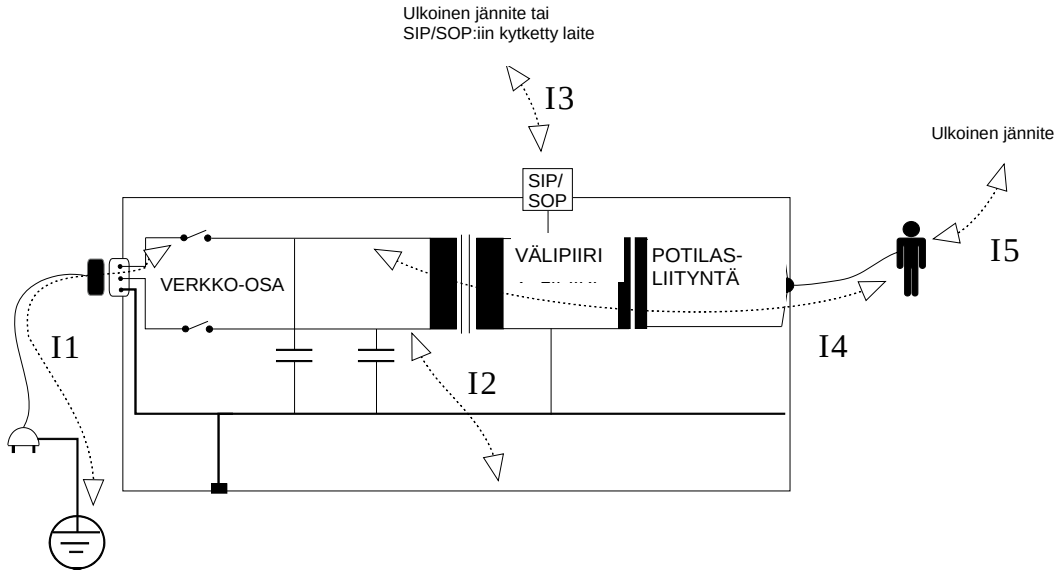
ERISTYS	VAATIMUS
A-a1	Jännitteisten osien ja suojamaadoitettujen kosketeltavien metalliosien välillä, eristyksen tulee olla peruseristys.
A-f	Verkko-osan niiden osien välillä, joilla on vastakkainen napaisuus, eristyksen tulee olla peruseristys.
A-e	Jännitteisten osien, jotka eivät ole signaalin tulo- tai lähtöosien osia, ja signaalin tulo- tai lähtöosien, jotka eivät ole suojamaadoitettuja, välillä, eristyksen tulee olla kaksoiseristys tai vahvistettu eristys.
B-a	Liityntäosan (potilaspiiri) ja jännitteisten osien välillä, eristyksen tulee olla kaksoiseristys tai vahvistettu eristys
B-d	Kelluvan liityntäosan ja kotelon, mukaan lukien signaalin tulo- ja lähtöosat välillä, eristyksen tulee olla peruseristys.
B-e	Kelluvan liityntäosan ja kotelon välillä, kun kelluvassa liityntäosassa on jännitteitä mukaan lukien liityntäosan minkä tahansa osan maadoittamisen mukaan lukien signaalin tulo- ja lähtöosat, välillä, eristyksen tulee olla kaksoiseristys tai vahvistettu eristys.

A.1.3 Vuotovirrat

Vuotovirrat ovat ei-toiminnallisia virtoja, jotka syntyvät sähkökäyttöisistä laitteista ja hakeutuvat eristysten yli ylemmästä potentiaalista alempaan potentiaaliin, jolloin kulkureittinä voi olla potilas, käyttäjä, laitteen runko, suojamaatien muu osa tai huonosti eristävä materiaali.

Lääkintälaitteen vuotovirtavaatimukset esitetään SFS-EN 60601 -standardisarjassa. Perusstandardi SFS-EN 60601-1 määrittelee lääkintälaitteen yleiset vuotovirtavaatimukset ja SFS-EN 60601-2 –standardisarja määrittelee lisävaatimukset eri laitetyypeille. Kuvassa A3 havainnollistetaan vuotovirtareittejä, joita yksittäisessä laitteessa syntyy. Vuotovirtareittien tarkempi selitys on esitetty taulukossa A2.

Käyttäjäorganisaation kannalta vuotovirtojen mittaukset ovat yksi hyvin tärkeä kunnonvalvontakohde. Tärkeää mittauksissa on se, että kullekin laitetyypille määritellään ja ohjeistetaan suoritettavat mittaukset. Mittaukset tulee suorittaa kalibroiduilla mittalaitteilla ja tulokset kirjataan kunnonvalvontapöytäkirjaan. Kunnonvalvontapöytäkirjan avulla voidaan seurata laitteessa tapahtuvia muutoksia ja ennakoida täten mahdollinen huollon tarve. Käyttäjäorganisaation valitessa vuotovirtamittalaitteita on varmistuttava, että valittu mittalaite soveltuu em. standardien mukaisiin vuotovirtamittauksiin.



Kuva A3. *Lääkintälaitteessa syntyviä vuotovirtareittejä*

Taulukko A2. Laitteessa syntyviä vuotovirtareittejä

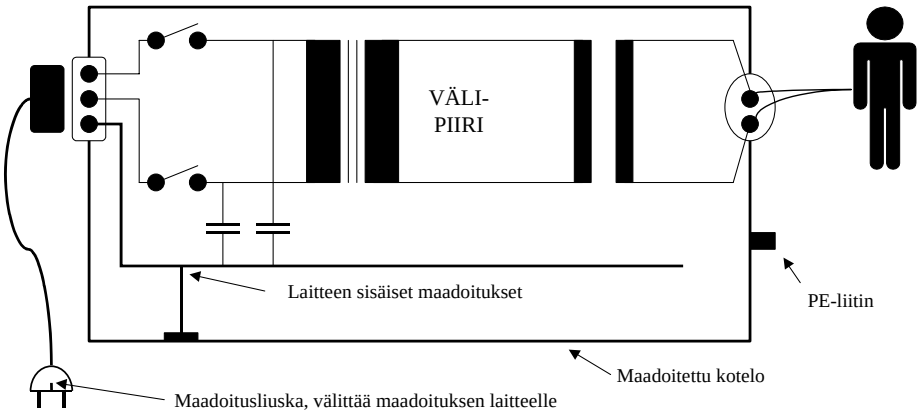
VIRTA	SELITYS
I1	Maavuotovirta hakeutuu laitteen jännitteisistä osista normaalikäytössä tai yhden vian tapauksessa maahan, käyttäjään, potilaaseen tai signaalijohtimien kautta toiseen laitteeseen. Laitteessa käytettävät häiriönpoistokondensaattorit kasvattavat maavuotovirtaa.
I2	Kotelovuotovirta hakeutuu laitteen jännitteisistä osista johtavan kotelon kautta normaalikäytössä tai yhden vian tapauksessa käyttäjään, potilaaseen tai toiseen laitteeseen. Yleensä laitteen johtavat kosketeltavat kotelon osat suojamaadoitetaan. Tällä estetään samalla ylimääräisiä häiriöitä ja vaaratilanne, että maadoittamattomat johtavat osat voisivat tulla jännitteisiksi.
I3	Vuotovirta voi näkyä laitteessa kasvaneena maa- kotelo- tai potilasvuotovirtana. Laitteessa olevat signaaliliittimet tulee määritellä tiettyyn tarkoitukseen tai tietylle laitteelle, jolloin vältetään tilanne, että ko. liittimiin kytkettäisiin standardin vastaisia laitteita ja täten heikennettäisiin laitteen sähköturvallisuutta. Mikäli signaaliliittimiin voidaan kytkeä useita erilaisia laitteita on signaaliliitimien galvaaninen yhteys katkaistava. Tässä yhteydessä on huomioitava myös järjestelmien aiheuttamat vuotovirrat.
I4	Potilasvuotovirta hakeutuu laitteen jännitteisistä osista normaalikäytössä tai yhden vian tapauksessa potilaaseen. Isolointikomponenttien, liittimien ja kaapeleiden sekä käytettyjen materiaalien valinta ja suunnittelu erityisen tärkeää vuotovirtojen rajoittamisessa.
I5	Potilaan tullessa jännitteiseksi vuotovirta hakeutuu laitteen eristeiden kautta maihin. Isolointikomponenttien, liittimien ja kaapeleiden sekä käytettyjen materiaalien valinta ja suunnittelu on erityisen tärkeää vuotovirtojen rajoittamisessa.

A.1.4 Maadoitukset

Maadoituksen tarkoituksena on suojella potilasta tai käyttäjää laitteen verkko-osan pettäessä siten, että laitteen kuoreen tai johtaviin osiin hakeutuva verkkojännite oikosulkeutuu maapotentiaaliin. Eristevian seurauksena laitteen suojalaitteet toimivat ja tekevät laitteen jännitteettömäksi.

Maadoituksessa tulee kiinnittää huomiota myös maadoituksen jatkuvuuteen, jotta se pysyy vaatimukset täyttävänä koko matkallaan (laitteen sisällä, laitteiden välillä). Laitteen kaikki johtavat osat, jotka voivat yhden vian tapauksessa tulla jännitteisiksi on suojamaadoitettava. Suojamaadoituksen tulee kestää 25 A:n virta, jolla varmistetaan ryhmäsulakkeen toimiminen. Käyttäjäorganisaation kannalta on tärkeää tarkastaa maadoituksen kunto määräajoin tapahtuvin visuaalisin kunnontarkastuksin ja 25A:n virralla tehtävin resistanssimittauksin.

Joissain tilanteissa laitteen luotettava toiminta edellyttää potentiaalintasauksen käyttöä (ks. kuva A4). Potentiaalintasausta voidaan käyttää esimerkiksi ympäristössä olevien häiriöiden eliminoimiseksi silloin, kun mitataan alhaisia jännitetasoja (esim. biosähköisten signaalien mittaus). Potentiaalintasaukset voidaan myös liittää määräaikaistarkastusten piiriin. Potentiaalintasausta ei tulisi käyttää lisäsuojamaadoituksena.



Kuva A4. *Laitteen maadoitukset*

A.2 Lyhyesti muista vaatimuksista

A.2.1 Mekaaninen turvallisuus

Yleiset vaatimukset lääkintälaitteen mekaaniselle turvallisuudelle määritellään standardissa SFS-EN 60601-1 ja SFS-EN 60601-2- standardisarja määrittelee lisävaatimuksia eri laitetyypeille. Mekaaniselle kestävyydelle ja turvallisuudelle on annettu useita vaatimuksia myös terveydenhoidon laitteita käsittelevissä ISO-standardeissa. Terveydenhuollon laitteita ja tarvikkeita koskevien säädösten kannalta standardiin perustuva ratkaisu ja sen toimivuuden toteaminen esitetyllä testimenetelmällä on valmistajalle helpompi tapa kuin oma ratkaisu. Yleisimmät vaarat ovat laitteen riittämätön lujuus potilaan aiheuttaman rasituksen kohteena, laitteen romahtaminen/kaatuminen potilaan päälle ja käyttö muulla tavoin kuin on tarkoitettu (esim. väärässä tilassa). Kuljetustilanteet ovat laitteelle yleensä hyvin rasittavia.

Käyttäjäorganisaation kannalta laitteiden vastaanottotarkastuksen tulisi kattaa toimituksen visuaalinen tarkastus mahdollisten kuljetusvaurioiden varalta. Valmistajan asennusohjeiden noudattamien on ensisijaisen tärkeää mekaanisen turvallisuuden varmistamiseksi. Lisäksi erilaisten kannatinrakenteiden säännöllinen kunnonvalvonta on tärkeää alkavien vaurioiden toteamiseksi.

A.2.2 Palo- ja lämpöturvallisuus

Yleiset vaatimukset lääkintälaitteen palo- ja lämpöturvallisuudelle määritellään standardissa SFS-EN 60601-1 ja SFS-EN 60601-2 -standardisarja määrittelee lisävaatimuksia eri laitetyypeille. Laitteen täyttäessä nämä vaatimukset, katsotaan laitteen täyttävän myös säädöksissä annetut terveydenhuollon laitteita ja tarvikkeita koskevat olennaiset vaatimukset.

Suunnittelijan kannalta palo- ja lämpöturvallisuuden varmistaminen määritellyissä vikatilanteissa on vaativa ja aikaa vievä tehtävä. Perinteisten mittausantureiden sijaan on nykyään käytettävissä mallinnukseen perustuvia analyysimenetelmiä ja myöskin lämpökameroita, joilla voidaan rekisteröidä myös lämpötilan muutoksia.

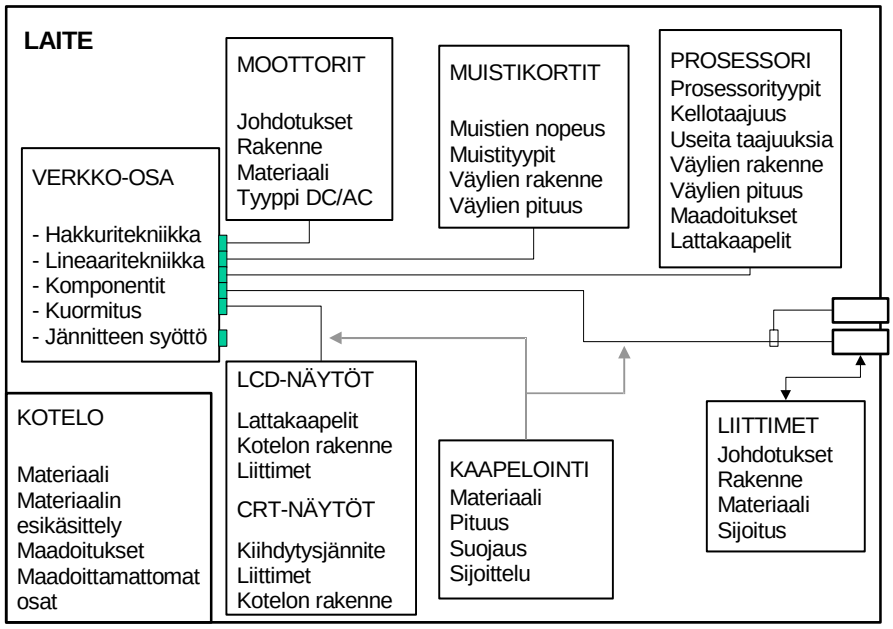
Palo- ja lämpöturvallisuuden varmistamiseksi käyttöorganisaation tehtäväksi jää varmistaa, että laitteet sijoitetaan valmistajan ohjeiden mukaisesti riittävän tuuletuksen varmistamiseksi. Samoin säännöllisessä kunnonvalvonnassa on hyvä tarkastaa laitteen suodattimet sekä tulenaran pölyn kerääntyminen laitteen sisäosiin.

A.2.3 Sähkömagneettinen yhteensopivuus

Uuden sähkökäyttöisen lääkintälaitteen tulee ennen markkinoilla saattamista täyttää sähkömagneettisen yhteensopivuuden asettamat sieto- ja päästövaatimukset, jotka määritellään standardissa SFS-EN 60601-1-2. Standardia noudattamalla ja sen vaatimukset täyttämällä voidaan olettaa lääkintälaitteita koskevien olennaisten vaatimusten mukaisuus sähkömagneettisen yhteensopivuuden (EMC) osalta.

Sähkökäyttöisen lääkintälaitteen sähkömagneettisen yhteensopivuuden suunnittelussa on huomioitava ns. hyväksyttämistestien suorittamisjärjestys. Tällä voi olla merkittäviä seurauksia tuotteen suunnittelukustannuksissa. Mikäli laitteesta tarkastetaan ensin sähköturvallisuus ja tämän jälkeen EMC-mittauksissa todetaan, että laitteeseen on tehtävä EMC-vaatimusten täyttämiseksi rakennemuutoksia, sähköturvallisuustestit on tehtävä mahdollisesti uudelleen. Muutokset erityisesti laitteen verkko-osassa ja laitteen potilasliitynnässä saattavat aiheuttaa sähköturvallisuustestien uudelleen suorittamisen. Tämän takia olisikin syytä tehdä ns. esitarkastuksia laitteen eri suunnitteluvaiheessa, jotta lopputuotteen vaatimusten täyttyminen voitaisiin varmistaa.

Sähkömagneettisen yhteensopivuuden kannalta tärkeitä laitteen osia ovat verkko-osa, kotelorakenne, näytöt, liitimet, ulkoinen ja sisäisen kaapelointi sekä muistit ja prosessorit (kuva A5). Taulukossa A3 on listattu joitain toimenpiteitä, joilla sähkömagneettisia häiriöitä voidaan pienentää.



Kuva A5. *Sähkömagneettiseen yhteensopivuuteen vaikuttavia laitteen*

Taulukko A3. Keinoja vähentää sähkömagneettisia häiriöitä

LAITTEEN OSA	HÄIRIÖN PIENENNYSKEINOJA
Verkko-osa	Häiriöitä voidaan pienentää komponenttivalinnoilla, tehokertoimen korjainpiireillä, häiriönvaimennuskondensaattoreilla ja piirikortin ground plate -tekniikalla.
Moottorit	Häiriöitä voidaan pienentää moottorityypin valinnalla, moottorin ja johtimien koteloinnilla, moottorin ohjauksen säädöillä ja käytettävällä tekniikalla tai moottorin jännitteen valinnalla (AC/DC tai verkkojännite vai pienjännite).
Kotelo	Häiriöitä voidaan pienentää kotelon materiaali valinnoilla, materiaalin esikäsitellyllä (esim. muovimateriaalin maalaaminen johtavalla maalilla kotelon sisäpuolelta) tai välttämällä maadoittamattomia kotelon osia.
Näytöt	Häiriöitä voidaan pienentää koteloimalla näytöt ja näytölle tulevat liittimet johtavalla maadoitetulla kotelolla, minimoimalla näytöille tulevat johtimet ja lattakaapelit tai käyttämällä johtimien ympärillä ferriittikeloja.
Prosessorit ja muistit	Häiriöitä voidaan pienentää alentamalla kellotaajuutta (mikäli sovelluksessa ei tarvita huomattavaa laskentatehoa), koteloimalla suurtaajuiset kellopiirit tai kiteet, minimoidaan kortilla olevat dataväylä- tai osoiteväyläfoliot, minimoidaan kortilta lähtevät tai kortille tulevat johtimet ja lattakaapelit tai käytetään johtimien ympärillä ferriittikeloja
Liittimet	Häiriöitä voidaan pienentää koteloimalla liittimet, välttämällä muovikuorisia liittimiä ja käyttämällä liittimille tulevissa johtimissa suojattuja kaapeleita, jotka voidaan maadoittaa liittimen runkoon.

Kun laitteelle tehdään ns. esitestejä, tulee huomioida kaikki mahdolliset käyttötilanteet. Laitetyypistä riippuen jollekin laitteelle voi olla epäedullista, kun sitä käytetään täydellä kuormalla tai vastaavasti toiselle laitteelle saattaa olla standby-tilanne kaikkein epäedullisin. Vastaavasti joku laitetyyppi saattaa häiriintyä eniten tietyllä toimintamuodolla, mutta päästää häiriöitä jollain toisella toimintamuodolla.

Mikäli valmistaja rakentaa laitetta erillisistä valmiista teholähde- tai näyttöyksiköistä, niin valmistajan kannattaa tilata kyseiset osat sellaiselta toimittajalta, joka kykenee toimittamaan komponentista myös tarvittavat hyväksyntätodistukset niin sähköturvallisuudesta kuin sähkömagneettisesta yhteensopivuudestakin. Todistuksista tulisi käydä ilmi, että ko. yksikkö/komponentti täyttää tarvittavat vaatimukset juuri niissä olosuhteissa, kuin mihin valmistaja ne on aikonut liittää. Käytännössä on usein havaittu, että erikseen hyväksytyt komponentit voivat lopullisessa sovelluksessa aiheuttaa liian suuria sähkömagneettisia häiriöitä.

Käyttäjäorganisaation tehdessä korjauksia tai muutoksia laitteeseen, tulee ottaa huomioon, että lähes minkä tahansa komponentin korvaaminen toisella komponentilla tai kaapelointien pituuksien ja kaapelointien sijoittelun muutos voi vaikuttaa laitteen sähkömagneettisiin ominaisuuksiin. Usein myös yksittäisten laitteiden kytkeminen järjestelmäksi aiheuttaa ominaisuuksien muutoksen.

A.3 Lähteet

1. SFS-EN 60601-1 Sähkökäyttöiset lääkintälaitteet. Yleiset turvallisuusvaatimukset. (IEC 601-1:1988), sisältää muutokset A1:1992, A11:1992, A12:1992
2. SFS-EN 60601-1-2 Sähkökäyttöiset lääkintälaitteet. Yleiset turvallisuusvaatimukset. Vaatimukset ja kokeet sähkömagneettiselle yhteensopivuudelle
3. SFS-EN 60601-2 -standardisarja eri lääkintälaiteryhmille. Sisältää laitekohtaiset standardit EN 60601-2-1 – EN 60601-2-50
4. Laki terveydenhuollon laitteista ja tarvikkeista 1505/94
5. Asetus terveydenhuollon laitteista ja tarvikkeista 1506/1994
6. Sosiaali- ja terveysministeriön päätös terveydenhuollon laitteista ja tarvikkeista 66:1994

LIITE B LAITEJÄRJESTELMÄN VASTAANOTTOTARKASTUS

B.1 Johdanto

Lääkintälaitteiden ja laitejärjestelmien hankintaprosessilla on merkittävä rooli hankinnan onnistumisessa. Hankintavaiheessa on mahdollista määritellä myös käyttöön, koulutukseen, huoltoon ja päivityksiin liittyvät toimenpiteet ja tehtävät. Keskitetyllä hankintaprosessilla voidaan myös poistaa niitä ongelmia, jotka aiheutuvat erilaisista hankintamenetelmistä terveydenhuollon yksikön sisällä (puutteelliset tilaukset, erilaiset hankintatavat -> osasto hankkii, tekniikka hankkii, lääkäri tuo tullessaan jne.).

Seuraavassa on esitetty malli, jonka mukaan vastaanottotarkastus voidaan tehdä. Ohjeet ovat vain viitteellisiä. Tärkeintä on kuitenkin se, että vastaavanlaisella menettelyllä pystytään kattamaan kunkin terveydenhuollon yksikön erityistarpeet. Tässä yhteydessä on tärkeätä kiinnittää huomiota myös erilaisiin rekisteröintitarpeisiin. Kukin organisaatio voi tarvittaessa muuttaa tai korjailla ehdotettua menettelyä omalle organisaatiolleen parhaiten sopivaksi.

B.2 Hankinta

Hankinta käsittää laitteen tai laitejärjestelmän esiselvitys-, tarjouspyyntö-, koekäyttö- ja toimitusvaiheen. Hankintavaiheessa syntyvät asiakirjat (määrittelyt, tarjouspyynnöt, lisäselvitykset ja tarjoukset) tulee tallettaa, jotta myöhemmin voidaan seurata tilauksen ja toimituksen tarkastamista tai ratkoa mahdollisia hankinnassa syntyneitä epäselvyyksiä. Hankinta voi sisältää useita eri toimitusvaiheita ja tämän takia on ehdottoman tärkeää nimetä vastuuhenkilö, joka valvoo toimitusta ja raportoi puutteista tarvittaessa.

Hankintavaiheessa on tärkeää määritellä laitteen tai järjestelmän spesifikaatiot, sekä menettelytavat, joilla määräaikaishuollot, kalibroinnit, vikakorjaukset ja päivitykset toteutetaan. Määrittelyllä varmistetaan laitteen tai järjestelmän turvallinen käyttö ja sovitaan selkeä vastuunjako käyttäjätahon ja toimittajan välillä. Määrittelyt ja spesifikaatiot on syytä kirjata sopimukseen.

B.2.1 Ohjelmiston sisältävien laitteistojen hankinta

Hankintavaiheessa on määriteltävä vaatimukset ohjelmiston sisältäville laitteille tai laitejärjestelmille. Vaatimusmäärittelyn on katettava sovellusohjelmat ja käyttöjärjestelmät sekä sovellettavat tietoturvaratkaisut. Vaatimuksissa tulisi huomioida:

- laitteistoalusta (prosessori, emolevysarja, välimuistivaatimukset, keskusmuistin määrä ja tyyppi)
- käyttöjärjestelmä (tyyppi, versio, kieliversio)
- sovellusohjelmat (ohjelmointikieli, päiväysasetukset, aikaformaatit, kielivaatimukset, tärkeää erityisesti tietokantasovelluksissa)
- kolmannen osapuolen ohjelmistojen käyttö (tarvitaanko niitä? Mitä ne ovat, esim. COTS-komponentit?)
- käytettyjen tietoverkkoratkaisujen asettamat vaatimukset
- ohjelmistosta johtuvat laiterajoitukset.

Mikäli laite tai laitejärjestelmä kytketään jo olemassa olevaan järjestelmään tai tietoverkkoon tulee myös liitynnän rajapintavaatimukset määritellä sisältäen sähköturvallisuuden, tietoturvan ja ohjelmistovaatimukset.

Tietoverkon määrittelyssä tulee ottaa huomioon kaapelointien ja verkon aktiivilaitteiden asettamat vaatimukset. Käytetyt ratkaisut vaikuttavat tietoturvateknologioihin ja fyysiseen tietoturvaan (laitteiden ja kaapelointien sijoittelu). Sovellettavien tietoturvaratkaisujen on noudatettava organisaation tietoturvapolitiikkaa.

B.3 Vastaanottotarkastus

Vastaanottotarkastuksen tarkoituksena on valvoa terveydenhuollon yksikössä käyttöön otettavan lääkintälaitteiden ja laitejärjestelmien vaatimustenmukaisuutta ja turvallisuutta, todeta tilausten ja toimitusten yhdenmukaisuus sekä määritellä erilaiset vastuuhenkilöt laitteen ja järjestelmän myöhempää käyttöä varten. Vastaanottotarkastus tulee suorittaa aina sillä tasolla, että varmistetaan laitteiden ja järjestelmien oikea ja turvallinen käyttö.

Mikäli laitteistot edellyttävät rakenteellisia muutoksia ne on syytä määritellä myös tilausasiakirjoissa. Terveydenhuollon toimintayksikön tulisi aina vaatia laitetoimittajaa tai laitetoimittajan valtuuttamaa tahoa suorittamaan muutostyöt. Valvojina muutostöille olisi laitteen toimittaja ja

tilauksen vastaanottaja. Tässä yhteydessä käynnistetään myös laitteen tai laitejärjestelmän käyttökoulutus, joka suunnitellaan yhdessä vastaanottotarkastuksesta vastaavan yksikön, laitteen käyttöpaikan henkilöstön ja laitteen toimittajan kanssa.

Vastaanottotarkastuksen tehtävänä on myös määritellä laitteen ja laitejärjestelmän huoltotarpeet ja tarvikkeet sekä nimetä huoltotoimiin soveltuvat henkilöt. Tämä edellyttää kiinteätä yhteistyötä vastaanottotarkastusyksikön, käyttöhenkilökunnan ja laitteen toimittajan kesken. Vastaanottotarkastuksen yhteydessä on määriteltävä myös laitteen toiminnan ja käytön kannalta tärkeät huollot, kalibroinnit ja määräaikaishuollot, joilla varmistetaan järjestelmän suorituskyky, sähköturvallisuus ja muu turvallisuus sekä jossain määrin myös käytettävyys. Vastaanottotarkastuksen yhteydessä laitteen tai laitejärjestelmän tiedot tallennetaan terveydenhuollon yksikön irtaimistokirjanpitoon.

B.3.1 Lähetysluettelo

Lähetysluettelo on se asiakirja, johon vedotaan jos toimituksen sisällössä havaitaan jotain huomauttamista. Tarkasta aina lähetysluettelon yhdenmukaisuus toimituksen kanssa. Kahden viikon kuluttua toimituksesta kukaan ei enää varmuudella voi sanoa, mikä oli toimituksen tarkka sisältö.

B.3.2 Yhdenmukaisuus

Koska tarjouspyynnön, tilauksen ja toimituksen välinen aikaväli saattaa olla hyvinkin pitkä on tilauksen ja toimituksen välinen yhdenmukaisuus syytä tarkastaa huolella. Joissakin terveydenhuollon yksiköissä on vastaanottotarkastukseen liitetty käytäntö, jonka mukaan laskut maksetaan vasta, kun tilaus ja toimitus ovat yhdenmukaisia ja laitteen toimittaja on järjestänyt sovitun käyttökoulutuksen.

B.3.3 Toiminnan toteaminen

Vastaanottotarkastuksessa laite ja laitejärjestelmä tarkastetaan huolella mahdollisten kuljetusvaurioiden tai muiden vaurioiden varalta. Tämän jälkeen laite tai laitejärjestelmä kytketään sähköverkkoon ja sille tehdään toiminnallinen tarkastus, jossa todetaan laitteen ja sen eri osien välinen toimivuus. Mikäli laite tai laitejärjestelmä ei toimi valmistajan ilmoittamalla tavalla tai se on vaurioitunut, vastaanottotarkastuksesta vastaava yksikkö ottaa yhteyttä laitteen toimittajaan. Vastaanottotarkastusta ei jatketa ennen kuin puutteet on korjattu.

B.3.4 Mukana seuraavat asiakirjat

Tuotteen mukana seuraavat asiakirjat kuvaavat laitteen tai laitejärjestelmän rakennetta ja toimintaa siten, että sitä voidaan käyttää sekä huoltaa tarkoituksenmukaisella tavalla. Asiakirjoja laadittaessa tulisi ensisijaisesti ottaa huomioon käyttäjä ja käyttöympäristö. Asiakirjoissa tulee kiinnittää huomiota myös valmistajan valtuuttaman jälleenmyyjän sekä huoltotahojen tarpeisiin. Tästä johtuen asiakirjat on tarkoituksenmukaista jakaa eri osiin. Asiakirjoissa tulee määritellä myös ne olosuhteet ja ehdot, joilla laite tai laitejärjestelmä toimii tarkoitetulla tavalla.

Asiakirjojen sisällön tulisi olla sellainen, että käyttäjä löytää sieltä tarvitsemansa asian helposti. Avainsanojen käyttö helpottaa huomattavasti tiedonhakua (esim. Puhdistus -> sivut ne ja ne jne.). Suunnittelussa tulisi kiinnittää erityistä huomiota asiakirjojen joustavaan käyttöön, luettavuuteen ja selkeisiin osakokonaisuuksiin. Vastaanottotarkastuksen tehtävänä on arvioida, että laitteen mukana seuraavien asiakirjojen avulla voidaan käyttää laitetta tai laitejärjestelmää asiaankuuluvalla tavalla. Laitteen asiakirjojen tulisi tapauskohtaisesti sisältää mm. seuraavia asioita:

A. Käyttöohjeasiakirja (käyttäjälle);
- laitteen suunniteltu käyttötarkoitus, jossa määritellään myös rajoitukset ja sivuvaikutukset (suorituskyky)
- käytön opastus (pikaopas, täydellinen opas)
- varoitukset
- merkinnät/symbolit ja niiden merkitys
- laitteen tai laitejärjestelmän luokitustiedot
- suorituskykytiedot
- puhdistusohjeet ja -aineet
- muut valmistajan tärkeäksi katsomat asiat.

B. Tekninen asiakirja (käyttäjälle, huoltajalle);
- laitteen suunniteltu käyttötarkoitus (tulee pysytellä määritellyissä rajoissa)
- huoltotiedot
- ongelmatilanteet
- merkinnät ja symbolit ja niiden merkitys
- laitteen luokittelutiedot
- suorituskykytiedot
- muut valmistajan tärkeäksi katsomat asiat.

Standardi SFS-EN 60601-1-1 määrittelee laitejärjestelmille lisävaatimuksia, jotka vastaanottotarkastuksen yhteydessä on tarkistettava. Järjestelmän mukana tulee toimittaa seuraavat asiakirjat jokaiselle sähkökäyttöiselle lääkintälaitteelle ja muille sähkökäyttöisille laitteille:

- **ohjeet** puhdistukselle jokaiselle sähkökäyttöisen lääkintälaitejärjestelmän osana olevalle laitteelle (sovellettavissa tapauksissa myös desinfioinnille ja steriloinnille)
- **määriteltävä lisäsuojatoimenpiteet**, joita tulisi soveltaa sähkökäyttöisen lääkintälaitejärjestelmän asennuksen aikana
- **määriteltävä** sähkökäyttöisen lääkintälaitejärjestelmän osat, jotka soveltuvat käytettäväksi hoitoalueella
- **määriteltävä lisämittaukset**, joita tulisi käyttää määräaikaishuolloissa
- **varoitus**, että moninapaista siirrettävää pistorasiaryhmää (MPSO) ei saa sijoittaa lattialle
- **varoitus**, että ylimääräistä moninapaista siirrettävää pistorasiaryhmää tai jatkojohtoa ei saa kytkeä sähkökäyttöiseen lääkintälaitejärjestelmään
- **varoitus**, joka kieltää kytkemästä spesifioimattomia laitteita sähkökäyttöiseen lääkintälaitejärjestelmään
- moninapaisen siirrettävän pistorasiaryhmän suurin sallittu kuormitettavuus
- **ohjeistus**, että moninapaisen siirrettävän pistorasiaryhmän syöttäessä, sähkökäyttöistä lääkintälaitejärjestelmää, sitä tulee käyttää syöttämään ainoastaan niitä laitteita, jotka kuuluvat sähkökäyttöiseen lääkintälaitejärjestelmään
- **selvitys riskeistä**, kun sähkökäyttöiseen lääkintälaitejärjestelmään kuuluva muu sähkökäyttöinen laite kytketään suoraan seinäpistorasiaan, vaikka se on syöttö on tarkoitettu toteutettavaksi erotusmuuntajalla varustetun moninapaisen siirrettävän pistorasia-ryhmän kautta
- **selvitys riskeistä**, kun järjestelmään kuulumaton sähkökäyttöinen laite kytketään suoraan moninapaiseen siirrettävään pistorasiaryhmään
- **määriteltävä** rajoitukset ympäristöolosuhteissa turvallisuuden varmistamiseksi (ks. SFS-EN 60601-1 kohta 10)
- **ohjeet käyttäjälle**, että ei kosketa standardin SFS-EN 60601-1-1 kohdassa 16.201[5] määriteltyjä osia ja potilasta samanaikaisesti

[5] Muun sähkökäyttöisen laitteen osat, joita käyttäjä voi olla kosketella hoitoalueella kansien, liittimien tms. irrottamisen jälkeen, käyttämättä työkalua, normaalin huollon, kalibroinnin tms. aikana, pitää toimia jännitteellä, joka ei ylitä 25 V vaihto- tai 60 V tasa- tai huippujännitettä, ja joka syötetään sähkölähteestä, joka on erotettu sähköverkosta yhdellä standardin SFS-EN 60601-1-1 kohdassa 17 g 1 - 5 kuvatulla tavalla.

- suositellaan **ohjetta** asentajalle, järjestelmän asentamiseksi parhaalla mahdollisella tavalla käyttäjän tarpeet huomioiden
- **ohjeet** käyttäjälle suorittaa kaikki puhdistukset, säädöt, sterilointi- ja desinfiointi-toimenpiteet.

Käytännössä tämä tarkoittaa muille kuin lääkintälaitteille lisäohjeistusten laadintaa, jotta em. vaatimukset tulevat täytetyiksi. Lisäohjeistusta tarvitaan myös silloin, kun järjestelmä kasataan vaikkapa jälleenmyyjän toimesta ja järjestelmään lisätään erillisiä laiteyksiköitä esim. erotusmuuntaja (MPSO).

Laitteen käyttöön, toimintaan ja suorituskykyyn liittyy aina riskejä, jotka jossain tietyssä olosuhteessa aiheuttavat riskin potilaalle, käyttäjälle tai ympäristölle. Riskienhallinnan keinoin nämä riskit on pienennetty hyväksyttävälle tasolle. Osalle riskeistä jää ns. hyväksyttävä jäännösriski, joka riskienhallintavaatimusten mukaisesti on talletettava tuotteen riskienhallintaselostukseen sekä tuotteen mukana seuraaviin käyttöohjeisiin. Seuraavassa muutama esimerkki ongelmista, jotka on tarvittaessa kuvattava laitteen mukana seuraavissa asiakirjoissa.

- Windows 95/98 -ohjelmisto asennetaan NT- tai Windows 2000 –ympäristöön.
  Jos tästä seuraa ongelma on valmistajan tarkennettava spesifikaatioita, määriteltävä ympäristö tai laitettava tarvittaessa varoitus käyttöohjeisiin.
- Käyttäjä asentaa uusia tai omia ohjelmaversioita järjestelmän tietokoneeseen, jolloin esimerkiksi yhteiset DLL-tiedostot muuttuvat. Valmistajan on estettävä käyttäjää asentamasta omia ohjelmia ja määriteltävä takuut ja lisättävä varoitus käyttöohjeisiin.
- Tärkeiden tietojen häviäminen. Kuvaile mahdollisuudet tietojen katoamiseen ja edellytä spesifikaatioissa katkeamatonta sähkönsyöttöä (UPS) sekä säännöllistä varmuuskopiointia.
- Laite toimii vain aikuisilla potilailla. Kiellä käyttöohjeissa käyttö lapsipotilaille ja määrittele laitteen käyttötarkoitus.

Erityisesti ohjelmiston osalta käsikirjojen tulisi sisältää tarkat määrittelyt eri ohjelmistojen versioista sisältäen käyttöjärjestelmäkomponentit, sovellusohjelmat, tietokannat ja tietokanta-ajurit sekä kolmannen osapuolen ohjelmistot. Määrittelyjen tulee sisältää myös kieliversiot ja käsiteltävien tietojen formaatti.

B.3.5 Turvallisuus- ja toimivuustarkastus sekä mittaukset

Vastaanottotarkastuksesta vastaavan yksikön tulee varmistua laitteen vaatimustenmukaisuudesta. Tämä voidaan todeta seuraavilla tavoilla.

A. Oma tarkastus
   Tehdään tarpeelliseksi katsotut mittaukset ja laaditaan vastaanottopöytäkirja. Turvallisuustarkastusmittaukset perustuvat yleisesti sähköturvallisuuden toteamiseen, mutta vastaanottotarkastuksen aikana voidaan tehdä myös erilaisia suorituskykymittauksia.

B. Laitetoimittajan vakuutus
   Laitteen mukana toimitetaan jonkun hyväksytyn tarkastuslaitoksen myöntämä lausunto ja mittaustulokset. Arvioidaan lausunnon ja mittauspöytäkirjojen sisältö ja yhdenmukaisuus toimitettuun laitteeseen nähden.

C. Pyynnöstä tehdyllä ulkopuolisen tarkastuslaitoksen tekemällä tarkastuksella
   Laitetoimittajan tai terveydenhuollon yksikön edustaja ottaa yhteyttä ulkopuoliseen tarkastuslaitokseen, jonka kanssa sovitaan tarkastusmenettelystä ja standardeista, jonka mukaan tarkastus tehdään.

Vastaanottotarkastuksesta tehdään aina pöytäkirja (malli liitteessä F). Mikäli laitteen vaatimustenmukaisuuden toteamiseen käytetään kohtia B tai C niin menettelytapa kirjataan pöytäkirjaan ja kyseinen lausunto ja mittauspöytäkirja liitetään vastaanottotarkastuspöytäkirjan liitteeksi.

Koekäyttöön tuleville laitteille suoritetaan tarpeelliset mittaukset tai muulla tavoin varmistutaan laitteen turvallisuudesta. Tämän jälkeen laite toimitetaan koekäyttöön. Laitteen toimittajan on annettava käyttökoulutus ennen laitteen käyttöönottoa. Mikäli koekäytössä oleva laite ostetaan, sille suoritetaan normaali vastaanottotarkastus. Mittauksia ei tarvitse toistaa, mikäli mittaustulokset on talletettu aiemmin ja koekäyttö ei ole heikentänyt laitteen ominaisuuksia.

B.3.5.1 Ohjelmiston vaikutus

Nykyaikaisen lääkintälaitteen tai laitejärjestelmän rakenne on lähes poikkeuksetta sellainen, että sen toimintoja ohjaa ja käsittelee jonkinlainen keskusyksikkö. Keskusyksikkö (standardi PC) voi olla integroitu

lääkintälaitteeseen. Se voi myös olla oma lääkintälaitteen sisällä oleva älykäs mikrosiru, joka kykenee hallitsemaan huomattavan määrän laskentatoimituksia, jotka johdetaan potilaasta mitatuista parametreistä. Samanaikaisesti mikrosiru voi käsitellä ja ohjata käyttäjän antamia näppäinpainalluksia lääkintälaitteen konsolilta. Laajimmillaan lääkintälaitteen ns. 'äly' saatetaan ladata lääkintälaitteeseen keskustietokoneelta lähiverkon kautta. Kaikkia näitä toimintoja pyörittää valtava määrä ohjelmakoodia.

Standardi SFS-EN 60601-1-4 käsittelee ohjelmoitavaa elektroniikkaa sisältävien lääkintälaitteiden turvallisuutta. Standardin painopiste on ohjelmiston kehityksen elinkaaressa ja järjestelmällisessä riskienhallinnassa, joiden avulla voidaan vähentää järjestelmällisiä virheitä ohjelmiston kehitystyössä. On selvää, että ohjelmiston testaaminen valmiista tuotteesta vastaanottotarkastuksen yhteydessä on mahdoton tehtävä ja huolellisenkin tarkastuksen tai arvioinnin jälkeen ohjelmistosta saattaa löytyä piileviä virheitä.

Vastaanottotarkastusta voisi tehostaa huolellinen käytön arviointi, jossa käyttäjien kanssa käytäisiin läpi laitteen toiminnan kannalta merkittävimmät toiminnot. Tällainen käytön arviointi edellyttää huolellista valmistelua ja yhteistyötä käyttäjien ja laitetoimittajan kanssa. Työmäärää lisää vielä se, että eri laitetyypeille tarvittaisiin erilaisia tarkastusproseduureja. Pidemmällä aikavälillä panostus voisi olla kannattava.

B.4 Käyttöönotto

Koska uuden laitteen tai laitejärjestelmän hankinta aiheuttaa aina erilaisia tarpeita käyttöorganisaatiossa niin käyttökoulutuksen kuin huoltojenkin suhteen, tulee vastaanottotarkastuksen yhteydessä järjestää käyttökoulutus ja määritellä erilaisten tarvikkeiden ja huoltojen tarve sekä nimetä siihen soveltuvat henkilöt.

B.4.1 Käytön vastuuhenkilö

Käytön vastuuhenkilö on se henkilö, joka tulee vastaamaan laitteen käyttökoulutuksesta ja myöhemmästä koulutustarpeesta kyseiselle laitteelle. Laitteen käytön vastuuhenkilö määritellään vastaanottotarkastusyksikön ja laitteen käyttöpaikan henkilöstön kesken. Vastaanottotarkastuksessa liitetään laitteen mukana meneviin asiakirjoihin vastuuhenkilön nimi ja yhteystiedot.

B.4.2 Käyttökoulutus

Vastaanottotarkastuksesta vastaavan yksikön tulee järjestää yhteistyössä laitteen toimittajan ja laitteen käyttöpaikan henkilöstön kanssa käyttökoulutus, jossa käsitellään kaikki laitteen turvallisen toiminnan ja käytön kannalta oleelliset asiat. Käyttökoulutusta varten voidaan etukäteen laatia lista niistä asioista, jotka askarruttavat käyttöhenkilökuntaa eniten tai aiheuttavat mahdollisia vaara- tai riskitilanteita potilaalle tai käyttäjälle. Valmis lista lähetetään laitteen toimittajalle, joka voi suunnitella kyseisen listan mukaisen käyttökoulutuksen, jolloin siitä saadaan sisällön suhteen mahdollisimman tehokas. Käyttökoulutukseen tulee osallistua myös laitteen huollosta vastaavat henkilöt.

B.4.3 Huoltotoimet

B.4.3.1 Käyttöhuolto

Käyttökoulutuksessa tulee selvittää ne rutiinitoimenpiteet ja normaalit käyttöhuollot, joita laitteen käyttäjä joutuu normaalin käytön aikana laitteelle tekemään (esim. suodattimien, paristojen ja tarvikkeiden vaihdot). Laitteen käyttöhuolloista vastuussa oleva(t) henkilö(t) määritellään vastaanottotarkastusyksikön ja laitteen käyttöpaikan henkilöstön kesken. Vastaanottotarkastuksessa liitetään laitteen mukana meneviin asiakirjoihin käyttöhuolloista vastuussa olevan henkilön nimi ja yhteystiedot.

B.4.3.2 Huollon vastuuhenkilö

Huollon vastuuhenkilö vastaa laitteen tai järjestelmän huollosta, korjauksesta tai muutoksista. Vastuuhenkilö määritellään vastaanottotarkastusyksikössä. Vastaanottotarkastuksessa liitetään laitteen mukana meneviin asiakirjoihin huolloista vastuussa olevan henkilön nimi ja yhteystiedot.

Huollon vastuuhenkilöllä on oltava riittävä pätevyys korjata vastuulleen kuuluvia laitteita ja järjestelmiä, mikä käytännössä tarkoittaa käyttökoulutusta ja laitetoimittajan järjestämää huoltokoulutusta. Pidetyistä kursseista lisätään maininta henkilön koulutusrekisteriin.

B.4.3.3 Määräaikaishuolto

Määräaikaishuoltoa vaativille laitteille avataan vastaanottotarkastuksen yhteydessä myös ns. määräaikaishuoltoloki. Määräaikaishuolto toteute-

taan hankintasopimuksessa sovitulla tavalla. Määräaikaishuollot tulee suunnitella yhdessä laitetoimittajan kanssa. Samassa yhteydessä sovitaan myös huoltojen tekijät ja vastuukysymykset siitä, että kuka huoltoja voi tehdä ja miten ne vaikuttavat laitteen takuuehtoihin.

Laitteen käyttäjän (osasto) on vastaanottotarkastuksesta vastaavan yksikön kanssa sovittava siitä, että kuka laitteelle tekee määräaikaishuollot (akkujen tarkistus ja vaihto, kalibrointi, turvallisuustarkastukset). Mikäli laitteelle tai järjestelmälle ei ole hankinnan yhteydessä määritelty määräaikaishuoltoa tai kunnonvalvontaa jää huoltojen määrittely teknisestä vastaanotosta vastaavan tahon tehtäväksi. Määräaikaishuolloissa tehtävät mittaukset on suoritettava aina kalibroiduilla mittalaitteilla.

B.4.3.4 Huoltosopimukset

Monet laitetoimittajat tarjoavat toimittamilleen laitteille erilaisia huoltosopimuksia, joilla taataan laitteen toiminta hyvin pienillä toimitusajoilla. Useissa tapauksissa nämä voivat olla hyvin järkevä vaihtoehto. Terveydenhuollon yksiköiden tulisi lisätä huoltosopimuksiin vaatimus, että laitteet ja laitejärjestelmät täyttävät huoltojen, korjausten ja muutosten jälkeen säädösten ja standardien vaatimukset sekä tarvittavat suorituskykyvaatimukset.

B.4.3.5 Huoltohistoria

Laitteen tai laitejärjestelmän vastaanottotarkastuksen yhteydessä laitteelle avataan ns. huoltotiedostoloki, joka voi olla elektroninen (erilaiset tietokannat) tai pelkkä kansio, johon sijoitetaan ko. laitteen vastaanottotarkastuksessa syntyneet tiedot ja huoltomanuaalit tai viite mistä kyseiset paperit löytyvät (huom. elektroninen rekisteri). Vastaanottotarkastuksen yhteydessä lisätään käyttäjille meneviin asiakirjoihin laitetta korjaavan ja huoltavan henkilön tai yrityksen nimi ja yhteystiedot.

Huoltohistoriaan lisätään kaikki laitteelle tehdyt toimenpiteet sisältäen korjaukset, muutokset, päivitykset ja tekijän tai tahon kuka toimenpiteen on tehnyt. Huoltolokissa tulisi soveltuvissa tapauksissa kuvata myös tehdyn toimenpiteen hyväksyntä ja perustelu hyväksynnälle. Perustelu voi olla testiraportti tai mittaustulos.

B.4.4 Muutokset ja päivitykset

Muutokset tuotteessa sen elinkaaren aikana ovat hyvin tavallisia. Muutoksilla valmistaja pyrkii esimerkiksi parantamaan tuotteen suorituskykyä, lisäämään tuotantomääriä, alentamaan tuotantokustannuksia, parantamaan tuotteensa kestävyyttä tai lisäämään uusia ominaisuuksia tuotteeseensa markkinoiden vaatimuksesta.

Valmistajan tulee aina kunkin tuotemuutoksen kohdalla harkita vakavasti muutoksen vaikutuksen seuraamusta tuotteeseen, sen ominaisuuksiin tai tuotantoon. Tuoteluokasta ja muutoksen laajuudesta riippuen on valmistajan tarvittaessa ilmoitettava muutoksesta myös ilmoitetulle laitokselle, joka käynnistää tarvittavat toimenpiteet vaatimustenmukaisuuden arvioimiseksi.

Muutokset kohdistuvat yleensä tuotteen rakenteen, materiaalien, tuotannon tai ominaisuuksien muutokseen, jotka voivat aiheuttaa välittömästi muutoksia esimerkiksi tuotteen mekaanisessa rakenteessa, sähköturvallisuudessa, kudosyhteensopivuudessa, suorituskyvyssä. Valmistajan tulee huolehtia myös uuden muutetun tuotteen vaatimustenmukaisuuden säilymisestä riskianalyysin, kliinisen tutkimuksen, sähköturvallisuustestien ja suorituskykymittausten avulla.

Muutos aiheuttaa myös huomattavan dokumentointitarpeen. Muutokset tuotteessa, tuotannossa ja suorituskyvyssä sekä vaatimustenmukaisuuden täyttyminen tulee dokumentoida. Muutoksessa ei saa myöskään unohtaa tuotteen mukana seuraavien asiakirjojen päivitystä.

Valitettavasti käytännössä on havaittu tapauksia, joissa laajojakaan muutoksia ei ole toimitettu ilmoitetulle laitokselle arvioitavaksi. Tästä syystä käyttäjäorganisaatiolla tulisi olla valmiudet osata kysyä muutoksen vaatimustenmukaisuuden osoittamisessa tarvittavia dokumentteja (tuotteen tekninen tiedosto tai osia siitä). Liitteessä G on esimerkki tuotteen teknisestä tiedostosta.

B.5 Lähteet

1.	SFS-KÄSIKIRJA 139 Pienjännitesähköasennukset SFS 6000:1999
2.	EN 60601-1 Medical electrical equipment. Part 1: General requirements for safety (IEC 601-1:1988+ A1:1991+ A2:1995 + corrigendum June 1995+ A13:1995)
3.	EN 60601-1-1 Medical electrical equipment. Part 1-1: General requirements for safety. Collateral standard: Safety requirements for medical electrical systems (2000)
4.	EN 60601-1-4 Medical electrical equipment - Part 1-4: General requirements for safety. Collateral standard: Programmable electrical medical systems (IEC 60601-1-4:1996 + Amd.1:1999)
5.	Guidance for the Content of Premarket Submissions for Software Contained in Medical Devices, FDA (1998)
6.	Jari Knuuttila: Terveydenhuollon laadunhallinta. Radiologisen laitteen vastaanottotarkastus, Lääkelaitoksen julkaisusarja 1/2001
WWW-linkit	
Sähköverkon asennukset ja turvallisuus	http://www.tukes.fi/ http://www.tukes.fi/sahko_ja_hissit/esitteet_ja_oppaat/sahkoasennusten_maaraikaistarkastukset.html Hakusanat: lääkintätilojen sähköasennukset, lääkintätilat
Tietoverkon asennus ja hankinta	http://www.edu.ouka.fi/ohjeet/tverkot7.htm

LIITE C LAITEJÄRJESTELMÄN MÄÄRITTELY

C.1 Hankinnan vaiheistus

Lääkintälaitejärjestelmiin liittyvät hankinnat ovat hyvin laajoja niin työajan kuin myös kustannusten suhteen. Hankinnoista muodostetaankin yhä useammin projekteja, joihin sidotaan eri henkilöryhmiä pidemmäksi aikaa. Tällöin projekti voidaan jakaa eri osavaiheisiin ja kunkin vaiheen tavoitteet hyväksytään ns. katselmuskokouksissa. Katselmusten avulla voidaan havaita jo hyvin aikaisessa vaiheessa projektia mahdollisesti uhkaavat aikataululliset, taloudelliset tai valitusta teknologiasta johtuvat riskit.

Katselmusten tueksi voidaan laatia erilaisia tarkastuslistoja, joissa esitetään riittävä määrä erilaisia kysymyksiä hankinnan eri osa-alueille (kuva C1). Menetelmä ei täytä ns. riskienhallinnan muodollisia menetelmiä, mutta on riittävän tehokas löytämään mahdolliset ongelmakohdat.

***Kuva C1**. Laitteen elinkaaren eri vaiheissa huomioitavia seikkoja*

Mikäli kysymysten avulla löydetään hankintaa mahdollisesti vaarantavia ongelmia, voidaan niitä ruveta analysoimaan tarkemmin esimerkiksi seuraavien analyysimenetelmien avulla:

- elinjaksoanalyysi; kustannusten kartoitus tietyllä aikavälillä
- riskianalyysi; laitteen tai laitejärjestelmän toimintaan tai käyttöön liittyvien vaaratilanteiden kartoitus (sisältää myös tietoturvan)
- kliininen tutkimus; laitteen tai laitejärjestelmän vaikuttavuuden tutkiminen (usein erittäin pitkäkestoisia tutkimuksia, joten ne eivät välttämättä sovellu oikein hyvin hankintatilanteen aikaisten ongelmien kartoitukseen)
- käytettävyystutkimus; käyttöön ja koulutukseen liittyvien ongelmien kartoitus.

Hankintaa valmisteltaessa on syytä muistaa, että tässä vaiheessa ostajalla on täydet mahdollisuudet varmistaa hankinnan onnistuminen. Vastaanottovaiheessa tehtävät muutokset tai korjaukset tietävät aina kustannuksia jommallekummalle osapuolelle ja aikatauluviiveitä niin tilaajallekin kuin toimittajallekin.

C.2 Hankinnassa huomioitavia seikkoja

Hankinnan yhteydessä on vaikeaa muistaa kaikkia tarkistettavia ja selvitettäviä asioita. Taulukossa C1 (a-h) on lueteltu joitain kysymyksiä, joita on hyvä käydä läpi hankintaan liittyvän tarvekartoitus- tai määrittelyvaiheen aikana. Kysymyksiä voidaan lisätä ja muokata vapaasti ja ne on syytä tehdä tarkistuslistan muotoon, jolloin ne tukevat mahdollisimman hyvin hankintaa. Mikäli mahdollista, niin listaa tulisi käydä läpi myös mahdollisten laitetoimittajien kanssa. Taulukon kysymykset on pyritty laatimaan teknologiasta tai tekniikasta riippumattomiksi. Kukin käyttäjä voi lisätä taulukkoon omat yksityiskohtaisemmat kysymyksensä.

Taulukko C.1a Hankinnan suunnittelun aikana varmistettavia asioita

SÄÄDÖKSET, STANDARDIT JA MUUT SEIKAT	
KYSYMYS	OSOITUS
1.-4. Terveydenhuollon laitteita koskevien säädösten tarkoituksena on varmista, että suunniteltu laite tai järjestelmä täyttää sille asetut vaatimukset liittyen turvallisuuteen ja vaikuttavuuteen. Vaatimukset on koottu STM: päätöksen 1994:66 liitteeseen I : Olennaiset vaatimukset. Liitteen I olennaiset vaatimukset katsotaan täytetyn, jos suunnittelussa noudatetaan harmonisoitujen standardien vaatimuksia (esim. sähköturvallisuus EN 60601-1, ohjelmistot EN 60601-1-4 jne.) Valmistaja voi käyttää myös muita vaihtoehtoisia suunnitteluratkaisuja, mutta tällöin käytettyjen ratkaisujen tulee tuottaa yhtä turvallinen tuote kuin standardin mukaan suunniteltukin on (edellyttää aina tapauskohtaista arviota, voi olla joskus aikaa vievä tapa)	
1. Voiko valmistaja osoittaa järjestelmän ja sen osien vaatimustenmukaisuuden (CE -merkinnät ja ilmoitetun laitoksen sertifikaatit) 2. Onko kliininen näyttö laitteen tai järjestelmän vaikuttavuudesta käytettävissä (erityisesti uudet laitteet, materiaalit ja tutkimusmenetelmät)? 3. Onko järjestelmä hyväksytty standardin EN 60601-1-1 mukaan ? 4. Jos ei ole niin, miten osoitetaan riittävä turvallisuus ? 5. Onko järjestelmä hyväksytty standardin EN 60601-1-4 mukaan ? 6. Jos standardia EN 60601-1-4 ei ole sovellettu, niin miten osoitetaan riittävä turvallisuus ohjelmiston osalta ?	
7. Onko järjestelmän kaikista osista toimitettu riittävä dokumentaatio (käyttö, huolto, asennus, sopimukset, tekniset eritelmät, käyttötarvikkeet)? 8. Sisältääkö dokumentointi riittävän tarkat spesifikaatiot (kaikki laitteet, yksiköt, ohjelmistot, ympäristövaatimukset, laitteistovaatimukset, ohjelmistovaatimukset ja tietoverkkovaatimukset sekä tarvittaessa kaapelointi) ? 9. Onko dokumenteissa huomioitu järjestelmien tuomat vaatimukset ? 10. Onko dokumenteissa kuvattu jäännösriskit ?	
11. Onko järjestelmien asennuksissa huomioitu sähköverkon, televerkon, ilmanvaihdon, veden, rakenteiden edellyttämät vaatimukset	

Taulukko C.1b Hankinnan suunnittelun aikana varmistettavia asioita

JÄRJESTELMÄ	
KYSYMYS	OSOITUS
Standardin EN 60601-1-1 tarkoituksena on varmistaa yhteen kytkettävien laitteiden turvallisuus. Perusajatuksena on varmistaa sähköturvallisuus. Sähköturvallisuuden varmistamiseksi riittää, että kukin laite on oma standardiryhmänsä vaatimusten mukainen. Ongelmana voi usein olla se, että määrittelyissä määritellään esim. tietokoneet sijoittavaksi hoitoalueen ulkopuolella. Tällä määrittelyllä riittää tietokoneelle, että se täyttää standardin EN 60950 vaatimukset. Käytännössä lääkintätilan hoitoalue ei ole mitenkään yksiselitteinen määritelmä ja pahimmassa 'hoitoalue' pienessä leikkaussalissa siirtyä jonkin verran, jolloin tietokone 'siirtyy hoitoalueelle'. Tässä tapauksessa tietokoneen tulee täyttää standardin EN 60601-1-1 vaatimukset.	
12. Onko järjestelmien rajapinnat määritelty (mitkä osat kuuluvat järjestelmään ja mitkä ei, entä tietoverkot)?	
13. Onko muiden laitteiden (ei-lääkintälaitteet) käyttöohjeistus riittävä ?	
14. Onko huomioitu yhteiskäytön aikana mahdollisesti kasvaneet vuotovirrat?	
15. Soveltuvatko laitteet käytettäväksi lääkintätiloissa tai osana lääkintälaitejärjestelmää?	
16. Kestävätkö muut laitteet (kotelointi ja materiaalikestävyys) lääkintätiloissa edellytettävää puhdistusta, sterilointia ja desinfiointia ?	
17. Kattaako riskianalyysi järjestelmän ja kaikki sen laitteet ? 18. Voiko järjestelmän laitteiden sijoittelu huonontaa tiloissa tapahtuvaa hoito/tutkimustyöskentelyä tai puhdistusta ? 19. Voiko järjestelmän kaapelointi aiheuttaa erillisiä vaaratilanteita (sijoittelunsa takia, väärien kytkentöjen takia tai vaurioitumisen takia) ? 20. Onko järjestelmän alasajo selvitetty käyttö- ja huoltohenkilökunnalle (esim. hätätapauksissa järjestelmän ohjelmallinen alasajo ja jännitteettömäksi tekeminen) ? <u>Huomautus</u> Riskianalyysiä on syytä kysyä laitetoimittajalta erityisesti isojen muutosten tai päivitysten yhteydessä. Analyysin on katettava yhteiskäytön mukanaan tuomat riskit sekä virheellistä käytöstä aiheutuvat seuraukset	

Taulukko C.1c Hankinnan suunnittelun aikana varmistettavia asioita

ASENNUS, KORJAUS JA MÄÄRÄAIKAISHUOLLOT	
KYSYMYS	OSOITUS
Asennusten, korjausten ja määräaikaishuoltojen avulla on tarkoitus varmistaa, että laite tai järjestelmä täyttää asetetut turvallisuus-, suorituskyky- ja toiminnalliset vaatimukset. Mittaukset eivät välttämättä paljasta puutteita vaatimusten mukaisuudessa. Tässä tapauksessa käyttäjän tulisikin laatia omat hankinta- ja määräaikaishuolto-ohjeensa sellaisiksi, että mittauksissa huomioitaisiin myös turvallisuusvaatimukset.	
21. Toimitetaanko järjestelmästä riittävät asennusohjeet ? - Tilavaatimukset (kosteus, lämpö, rakenteiden kestävyys), - Sähkönsyötön (isolointi, tehonkesto, ylivirtasuojaus, toimiiko ylivirtasuojat normaalikäytössä, onko valmistaja pyrkinyt estämään ylivirtasuojien tahattoman laukeamisen, mitä riskejä voi aiheutua ylivirtasuojien laukeamisesta?) - Kaapelointi (sähköverkko, tietoliikenne, potilaspaikat, valvomot), - Sijoitus (lääkintätilat, ryhmäkeskukset, valvomot joilla varmistetaan esim. riittävä käytettävyys, turvallisuuteen, suorituskyky, puhdistettavuus, tietoturva jne.)	
22. Ovatko ohjeet riittävät asennusmittausten tekemiseksi, jos niitä tekee muu kuin laitetoimittaja (Huom.: Osa ym. seikoista tulisi määritellä jo hankintavaiheessa)?	
23. Täyttääkö koko järjestelmä tarvittavat EMC-vaatimukset ? 24. Täyttyykö EMC–vaatimukset edelleen asennusten ja korjausten jälkeen ? <u>Huomautus</u> Lähes kaikki yksittäiset laitteet täyttävät EMC –vaatimukset, mutta kun laitteita kytketään toisiinsa niiden EMC -ominaisuudet voi muuttua. Lisäksi IT –laitteiden tulisi hoitoalueella olla standardin EN 60601-1 edellyttämällä tasolla, jolloin noudatetaan standardin EN 60601-1-2 vaatimuksia. Lääkintälaitteiden ja muiden laitteiden EMC–vaatimukset eivät välttämättä vastaa toisiaan (testit voi olla samoja, mutta hyväksyntäkriteerit poikkeavat.	
25. Kuka saa huoltaa järjestelmän laitteita ?	
26. Onko huoltoon varattu riittävästi resursseja ja onko huoltohenkilökunnalla riittävä ammattitaito huoltaa hankittavaa järjestelmää [erityisesti uudet järjestelmät ja uudet teknologiata]?	
27. Miten tehtyjen korjausten jälkeen varmistetaan laitteen tai sen osan vaatimustenmukaisuus ja suorituskyky?	
28. Kuka saa asentaa ohjelmistoja ? 29. Salliiko laitetoimittaja käyttäjän asentavan omia ohjelmistoja järjestelmään (onko pohdittu riskejä) ? 30. Kuka valvoo ja miten tätä valvotaan ?	
31. Jos kalibrointi suoritetaan itse, onko organisaatiolla siihen tarvittavat resurssit ?	

ASENNUS, KORJAUS JA MÄÄRÄAIKAISHUOLLOT	
KYSYMYS	OSOITUS
32. Onko kalibrointien mittausepävarmuus määritelty asianmukaisesti ? 33. Edellyttävätkö tehtävät kalibroinnit myös kalibroituja mittalaitteita (onko mittalaitteiden kalibrointi kunnossa, onko huomioitu mahdolliset kustannusvaikutukset) ?	
34. Onko määräaikaishuollot määritelty ?	
35. Ovatko kaapelit asianmukaisessa kunnossa (esim. kaapeleiden vaippojen rikkoontuminen voi vaikuttaa järjestelmän vuotovirtojen tai sähkömagneettisten häiriöiden kasvamiseen) ?	
36. Siirtyvätkö hälytykset sinne minne pitääkin (valvomot, kirjoittimet jne.) ?	
37. Mikä on erotusmuuntajien kunto (mekaaninen kunto, ylivirtasuojat, neste jne.)?	
38. Miten erotusmuuntajat on sijoitettu (ei saa sijaita lattialla) ?	
39. Miten erotusmuuntajien käytetään (eihän erotusmuuntajaa ole ohitettu jostain syystä) ?	
40. Määritelläänkö järjestelmälle määräaikaishuolto tai tarkastukset, sen tekijät ja sisältö sekä aikataulut? 41. Sisältääkö määräaikaishuolto vaatimukset mekaaniselle turvallisuudelle (kantavat rakenteet, kiinnitykset, kuka vastaa jne.) ? 42. Sisältääkö määräaikaishuolto vaatimukset korroosiolle ja nesteiden sisäänpääsylle (vesi, veri tai muut nesteet erityisesti leikkaussaleissa käytettävät laitteet, kuka vastaa) ? 43. Sisältääkö määräaikaishuolto vaatimukset sähköturvallisuudelle, jossa tarkistetaan esim. laitteen eristysvälejä ja vuotovirtoja 44. Kuka saa suorittaa sähköturvallisuusmittaukset ? Mittaukset voivat koostua esimerkiksi seuraavista: - eristysvastusmittaukset - suojamaatiemittaukset - vuotovirtamittaukset - visuaalinen tarkastus	
45. Onko määräaikaishuoltojen, korjausten ja muiden toimintojen dokumentointitarve määritelty (jäljitettävyys, tarkkuus, käytetyt mittalaitteet) ?	

Taulukko C.1d Hankinnan suunnittelun aikana varmistettavia asioita

OHJELMISTOT	
KYSYMYS	OSOITUS
46. Onko ohjelmistot ja niihin liittyvät lisenssisopimukset määritelty riittävän tarkasti (käyttöjärjestelmät, sovellusohjelmat, ajurit, muut varusohjelmistot)? Huomautus Ohjelmiston määrittelyssä ei riitä pelkkä sovellusohjelman määrittely. Määrittelyssä tulee huomioida koko ohjelmistoarkkitehtuuri, erityisesti määrittely on tärkeää hankittaessa uutta ohjelmistoa olemassa olevaan ohjelmistoarkkitehtuuriin. - laitteistoalusta (prosessori, emolevysarja, välimuistivaatimukset, keskusmuistin-määrä ja tyyppi) - käyttöjärjestelmä (tyyppi, versio, kieliversio) - sovellusohjelmat (ohjelmointikieli, päiväysasetukset, aikaformaatit, kielivaatimukset, tärkeää erityisesti tietokantasovelluksissa) - kolmannen osapuolen ohjelmistojen käyttö (tarvitaanko niitä. Mitä ne ovat esim. COTS –komponentit?) - käytettyjen tietoverkkoratkaisujen asettamat vaatimukset - ohjelmistosta johtuvat laiterajoitukset - vastuun jako ja vastuuhenkilöt.	
47. Onko ohjelmiston kieliversiolla vaikutusta toimintaan ?	
48. Sisältääkö järjestelmä COTS-komponentteja ja jos sisältää niin mitä ?	
49. Onko sovelluksessa sellaisia ohjelmia tai ohjelmayksiköitä, jotka kytkeytyvät tietoverkkoon tai palomuurin kautta muihin verkkoihin ?	
50. Salliiko ohjelmisto muunneltavuuden ja päivityksen ?	
51. Sallitaanko ohjelmiston uudelleenkäytettävyys ?	
52. Määritelläänkö ohjelmistolle testitapaukset, joilla varmistetaan ohjelmiston luotettava toiminta ? Huomautus Hankintavaiheen määrittelyssä tulisi ottaa huomioon myös mahdolliset päivitykset tai ohjelmistomuutokset ja niiden testaus. Testauksessa on huomioitava esimerkiksi käyttäjien määrä, avoimien tietokantayhteyksien määrä, tietoturvaratkaisut, hälytysrajat, oletusarvot sekä lokalisointiasiat.	
53. Voidaanko valmistajalta pyytää selvitystä käyttämistään ohjelmistoratkaisuista, joilla ohjelmiston kokonaisluotettavuutta pyritään parantamaan ? 54. Onko valmistaja luokitellut käyttämänsä suojatoimenpiteet teknologian, soveltuvuuden ja tehokkuuden mukaan.	

OHJELMISTOT	
KYSYMYS	OSOITUS
Huomautus Käytettyjä suojatoimenpiteitä voidaan määritellä esimerkiksi osaksi ohjelmoinnin tyylioppaita. Suojatoimenpiteet ohjelmistolle voivat olla seuraavanlaisia: - alustustoimenpiteet - virheenhallintarutiinien määrittely - minimoi samanaikaisesti auki olevien prosessien määrä - prosessien priorisointi - HW–varmistuksen käyttö kriittisten ohjelmistomoduulien suojaukseen - dynaamisen muistin käytön allokoinnin välttäminen, jos se vain on mahdollista - hyvin laaditut testitapaukset eli testaa ja verifioi 'tuplasti' ohjelmiston kriittiset toiminnot, kuten esimerkiksi suuri CPU–kuormitus, dynaaminen muistin allokointi, ajastukset, sanomanvälitys ja samanaikaisten prosessien käyttäytyminen - ohjelmistokehityksen ohjedokumenteissa tulisi huomioida myös tietoturvavaatimukset.	
55. Noudattaako valmistaja ohjelmistotuotannossaan mitään tunnettua ohjelmistotuotannon arviointimallia (esim. CMM, SPICE) ? Huomautus Valmistajan ohjelmistotuotantoprosessi tuottaa hyvin suurella todennäköisyydellä toistettavampaa ja luotettavampaa ohjelmistoa, jos valmistajalla on käytössään 'arvioitu ja rankattu' prosessi.	

Taulukko C.1e Hankinnan suunnittelun aikana varmistettavia asioita

WWW-SOVELLUKSET	
KYSYMYS	OSOITUS
56. Mitä www-palvelinta sovellus tarvitsee (IIS, Apache, joku muu) ? 57. Onko sovelluksissa huomioitu viimeisimmät tietoturvapäivitykset em. palvelimiin liittyen ?	
58. Edellyttääkö sovellus tietokantoja (onko tietokantojen vaikutus ohjelman luotettavuuteen arvioitu)?	
59. Tarkastetaanko sovellusten käyttäjätunnistus ?	
60. Sallitaanko paikallisten työasemien vastaanottaa tai käynnistää evästeitä tai skriptejä ?	
61. Rajoitetaanko www-sovellusten syötekenttien kokoa tai maksimipituuksia turvallisuusmielessä ?	
62. Eliminoidaanko syötekentissä mahdollisuus syöttää esim. php -koodia suoraan syötekenttään ?	
63. Jos käyttäjien salasanat talletetaan tietokantoihin, niin talletetaanko ne salattuina vai salaamattomina ?	
64. Suojataanko käyttäjätietokannat tahatonta tai tahallista muuttamista vastaan tai otetaanko tietokannoista varmuuskopioita ?	
65. Onko sovelluksessa sellaisia ajureita, jotka kytkeytyvät tietoverkkoon tai palomuurin kautta muihin verkkoihin ?	
66. Voidaanko lääkintälaitejärjestelmään kuuluvilta työasemilta avata www-yhteys?	
67. Käytetäänkö tietoturvaratkaisuissa tiedostovarmenteita ja onko niiden kopiointi tai muuttaminen mahdollista ?	

Taulukko C.1f Hankinnan suunnittelun aikana varmistettavia asioita

PÄIVITYKSET	
KYSYMYS	OSOITUS
68. Onko valmistaja toimittanut muutosselvityksen (mitä on muutettu, miksi on muutettu, kuka on muuttanut ja arvio muutoksen merkittävyydestä) ?	
69. Onko ilmoitettu laitos arvioinut muutoksen ja jos ei ole, niin millä perusteella muutosta ei ole arvioitu ?	
70. Aiheuttaako muutos uusia vaaroja, joita aiemmin ei ole käsitelty ? 71. Onko mahdolliset uudet jäännösriskit siirretty käyttöohjeisiin ?	
72. Muutetaanko tuotteen suorituskykyä, aiottua käyttötarkoitusta tai käyttötapaa ?	
73. Kattaako olemassa olevat kliiniset tiedot myös uudet ominaisuudet ?	
74. Onko edellisen ohjelmaversion räätälöinnit huomioitu muutoksessa tai päivityksessä ? 75. Kuka tekee uuden päivityksen räätälöinnit (jos muu kuin valmistaja tai valmistajan edustaja, niin onko vastuujako selvitetty)?	
76. Onko kieliversiot ja päivämääräasetukset vastaavat kuin vanhalla ohjelmaversiolla ?	
77. Onko muutoksesta tai päivityksestä toimitettu riittävät testaus-, verifiointi- ja validointiraportit ?	
78. Kattaako testaus myös suorituskykytestaukset ?	
79. Onko tietorakenteiden yhteensopivuus varmistettu ?	
80. Onko mukana seuraavat asiakirjat päivitetty päivitystä vastaaviksi (onko vanhat manuaalit poistettu käytöstä ja onko tästä tiedotettu käyttäjiä sekä huoltajia) ?	

Taulukko C.1g Hankinnan suunnittelun aikana varmistettavia asioita

TIETOTURVA	
KYSYMYS	OSOITUS
81. Onko organisaatiossa tehty tietojärjestelmien riskianalyysi, jonka perusteella on määritelty organisaation tietoturvapolitiikka ja käytetyt tietoturvaratkaisut (BS 7799-1, BS 7799-2)? Huomautus Analyysin on katettava myös käytettyjen ohjelmien ja laitteiden kartoitus. Onko ohjelmien tai laitteiden käytössä tapahtunut muutoksia ? Onko käytettyjen ohjelmien tai laitteiden tekniikoissa tapahtunut muutoksia, muutostilanne edellyttää aina uusintatarkastelua?	
82. Noudattavatko järjestelmän tietoturvaratkaisut organisaation tietoturvapolitiikkaa ?	
83. Onko tietoturvaratkaisujen käyttöönotolle laadittu riittävät ohjeet (johdon hyväksyntä, kriteerit, testaus, asennus, tiedottaminen ja koulutus) ?	
84. Onko käyttäjätietokantojen suojaamiseksi laadittu ohjeet (pääsyoikeudet, tietokantojen kirjoitussuojaukset jne.) ?	
85. Onko ohjelmistojen ja tietoturvaratkaisujen asennukseen riittävä ammattitaito ? Huomautus Useisiin ohjelmiin on nykyisin implementoitu huomattava määrä erilaisia tietoturvaominaisuuksia, mutta ohjelmistojen yhteensopivuuden varmistamiseksi nämä oletusarvoisesti jätetään kytkemättä päälle. Ohjelmistojen asentaminen next-next-next-next -tyylillä ei ota käyttöön ko. ohjelmistojen viimeisimpiä tietoturvaratkaisuja. Näiden palveluiden käyttöönotto edellyttää ohjelmistojen asentajalta huomattavaa ammattitaitoa.	
86. Ovatko järjestelmän tietoturvaratkaisut yhteensopivia organisaation omien tietoturvaratkaisujen kanssa ?	
87. Onko tietoturvaratkaisuissa huomioitu mm. mobiilitekniikan erityispiirteet, kuten esimerkiksi WebPadin käyttö, käyttäjän luokittelu, tiedon keruu sekä W-LAN- ja VPN –yhteydet ?	
88. Täyttääkö tietoturvaratkaisut säädösten vaatimukset?	
89. Suojataanko tiedostot ja tiedostoalueet riittävästi erityisesti niissä tapauksissa, joissa lääkintälaitejärjestelmät käyttävät yhteisiä levyalueita ?	
90. Käyttääkö yrityksen järjestelmämanagerit oletusarvoisesti määriteltyä 'Administrator' käyttäjätunnusta ? Huomautus Muuta 'Administrator' käyttäjätunnus joksikin muuksi ja seuraa lokeissa 'Administrator' käyttäjätunnukselle tehtyjä sisään kirjautumisyrityksiä.	
91. Käytetäänkö riittävän 'vaikeita' salasanoja ja 'pakotetaanko' käyttäjät vaihtamaan salasanaa riittävän usein ?	

TIETOTURVA	
KYSYMYS	OSOITUS
92. Estetäänkö lääkintälaitejärjestelmien tietokoneiden käynnistyminen levykkeiltä (BIOS–ominaisuus, käynnistyslohkovirukset) ?	
93. Käytetäänkö lääkintälaitejärjestelmän tietokoneita tutkimuskäytössä, jolloin esim. tutkimustuloksia siirretään tietokoneelta toiselle levykkeiden avulla ? 94. Tarvittaessa laadittava ohjeistus levykkeiden käytöstä	
95. Suojataanko työasemien levyjen käyttö ulkopuolisilta (estetään levyjen jako ulkopuolisilta käyttäjiltä) ?	
96. Voiko lääkintälaitejärjestelmien tietokantoja selailla erillisillä tietokantaselaimilla? 97. Jos näin voidaan tehdä, onko määritelty kuka sen saa tehdä ja onko se estetty muilta?	
98. Onko järjestelmässä olevien kannettavien mikrotietokoneiden tietoturvaseikat huomioitu asianmukaisesti ?	
99. Onko järjestelmän sijaintipaikkaan estetty pääsy sivullisilta ?	
100. Valvotaanko järjestelmän sijoituspaikkaa esim. kulunvalvonnalla ?	
101. Mahdollistaako kulunvalvonta lokitiedostojen keruun ?	
102. Onko tietoverkon vapaat seinäpistorasiat kytketty tietoliikennekeskuksen tai -kaapin toistimilla tai kytkimillä ? <u>Huomautus</u> Yleisissä oleskelutiloissa tai kahvioissa saattaa olla lähiverkkopistokkeita, joiden kautta ulkopuolinen taho voi kytkeytyä talon lähiverkkoon	
103. Voidaanko lääkintälaitejärjestelmän tietokoneilta lähettää tai vastaanottaa sähköposteja tai onko niihin asennettu www-selaimia, joilla voidaan ottaa yhteys joko sisäiseen tai ulkoiseen verkkoon (jos näin voidaan menetellä, onko siitä aiheutuvat riskit analysoitu)?	
104. Onko lääkintälaitejärjestelmän tietojen varmuuskopiointi ohjeistettu (kuka, mitä, milloin) ?	
105. Onko käytetyt tietoturvaratkaisut ohjeistettu riittävästi ?	
106. Onko ulkomaailmaan kytkeytyvät ohjelmat kartoitettu ?	
107. Seurataanko näiden ohjelmien tietoturvakehitystä aktiivisesti ?	
108. Onko selaimien, palomuurien ja virussuojausten asetukset, sekä päälläolo tarkistettu?	
109. Pidetäänkö lokitiedostoja, tarkastetaanko ja seurataanko niiden sisältöä säännöllisesti?	
110. Käytetäänkö laitteiden välisissä yhteyksissä salaamattomia yhteyksiä (telnet, ftp)?	

TIETOTURVA	
KYSYMYS	OSOITUS
111. Käytetäänkö virussuojaustyökaluissa viimeisimpiä versioita ?	
112. Suoritetaanko sovellusohjelmien syötteiden tarkastus riittävän kattavasti (esim. www-sovelluksissa syötekenttiin saatetaan syöttää PHP –koodia tai syötekenttään syötetään liian pitkä merkkijono, jolla aiheutetaan puskurin ylivuoto) ?	
113. Tarkastetaanko sovellusten käyttäjätunnistus sekä evästeiden luonti ?	
114. Voidaanko lääkintälaitejärjestelmien tietokantoja selata tietokantaselaimilla (sovellus voi olla erikseen salasanasuojattu, mutta tietokantaan päästään käsiksi tietokantaselaimilla (toisaalta näin pitää voida tehdäkin, mutta pitää määritellä kuka näin saa tehdä -> tiedon luottamuksellisuuden mielessä tai tiedon saatavuuden ja luotettavuuden mielessä) ?	
115. Onko tiedon hävitykselle määritelty ohjeet (tiedon hävitys, missä tietoa sijaitsee ja miten se hävitetään) ?	

Taulukko C.1h Hankinnan suunnittelun aikana varmistettavia asioita

KÄYTETTÄVYYS	
KYSYMYS	OSOITUS
Käytettävyys tarkoittaa sitä tehokkuutta, hyötyä ja tyydytystä, jolla määrätyt käyttäjät voivat saavuttaa tietyt päämäärät tietyissä ympäristöissä. (ISO 9241) Toisin sanoen käytettävyyden tarkoituksena on varmistaa tuotteen soveltuvuus suunniteltuun käyttötarkoitukseen siten, että sen käyttö ei tuota tai aiheuta tarpeettomia vaaratekijöitä. Toisaalta käytettävyyden tulisi osaltaan myös estää tarpeettomien vaaratekijöiden toteutumista. Ensisijaisesti käytettävyyden tulisi ohjailla ja ratkaista ainakin seuraavia tekijöitä: - Tuotteen tulee soveltua suunniteltuun käyttötarkoitukseen (vaikuttavuus, suorituskyky). - Tuotteen käyttö (tuotteen ja käyttäjän välinen kommunikointi, helppokäyttöisyys, mukavuus, tehokkuus, ymmärrettävä MMI niin nappuloiden, mekaniikan kuin ohjelmistonkin suhteen). - Tuotteen suunnitteluprosessissa käytettävyys tulee sijoittaa erääksi suunnittelun lähtötiedoksi (käyttäjän tarpeista lähtevä suunnittelu, käyttäjän tarpeet vs. lopputuote). - Usein tuotteiden suunnittelussa ei kuitenkaan oteta käytettävyyttä riittävästi huomioon, koska suunnittelijat eivät välttämättä tunne riittävän hyvin sovellusaluetta, ympäristöä tai käyttötilannetta. - Lisäksi käytettävyydelle ei vielä olla määritelty selkeitä vaatimuksia, jotka suunnittelijat voivat noudattaa tuotteen suunnittelussa. (Käytettävyydelle on valmisteilla uusi standardi IEC 60601-1-6).	
116. Onko laitteet tai laitteistot suunniteltu siten, että ergonomiset tekijät eivät aiheuta ylimääräisiä vaaratekijöitä (työasennot, selkokielisyys, kieli, ympäristötekijät jne.) ?	
117. Onko uudet laitteet tai järjestelmät yhteensopivia vanhempien laitteiden tai laitteistojen kanssa ?	
118. Onko käyttöhenkilökunnan tai huoltohenkilökunnan osaaminen riittävää uusien laitteiden ja laitteistojen osalta ?	
119. Onko laitteissa käytetyt näppäimet, merkistöt, symbolit ja äänet sellaisia, että kaikki käyttäjäryhmät ymmärtävät yksiselitteisesti niiden toiminnan ?	

C.3 Lähteet

1. EN 60601-1 Medical electrical equipment - Part 1: General requirements for safety (IEC 601-1:1988, A1:1992, A11:1992, A12:1992)

2. EN 60601-1-4 Medical electrical equipment – Part 1-4: General requirements for safety. Collateral standard: Programmable electrical medical systems (IEC 60601-1-4:1996 + A1:1999)

3. IEC 60601-1-6 (Draft) Medical Electrical Equipment – Part 1-6: General requirements for safety. Collateral standard: Usability: Analysis, test and validation of human factors compatibility

4. BS 7799-1:fi Tietoturvallisuuden hallinta. Osa 1: Tietoturvallisuuden hallintajärjestelmiä koskeva menettelyohje

5. BS 7799-2:fi Tietoturvallisuuden hallinta. Osa 2: Tietoturvallisuuden hallintajärjestelmiä koskevat vaatimukset

LIITE D OHJELMISTON TESTAUSKOHTEITA

D.1 Käyttäjän suorittama testaus

Ohjelmiston testaus voidaan suorittaa joko käyttäjän toimesta tai yhteistyössä käyttäjän ja laitetoimittajan kanssa. Käyttäjän tulee huomioida, että täydellistä testausta ei voi hankintavaiheessa edellyttää ja osa testeistä voi rikkoa laitetta tai aiheuttaa tiedostojen korruptoitumista.

Testitapaukset, hyväksyntäkriteerit ja niiden raportointi tulee suunnitella huolella yhteistyössä valmistajan tai maahantuojan kanssa. Alustava testaussuunnitelma tulee laatia jo hankinnan määrittelyvaiheessa. Sitä voidaan päivittää asennuksen ja käyttöönoton yhteydessä. Seuraavanlaisia testejä voidaan kuitenkin edellyttää, kunhan ne on määrittelyvaiheessa sisällytetty osaksi asennusta ja vastaanottotarkastusta:

- Toiminto- ja suorituskykytestaus, kattaen kaikki tarvittavat toiminnot ja toimintosekvenssit (muista tarkastaa indeksointien toimivuus muutostilanteissa kuten alustukset eri sekvensseihin, uuden potilaan asettelu jne.).
- Tulo- ja lähtöalueiden testaus (raja-arvot ja syötteen laatu).
- Lääkintälaitteiden hälytykset eivät saa häiriintyä muiden laitteiden toimesta. Voidaan tarkastaa normaalissa käyttötilanteessa useiden eri laitteiden yhtäaikaisella käytöllä. Hälytykset eivät saa myöskään kadota. Tee riittävä määrä hälytyksiä. Hälytyksiä ei voi ohjata pois päältä toiselta laitteelta.
- Laitteen käynnistyessä hälytysten ja mittaustoimintojen (default values) tulee olla suunniteltu siten, että laitteen turvallinen toiminta on taattu jo käynnistymisestä alkaen. Hälytysten estäminen oletusarvona ei saa aiheuttaa riskiä, muussa tapauksessa hälytyksen tulee olla aktivoituna.
- Ei-lääkintälaitteet eivät saa ohjata lääkintälaitetta vaaralliseen tilaan normaalissa käyttötilanteessa eikä yhden vian tapauksessa.
- Vikatilanteessa potilaan tilan indikointi tulee estää.
- Lääkintälaitteen antojen aktivoitumiset virhetilanteissa tulee estää.
- Laitteen toimintojen palauttaminen turvalliseen tilaan, laitteen suorittaessa uudelleen käynnistystä.
- Ohjelmiston turvallinen toipuminen sähkö- tai tietoverkon katkoksista.
- Lokalisointitestaus (päivämäärät, aikavyöhykkeet, näppäimistöt ja skandinaaviset merkistöt).

Erityisesti tietokantasovelluksissa tulee huomioida kansalliset erikoismerkit (Ää, Öö, Åå). Mikäli kansallisia erikoismerkkejä ei määritellä oikein, voi erilaisissa raporteissa ja hakutoiminnoissa esiintyä ongelmia tai toimimattomuutta. Kansalliset merkistöt voidaan määritellä ns. tietokantamoottoreiden kieliasetuksissa. Mikäli kieliasetuksia ei määritellä, voi kieliasetuksiksi oletusarvoisesti tulla käyttöjärjestelmässä määritelty kieli (riippuu käyttöjärjestelmästä ja käytetystä tietokanta-ajurista). Päiväysasetukset voivat aiheuttaa myös sovelluksen toimimattomuutta ja tämä tulee ottaa huomioon asennuksen aikana tehtävissä suorituskykytestauksissa. Lokalisointiasia on oikeastaan hankintavaiheen määrittelykysymys.

D.2 Laitetoimittajan suorittama testaus

Käyttäjän hyväksyessä valmistajan tai maahantuojan testausraportit, tulee raporttien sisältää versiotunnisteet ohjelmistolle ja testitulosten tulisi soveltuvin osin sisältää perustelu siitä, kuinka seuraavat kohdat on testattu:

- vikakorjaukset
- oletusarvot ja hälytykset, virheet, aluetarkistukset ja raja-arvojen testaus
- kieli ja muut lokalisointitekijät
- mittausalgoritmien testausohjeet
- kuormitustestaus (maksimikäyttäjät, avoimet tiedostot, avoimet tietokantayhteydet)
- laitteen optiot, tarvikkeet ja kokoonpanon testaus, rajapinta- ja kommunikointitestaus
- muistin käyttötestaus
- kolmannen osapuolen (COTS) ohjelmistojen kelpuutus, hyväksyntätestaus.

LIITE E MÄÄRÄAIKAISHUOLTO JA KUNNONVALVONTA

Laitteiden ja laitejärjestelmien luotettavan toiminnan kannalta merkittävässä asemassa on säännöllisin välein suoritettu kunnonvalvonta ja määräaikaishuolto. Säännöllisellä määräaikaishuollolla pidennetään myös järjestelmän käyttöikää ja eliminoidaan mahdollisten äkillisten rikkoontumisten aiheuttamia toiminnan keskeytyksiä.

E.1 Visuaalinen tarkastus

Visuaalisella tarkastuksella voidaan järjestelmistä tarkastaa laitteen ulkoiseen kuntoon, oletusarvoihin, sijoitteluun ja puhdistukseen liittyviä seikkoja. Tarkastuskohteiksi voidaan valita ainakin seuraavia kohteita:

- Jos järjestelmään kuuluu useampia vuodepaikkoja ja jokaisessa vuodepaikassa on laitteita, niin onko liittimet ja kaapelit kytketty varmasti oikean potilaspaikan oikeisiin laitteisiin?
- Siirtyvätkö hälytykset sinne minne pitääkin (valvomot, kirjoittimet jne., hälytykset voi olla estetty tai syynä voi olla kaapeli- tai laitevika).
- Erottuvatko visuaaliset hälytykset kyllin selvästi (fonttikoot, värit jne.).
- Erotusmuuntajien kunto (mekaaninen kunto, ylivirtasuojat, neste jne.).
- Erotusmuuntajien sijoitus (ei saa sijaita lattialla).
- Erotusmuuntajien käyttö (eihän erotusmuuntajaa ole ohitettu jostain syystä?)
- Maadoitusten silmämääräinen tarkastus, erityisesti lisäsuojamaajohtimet.
- Kaapelointien, johtimien kunto ja sijoittelu.
- Oletusarvojen ja raja-arvojen tarkastus.

Huoltotietokansioon kirjataan kaikki visuaaliset havainnot, joilla saattaa olla merkitystä laitteen tai laitejärjestelmän käytön kannalta.

E.2 Sähköturvallisuus

Sähköturvallisuusmittauksilla varmistetaan järjestelmän sähköturvallisuus. Järjestelmän laajuudesta riippuen mittaukset voivat kattaa useita eri mittauksia, joilla taataan järjestelmän sähköturvallisuus. Sähköturvallisuuden varmistavat mittaukset voidaan kohdistaa seuraaviin kohtiin:

- jakeluverkon mittaukset
- vuotovirtamittaukset
- eristysvastusmittaukset
- kaapelien kunnon tarkastus (esim. kaapeleiden vaippojen rikkoontuminen voi vaikuttaa järjestelmän vuotovirtojen tai sähkömagneettisten häiriöiden kasvamiseen)
- liittimien ja kojevastakkeiden mekaaninen kunto (suoja nesteiden sisäänpääsyä tai kosketusta vastaan on huonontunut, mittaus voidaan tehdä eristysvastusmittauksin ja visuaalisin tarkastuksin)
- suojamaadoitusten tarkastus
- pinta- ja ilmavälien tarkastus jännitekokein (pinta- ja ilmavälien tarkastuksessa voidaan tehdä myös ns. silmämääräinen tarkastus, jossa etsitään laitteesta mahdollisia mekaanisia vaurioita tai lian ja nesteiden aiheuttamia pinta- ja ilmavälien huononemisia)
- korroosiovaikutukset.

E.3 Ohjelmistojen määräaikaishuollot

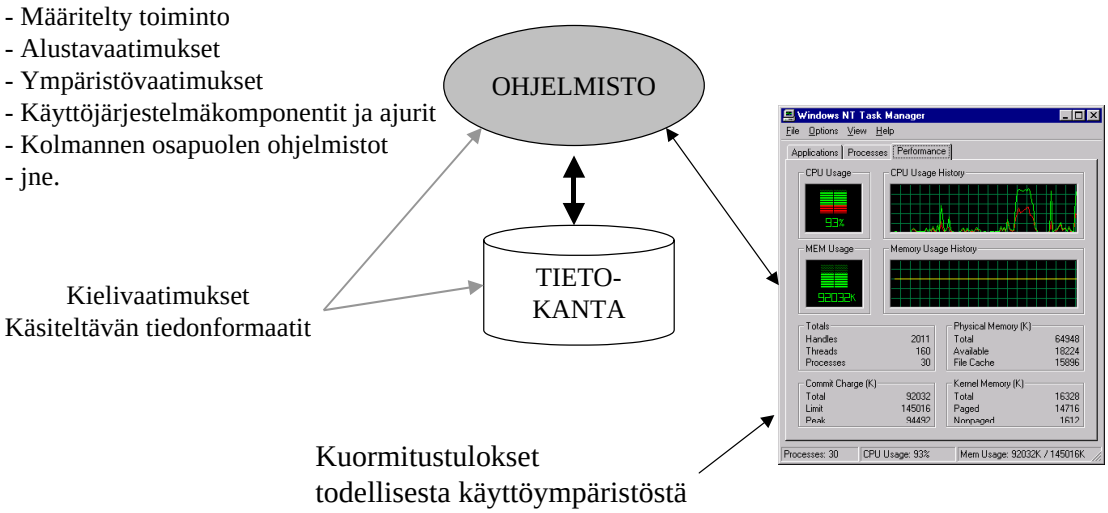
Ohjelmistojen määräaikaishuollot eivät ole niin merkittävässä osassa, koska toimiva ohjelmisto ei voi ilman muutoksia vikaantua tai alentaa laitteiston toimivuutta.
Määräaikaishuollot tai kalibroinnit ovat tärkeitä silloin, kun ohjelmiston avulla luetaan tai kerätään tietoa mittauslaitteilta ja mittauslaitteiden anturit tai elektroniikka edellyttää tietyin välein ohjelmallisesti suoritettavaa kalibrointia muuttamalla esim. mittausalgoritmien kertoimia. Näissä tapauksissa kalibroinneista on laadittava mittauspöytäkirja, johon kirjataan mittaustulosten lisäksi ohjelmiston ja laitteiston tyypit sekä versionumerot, olosuhteet, kalibroinnin tekijät ja käytetyt mittalaitteet.

Ohjelmistojen määräaikaishuolloissa voidaan tarkastaa ainakin seuraavia seikkoja:
- virustarkastus ja virusohjelmistojen versionumerot
- sovellusohjelmien versionumerot (nähdään onko käyttäjät tai joku muu taho tehnyt muutoksia järjestelmään)
- levyjen pirstoutuminen ja virheentarkastus
- muistitestit
- levytilan riittävyys
- lokien tarkastukset (mikäli lokitiedostoja tyhjätään välillä, muista arkistoida poistettavat tiedostot joko paperi- tai sähkömuodossa)
- järjestelmän ohjelmalliset oletusarvot
- hälytysten estot

- järjestelmän käyttäjämäärät verrattuna hankinnassa määriteltyihin käyttäjämääriin
- vasteajat (kyselyt, tallennukset, raportit, haut).

Ohjelmiston määräaikaishuoltoihin voidaan lisätä myös suorituskykymittaukset, joilla haetaan varmuutta, että laite täyttää sille asetetut suorituskyky- ja toiminnallisuusvaatimukset. Kuvassa E1 on esimerkki ohjelmiston kuormitustestauksesta ja testaukseen vaikuttavista tekijöistä. Mittaukset voivat sisältää:

- kuormitus- ja suorituskykymittaukset (prosessori, muisti, levy, tietoliikenne jne.)
- käytettävyyden varmistavia testejä (esim. käyttöliittymävaatimukset ja käyttöliittymien ns. personointi)
- toiminnallisuustestit (virheistä toipuminen, vikasietoisuus, väärinkäyttö, tietoliikenneverkon mittaukset).



***Kuva E1**. Ohjelmiston kuormitustestaus osana määräaikaishuoltoa*

E.4 Esimerkki sähköturvallisuusmittauksesta

E.4.1 Kuvaus

Seuraavassa on eräs esimerkki sähköturvallisuuden toteamiseksi tehtävästä kunnonvalvontamittauksesta. Järjestelmän sähkönsyöttö on vuotovirtojen rajoittamiseksi toteutettu erotusmuuntajien avulla. Tässä tapauksessa järjestelmän käynnistysvirta voi aiheuttaa johdonsuojaautomaattien laukeamisen.

Järjestelmätoimittajan tulisi rakentaa järjestelmä siten, että 16 A :n hitaimmat johdonsuojakatkaisijat eivät laukea. Vastaanottotarkastuksen tulisi tapauskohtaisesti arvioida johdonsuoja automaattien toimimisesta aiheutunut riski seuraavilta osin:

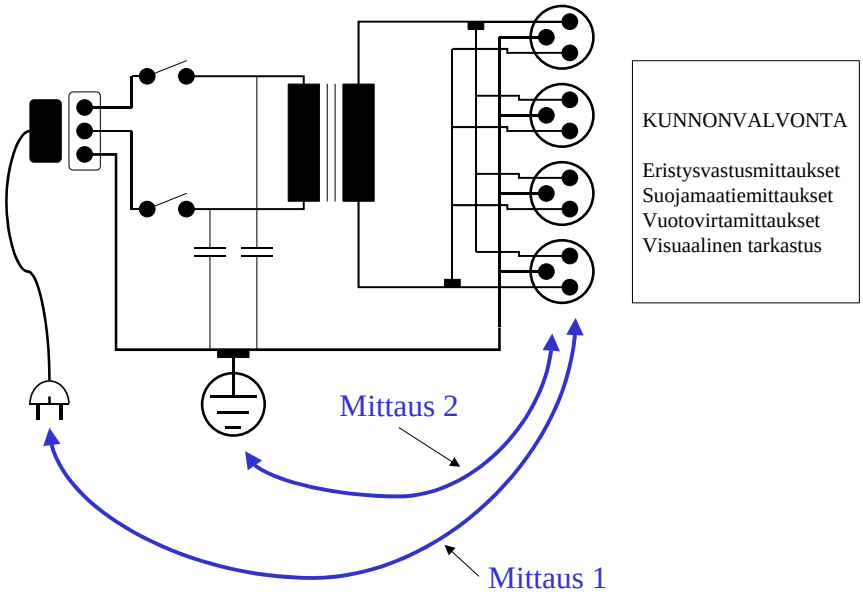
- Kuinka kriittinen sovellus on kyseessä ?
- Toimiiko ylivirtasuojat normaalikäytössä ?
- Onko laitetoimittaja pyrkinyt jollain tavoin pyrkinyt estämään ylivirtasuojien tahattoman laukeamisen ?
- Mitä riskejä voi aiheutua ylivirtasuojien laukeamisesta ?

E.4.2 Mittaus

Esimerkkimittauksessa varmistetaan muuntajan erotuskyky. Kuvassa E2 on esimerkki erotusmuuntajille suoritettavista tarkastuksista.

Mittaus 1: Mitataan erotusmuuntajan ensiöpiirin ja toisiopiirin välillä olevaa eristysvastusta eristysvastusmittarilla

Mittaus 2: Mitataan erotusmuuntajan toisiopiirin ja suojamaan välillä olevaa eristysvastusta eristysvastusmittarilla



***Kuva E2**. Erotusmuuntajalle suoritettava kunnonvalvontamittaus*

Tulokset kirjataan järjestelmän määräaikaishuolto tai kunnonvalvontalomakkeeseen. Tuloksiin kirjataan myös käytetyt mittalaitteet, joilla mittaukset on suoritettu. Kunnonvalvontamittaukset esimerkkitapauksessa voivat sisältää myös suojamaatien resistanssimittauksia, vuotovirtamittauksia tai visuaalisia tarkastuksia.

E.5 Mittauksista yleensä

Alla on kuvattu muutamia seikkoja, jotka on huomioitava kalibrointeja suoritettaessa:

- Kalibroinnissa käytettyjen mittalaitteiden on oltava kalibroituja.
- Muista päivittää laitekortti ja dokumentoida mittaukset ja havainnot.
- Tarkastuksia voidaan tehdä joko jännitetestein tai vuotovirtamittauksin.
- Jännitekokeita määriteltäessä on huomioitava, että liian korkeat testijännitteet vanhentavat laitteen eristeitä. Eristysvastusmittauksia voidaan tehdä esimerkiksi 500 V:n testijännitteellä.

Mikäli haluat tutustua tarkemmin kalibrointiin liittyviin tekijöihin ja esimerkiksi kalibroinnin epävarmuuden määrittämiseen tutustu www-sivuihin http://www.mikes.fi/. Sivuilta löytyy useita kalibrointiin ja kalibroinnin epävarmuuteen liittyviä julkaisuja.

E.6 Kirjallisuutta

1. Jari Knuuttila, Kaarle Kylmälä, Ilpo Pöyhönen: Terveydenhuollon laadunhallinta. Sähkökäyttöisten lääkintälaitteiden vuotovirtojen vertailumittaus. Lääkelaitoksen julkaisusarja 2/1998

2. Jari Knuuttila, Kylmälä Kaarle, Matti Liukko, Petri Pommelin: Terveydenhuollon laadunhallinta. Suuntaviivoja terveydenhuollon laitteiden kalibroinnille. Lääkelaitoksen julkaisusarja 2/1999.

LIITE F MALLI VASTAANOTTOTARKASTUS-PÖYTÄKIRJAKSI

VASTAANOTTOTARKASTUSPÖYTÄKIRJA

[JÄRJESTELMÄN NIMI]

F.1 Järjestelmän tunnistetiedot

Tunnistetietoihin lisätään kaikki se tieto, joka on merkityksellistä laitteen myöhemmän käytön kannalta sisältäen vastuukysymykset, koulutuksen, huollot, päivitykset sekä turvallisen ja suorituskykyisen käytön.

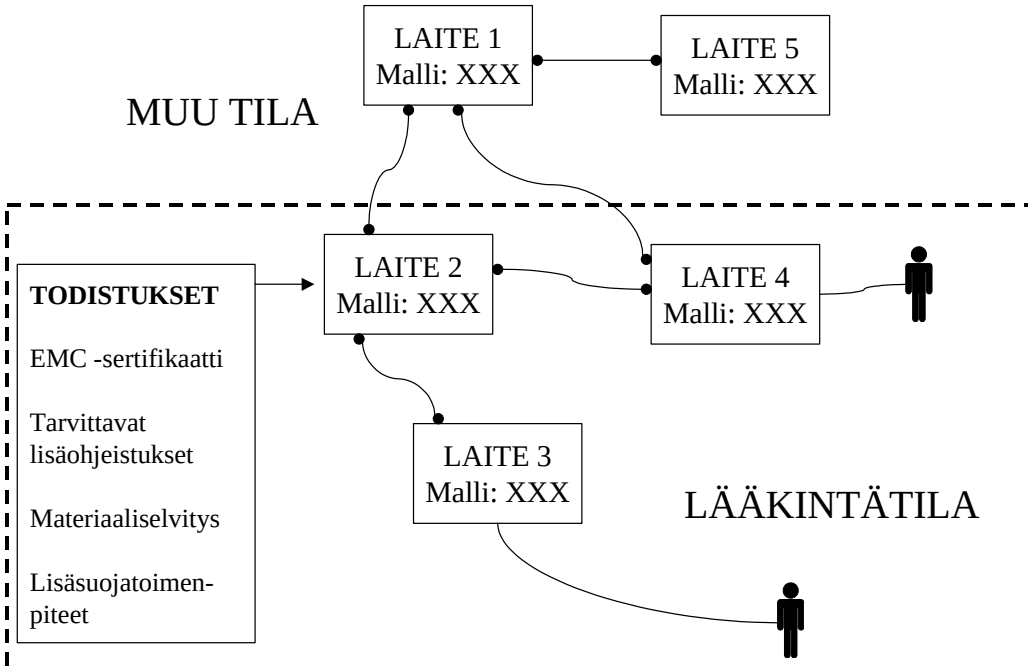
JÄRJESTELMÄ	*[Nimi, malli, sarjanumero, valmistaja ja muut tarvittavat tunnisteet]*		
KUVAUS	*[Mikä järjestelmä, mitä se tekee]*		
VERSIOINTI	*[Laitteistoversio]*	*[Ohjelmaversio]*	*[Muu]*
SOPIMUKSET	*[Viittaukset tilaukseen, tarjoukseen ja muihin tarvittaviin sopimuksiin]*		
MAKSUAIKATAULU	*[Kirjallisen sopimuksen mukaan, määriteltävä ehdot]*		
TOIMITTAJA	*[Toimittajan nimi]*		
- Osoite	*[Yrityksen osoite]*		
- Toimittajan yhteyshenkilö	*[Henkilön nimi ja yhteystiedot]*		
TAKUU			
- Takuuehdot ja rajoitukset	*[Kirjallinen, määriteltävä mitä takuu kattaa ja mitä ei kata]*		
- Aika	*[Takuun kesto, määriteltävä alkamisajankohta]*		
SUORITUSKYKY			
- Tekniset tiedot	*[Mistä tiedot löytyy, vastaako tilaussopimuksen tietoihin]*		
- Mittaukset	*[Raportit mittauksista, validointiraportit]*		
HUOLTOSOPIMUS	*[Sopimusnumero / diariointi, kattavuus]*	Päiväys: *[dd.mm.year pakollinen]*	
VASTAANOTETTU			
- Vastaanottaja:	*[Vastaanottaja]*	Päiväys: *[dd.mm.year pakollinen]*	
- Hyväksyjä:	*[Hyväksyjä]*	Päiväys: *[dd.mm.year pakollinen]*	
KÄYTTÖPAIKKA			
- Vastuuhenkilö	*[Käytöstä vastaava henkilö]*		
- Yhteystiedot	*[Osasto, puh.no, e-mail]*		
KÄYTTÖKOULUTUS	*[Paikka, osallistujalista]*	Päiväys: *[dd.mm.year pakollinen]*	
HUOLTOKOULUTUS	*[Paikka, osallistujalista]*		
PÖYTÄKIRJA	Sivuja: *XXX kpl*	Liitteet: *XXX* kpl	

F.2 Järjestelmän muutos- ja huoltohistoria

Muutos / Korjaus	Korjaus/Muutos raportit	Tekijä & Pvm.	Hyväksyjä & pvm.
[Tähän kuvataan muutoksen tai korjauksen syy ja tehdyt toimenpiteet] *[Muutoksen osalta kuvataan muutoksen vaikutus edelliseen malliin verrattuna]* *[Järjestelmän toimivuus ja suorituskyky on tarkastettava muutoksen/ korjauksen jälkeen]*	*[Tähän listataan ne raportit ja dokumentit, joilla kuvataan tehty muutos ja varmistetaan tuotteen täyttävän edelleen sille asetut vaatimukset]*	*[Kuka teki, milloin teki]*	*[Kuka hyväksyi, milloin hyväksyi]*

F.3 Järjestelmän kokoonpano

Laite	**Kuvaus ja rajoitteet**
LAITE 1	Laserkirjoitin XXX, IEC XXX hyväksytty, hyväksyntätodistus liitteessä 1. Laite sijaitsee lääkintätilan ulkopuolella. Huom! Kirjoitin kytkeytyy laitteeseen 2 sarjaportin kautta, jotta lääkintätilassa olevien laitteiden vuotovirta ei kasvaisi liian suureksi on sarjaporttiin kytketty optinen erotin. Optisen erottimen tekniset tiedot liitteessä 2. Kirjoitin ei sovellu käytettäväksi lääkintätilassa.
LAITE 2	Lääkintätilassa oleva tiedonkeruulaite, IEC XXX, hyväksyntätodistus liitteessä 3. Maavuotovirtojen rajoittamiseksi sähkönsyöttö laitteelle on toteutettu erotusmuuntajalla, jonka tekniset tiedot ja eristysvälit liitteessä 4.
LAITE 3	Lääkintätilassa oleva lääkintälaite, CE-merkitty, sertifikaatti liitteessä 5. Lääkintälaitteen liityntäosa CF –tyyppiä.
LAITE 4	Lääkintätilassa oleva lääkintälaite, CE-merkitty, sertifikaatti liitteessä 6. Lääkintälaitteen liityntäosa CF –tyyppiä.
LAITE 5	Lääkintätilan ulkopuolella oleva tietokone, IEC XXX, hyväksyntätodistus liitteessä 7. Sähkönsyöttö toteutettu erotusmuuntajalla, jonka tekniset tiedot ja eristysvälit liitteessä 4. Järjestelmän vuotovirtamittaustulokset liitteessä 8. Huom! Lohkokaavioesityksessä tulee näkyä, mistä laitteesta on kytkentä potilaaseen ja missä kohtaa kulkee ei-lääkintätilan ja lääkintätilan raja. Lisäksi kokoonpanossa tulee käydä ilmi, täyttääkö ei-lääkintälaite kotelointiluokitusvaatimukset mahdollisesti vaativammassa käyttöympäristöss



***Kuva F1**. Esimerkki järjestelmän laitteista ja sijoituksesta eri tiloihin*

F.4 Tiedot erillisliitteistä

HYVÄKSYNTÄTODISTUKSET TAI RAPORTIT	LIITENUMERO	HYVÄKSYTTY	
		Kyllä	Ei
Järjestelmän EMC –raportti	9	X	
Toksisuus (mikäli sovellettavissa, tapauskohtaisesti arvioitava)	10	X	
Järjestelmän riskianalyysi	11	X	
Järjestelmän vuotovirtamittaukset	12	X	
Tekniset tiedot erilliskomponenteista (tarvittaessa)	XX		
Sterilointia koskevat raportit	XX		
Muut tärkeät asiakirjat	XX		
Hyväksyntätodistukset ja raportit tarkasti:		Pvm:	

F.5. Mukana seuraavat asiakirjat

F.5.1 Käyttöohjeet

KÄYTTÖOHJEKÄSIKIRJAT	Tunniste	Kieli	
Laitteen 1 käyttöohjekäsikirja + lisäohjeistus optiselle erottimelle	XXX1.2		
Laitteen 2 käyttöohjekäsikirja + lisäohjeistus erotusmuuntajalle	XXX2.2		
Laitteen 3 käyttöohjekäsikirja	XXX3.2		
Laitteen 4 käyttöohjekäsikirja	XXX4.2		
Laitteen 5 käyttöohjekäsikirja	XXX5.2		
JÄRJESTELMÄKÄYTÖSTÄ AIHEUTUVAT DOKUMENTOINTIVAATIMUKSET	Tunniste	HYVÄKSYTTY	
		Kyllä	Ei
Dokumentoinnissa on huomioitu laitteiden yhteiskäytöstä aiheutuvat vaatimukset	-----	-	
Dokumentoinnissa on huomioitu ei-lääkintälaitteiden mahdollisesti tiukemmat puhdistusohjeet	XXX2.2	X	
Ohjeistus laitteelle 2, että sen sähkönsyöttö tulee järjestää erotusmuuntajalla	XXX2.2	X	
Ohjeistus laitteelle 1, että kytkentä laitteeseen 2 tulee tehdä optisen erottimen kautta	XXX1.2	X	
Käyttöohjeluettelon laati	Pvm:		
Käyttöohjeluettelon tarkasti	Pvm:		

F.5.2 Tekninen dokumentaatio

TEKNINEN DOKUMENTAATIO	Tunniste	Kieli
Laitteen 1 huolto-ohjekäsikirja + lisätiedot optiselle erottimelle	XXX1.1	Suomi
Laitteen 2 huolto-ohjekäsikirja + lisätiedot erotusmuuntajalle	XXX2.1	Englanti
Laitteen 3 huolto-ohjekäsikirja	XXX3.1	
Laitteen 4 huolto-ohjekäsikirja	XXX4.1	
Laitteen 5 huolto-ohjekäsikirja	XXX5.1	
Asennusohjeistus		

JÄRJESTELMÄKÄYTÖSTÄ AIHEUTUVAT DOKUMENTOINTIVAATIMUKSET		HYVÄKSYTTY	
Dokumentoinnissa on huomioitu laitteiden yhteiskäytöstä aiheutuvat vaatimukset	Tunniste	Kyllä	Ei
Ohjeistus laitteelle 2, että sen sähkönsyöttö tulee järjestää erotusmuuntajalla	XXXX2.1	X	
Ohjeistus laitteelle 1, että kytkentä laitteeseen 2 tulee tehdä optisen erottimen kautta	XXXX1.1	X	
Asennusohjeistus			

Teknisen dokumentaatioluettelon laati:	Pvm:
Teknisen dokumentaatioluettelon tarkasti:	Pvm:

F.5.3 Muu dokumentaatio

MUUT JÄRJESTELMÄN MUKANA SEURAAVAT ASIAKIRJAT:	IdNro:	Pvm:	Kieli
Esim. Asennusohjeistus			

LIITE G TEKNINEN TIEDOSTO

G.1 Yleistä

Teknisen tiedoston avulla valmistaja voi varmentaa, että hänen tuotteensa on säädösten ja standardien vaatimusten mukaisia sekä kykenee osoittamaan tuotteensa vaatimustenmukaisuuden. Valmistaja määrittelee laatujärjestelmäänsä eri osastojen (tuotekehitys-, suunnittelu-, valmistus- ja markkinointiosastot) tehtävät ja kussakin osastossa syntyvän teknisen tiedoston vaatimat tiedot.

G.2 Teknisen tiedoston rakenne ja laadinta

Terveydenhuollon laiteita ja tarvikkeita koskevat säädökset ja määräykset edellyttävät valmistajaa ylläpitämään tuotetta koskevaa teknistä tiedostoa, jonka avulla valmistaja kykenee osoittamaan tuotteensa vaatimusten mukaisuuden valvontaviranomaisille. Tiedoston rakenne ja vastuut tietotuotannosta ovat tämän vuoksi valmistajan ratkaistava ja otettava käyttöön ennen tuotteen markkinoille saattamista. Määrätyt osat teknisestä tiedostosta on oltava viranomaisten ja valmistajan valitseman ilmoitetun laitoksen saatavilla vaatimustenmukaisuuden arviointia varten.

Olennaiset vaatimukset on jaettu yleisiin vaatimuksiin sekä suunnitteluja rakennevaatimuksiin, jotka tuotteen tulee täyttää tai valmistajan tulee osoittaa, että vaatimus ei koske tuotetta. Olennaiset vaatimukset kohdistuvat pääasiassa tuotteiden turvallisuuteen ja jossain määrin niiden soveltuvuuteen suunniteltuun käyttöön. Suorituskykyyn olennaiset vaatimukset eivät suoraan puutu, mutta vaatimus soveltuvuudesta tuotteelle suunniteltuun käyttöön sisältää usein implisiittisesti myös suorituskykyyn kohdistuvia vaatimuksia. Lisäksi tuotteen ominaisuudet ja toiminnot eivät saa elinaikana muuttua siten, että seurauksena olisi liian suureksi kasvanut turvallisuusriski. Kuljetus- ja varastointijaksot kuuluvat tuotteen elinkaareen. Riskien, jotka liittyvät erityisesti sähkökäyttöisten lääkintälaitteiden käyttöön, minimointi on osa olennaisia vaatimuksia.

Vaatimusten toteuttamisessa valmistaja voi käyttää omia sisäisiä standardeja, mutta turvallisempi tapa osoittaa vaatimustenmukaisuus on käyttää soveltuvia eurooppalaisia harmonisoituja standardeja silloin kun niitä on olemassa. Tekninen tiedosto on mielekästä (tietotuotanto) ja-

kaa kahteen osaan: tuotteen suunnittelua koskevat ja tuotteen tuotantoa koskevat tiedostot. Syntyvät tiedostot, niiden tuotantotapavastuu ja päivittäminen ovat luontevasti osa yrityksen laatujärjestelmää (vrt. device history record, device master record).

Tuotteen suunnittelua koskeva tiedosto (product design dossier) voidaan jakaa kahteen osaan:

1. Yhteenveto oleellisista teknisistä tiedoista (technical data) vaatimustenmukaisuuden osoittamiseksi.
2. Tuotetta koskevat testausselosteet, tiedot tuotteen suunnittelun ja valmistuksen laatumanuaaleista, suunnitelmat, tuotteen ja sen valmistuksen kuvaus sekä käytetyt standardit.

Teknisen tiedoston sisältö muodostuu useasta eri dokumentista. Näillä dokumenteilla on erilaisia käyttötarkoituksia tuotteiden turvallisuuden varmistamiseksi ja niitä syntyy tuotteen eri elinjaksoilla. Tämän vuoksi selkeä indeksointi- ja referointijärjestelmä dokumenttituotannossa on välttämätön.

Tietosisältö jakautuu neljään osaan seuraavasti:

1. asiakkaalle tuotteen mukana toimitettavat tiedot
2. tekninen huolto-ohje huoltopisteille ja tarvittaessa asiakkaalle
3. vaatimuksenmukaisuuden osoittamiseksi ilmoitetulle laitokselle ja viranomaiselle
4. tuotanto- ja laadunvarmistusdokumentaatio.

Taulukossa G1 on eräs malli teknisen tiedoston pääjaotteluksi. Taulukkoon G1 on lisätty sarake 'merkitys sairaalalle', johon on liitetty merkinnät ”H & M” (= hankinta ja muutokset), joissa eniten on syytä tarkastaa ko. kohdan vaatimustenmukaisuus. Listaa on mahdotonta tehdä kaikenkattavaksi ja tarkka pohdinta on tehtävä jokaisen tapauksen kohdalla erikseen.

Taulukko G1a. Esimerkki teknisen tiedoston sisältämästä dokumentoinnista

DOKUMENTTI	TUOTTEEN MUKANA	TEKNINEN	VAATIMUSTEN MUKAISUUDEN OSOITTAMINEN	MERKITYS SAIRAALALLE
Tuotteen yleiskuvaus, eri variaatiot	X	X	X	H & M
Suunnittelupiirustukset		X	X	
Valmistusmenetelmät		X	X	
Osapiirustukset		X	X	H & M
Rakenne-elementit		X	X	H & M
Tarkastuksien ja suunnittelulaskelmien tulokset		X	X	
Liitännäislaitteiden ominaisuuksien spesifikaatiot ja käyttö yhdessä	X	X	X	H & M
Kuvaukset ja selitykset				
Suunnitelmat ja piirustukset			X	H & M
Tuotteen toiminta				H & M
Olennaisten vaatimusten täyttyminen			X	Muutokset
Lista käytetyistä standardeista		X	X	
Ei-standardoidut ratkaisut			X	H & M
Riskianalyysiraportit			X	H & M
Jäännösriskit	X		X	H & M
Sterilointi				
Steriloinnin vaikutukset tuotteeseen ja käyttöön, sterilointitapa, validointi	X	X	X	H & M
Kliininen tutkimus				
Testausselosteet ja tiedot kliinisestä arvioinnista		X	X	Hankinta
Kirjallisuustutkimus tai kliinisen tutkimuksen tulokset		X	X	Hankinta, muutoksen laajuus vaikuttaa
Merkinnät ja käyttöohje	X	X	X	H & M

Taulukko G2b. Esimerkki teknisen tiedoston sisältämästä dokumentoinnista

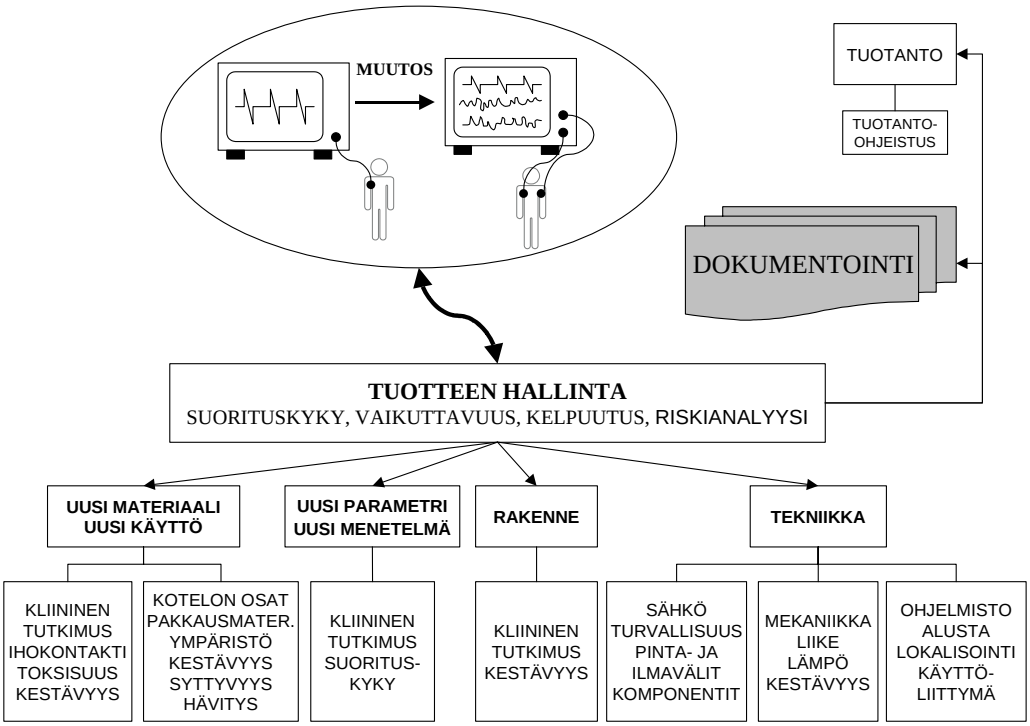
DOKUMENTTI	TUOTTEEN MUKANA	TEKNINEN	VAATIMUSTEN MUKAISUUDEN OSOITTAMINEN	MERKITYS SAIRAALALLE
Tuotemuutokset				
Muutoksen syy		X	X	Muutokset
Dokumentointi	X	X	X	Muutokset
Testiraportit		X	X	Muutokset
Päivitetty riskianalyysi		X	X	Muutokset
Jäännösriskit	X		X	Muutokset
Verifiointi- ja validointiraportit		X	X	Muutokset
Laadunvarmistus				
Suunnitelmat ja niiden noudattaminen		X	X	
Testiraportit		X	X	H & M
Suunnittelukatselmukset		X	X	
Verifiointiraportit		X	X	
Validointiraportit		X	X	H & M

G.3 Tekninen tiedosto käyttäjän kannalta

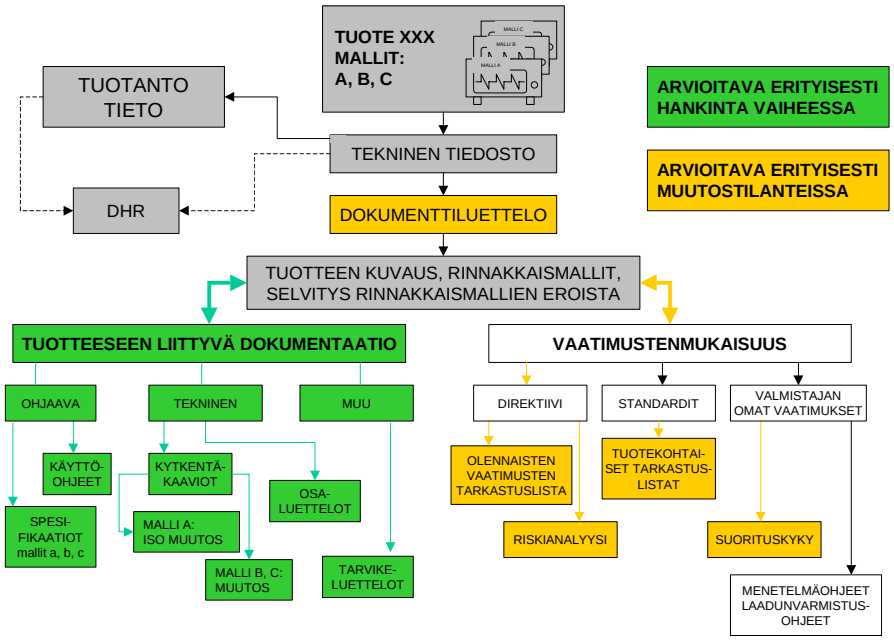
Terveydenhuollon toimintayksikön kannalta teknisen tiedoston rakenteen tunteminen on oleellista erityisesti muutostilanteissa. Esimerkiksi tuotteen muutokset ja päivitykset saattavat edellyttää muutoksia tuotteen teknisen tiedostoon, jolloin esim. sairaala voi pyytää valmistajalta tiettyjä suunnitteludokumentteja, joilla valmistaja osoittaa tuotteen täyttävän edelleen sille asetetut vaatimukset.

Laitteiden ja laitejärjestelmien muutos- ja päivitysmenettelyt tulisi määritellä jo hankintavaiheessa, jolloin sairaala saisi oletettavasti helpommin kaiken pyydettävän dokumentaation käyttöönsä. Tärkeitä muutostilanteen dokumentteja ovat ainakin päivitetty riskianalyysi ja suorituskyvyn osoittamiseen liittyvät testausselosteet, jotka sairaalan tulisi pyytää käyttöönsä muutoksen hyväksymisvaiheessa.

Kun tuotteesta laaditaan jokin asiakirja ja se liitetään asiakirjaluetteloon on se osa tuotetiedostoa (Device Master Record), mutta kun kyseistä asiakirjaa päivitetään muuttuu se tuotantotiedoston (Device History Record) osaksi (kuva G1) ja kyseisen asiakirjan päivitetty versio muuttuu tuotetiedoston osaksi. Kaikki tämä tulee kirjata asiakirjaluetteloon ja kyseinen asiakirja tulee siirtää tuotantotiedostoon. Asiakirjaluetteloa täydennetään vain siltä osin jota muutos koskee. Kuvan G2 esimerkissä kuvataan valmistajan tuote ja tuotteeseen liittyvät asiakirjat ja niiden liittyminen toisiinsa.



***Kuva G 1**. Tuotemuutoksessa huomioitavia seikkoja*



***Kuva G 2**. Teknisen tiedoston rakenne*

Taulukko G2a. Tekniseen tiedostoon liittyvää terminologiaa

TERMI	SELITYS	LÄHDE
TERVEYDENHOIDON LAITE JA TARVIKE (lääkinnällinen laite) *Medical device*	Terveydenhuollon laitteella ja tarvikkeella tarkoitetaan kaikkia instrumentteja, laitteistoja, välineitä, materiaaleja tai muita tarvikkeita, joita käytetään joko yksinään tai yhdistelminä, sekä niiden asianmukaiseen toimintaan tarvittavia ohjelmistoja, joita valmistaja on tarkoittanut käytettäviksi ihmisten: - sairauden diagnosointiin, ehkäisyyn, tarkkailuun, hoitoon tai lievitykseen - vamman tai vajavuuden diagnosointiin, tarkkailuun, hoitoon, lievitykseen tai kompensointiin - anatomian tai fysiologisen toiminnon tutkimiseen, korvaamiseen tai muunteluun - hedelmöittymisen säätelyyn ja joiden pääasiallista aiottua vaikutusta ihmiskehossa tai -kehoon ei saavuteta farmakologisin, immunologisin tai metabolisin keinoin, mutta joiden toimintaa voidaan tällaisilla keinoilla edistää	Laki terveydenhuollon laitteista ja tarvikkeista, 1505/1994
VALMISTAJA *Manufacturer* OMA VALMISTUS	Valmistajalla tarkoitetaan luonnollista henkilöä tai oikeushenkilöä, joka on vastuussa laitteen suunnittelusta, valmistuksesta, pakkaamisesta ja merkitsemisestä sen markkinoille saattamiseksi omalla nimellään, nämä toimet voi suorittaa tämä sama henkilö tai kolmas henkilö tämän lukuun. Tämä tarkoittaa, että laitteen valmistus ja/tai suunnittelu voi olla joko kokonaan tai osittain aliurakoitu mutta lainsäädännön muut velvoitteet eivät. Näitä ovat mm. sitoumus ilmoitetun laitoksen kanssa, vaatimustenmukaisuusvakuutus ja sen edellytysten osoitus, tuotteen seuranta markkinoilla (jäljitettävyys, korjaavat toimenpiteet, markkinoilta poistaminen). Jos sairaala valmistaa tuotteita omaan sisäiseen käyttöön, niin tällöin sitä ei pidetä lain tarkoittamana valmistuksena ja CE-merkintää vaadittuine toimenpiteineen ei tarvita. Mutta jos näin valmistettuja tuotteita annetaan potilaiden käyttöön käyttötarkoituksensa mukaisesti, niin sairaalasta tulee lain tarkoittama valmistaja.	Laki terveydenhuollon laitteista ja tarvikkeista, 1505/1994
YKSILÖLLISEEN KÄYTTÖÖN VALMISTETTU LAITE *Custom-made device*	Laitteita, jotka on erityisesti valmistettu asianmukaisesti pätevän lääkärin kirjallisen määräyksen mukaisesti, jossa tämän vastuulla annetaan laitteen yksityiskohtaiset suunnitteluominaisuudet, ja jotka on tarkoitettu käytettäväksi ainoastaan tietylle potilaalle.	Laki terveydenhuollon laitteista ja tarvikkeista, 1505/1994
LISÄLAITE	Lisälaitteella tarkoitetaan kaikkia tarvikkeita, vaikka ne eivät olisi laitteita, joita valmistaja on erityisesti tarkoittanut käytettäväksi laitteen kanssa mainitun laitteen käyttä-	Laki terveydenhuollon laitteista ja tarvikkeista, 1505/1994

TERMI	SELITYS	LÄHDE
Accessory	miseksi tämän laitteen valmistajan aikomuksen mukaisesti. Lisälaitteet luokitellaan niiden omista lähtökohdista (aiottu käyttötarkoitus, kytkeytyminen potilaaseen) ja näin kysymyksellä, onko tuote lääkinnällinen laite vai lisälaite, ei ole käytännön merkitystä. Merkittävin seuraus laitteen ja lisälaitteen "erottamisesta" on se, että monesti perinteisesti ajateltuna varsinainen laite putoaa alempaan riskiluokkaan, koska vain lisälaite on kontaktissa potilaaseen. Tämä tuo helpotuksia valmistajalle. Esimerkkejä: Kaasupullot ja paineenalennusventtiilit, jotka on tarkoitettu käytettäväksi anestesialaitteen yhteydessä. Uudelleensteriloitavien tuotteiden pakkauspussit.	
VARAOSA *Spare part*	Yleensä varaosat eivät ole lääkinnällisiä laitteita. Mutta jos varaosa vaikuttaa merkittävästi laitteen ominaisuuksiin tai suorituskykyyn ajatellen sen vaatimustenmukaisuutta niin tällaista varaosaa tulee pitää lääkinnällisenä laitteena.	
KÄYTTÖTARKOITUS *Intended purpose*	Tällä tarkoitetaan käyttöä, johon laite valmistajan merkinnöissä, käyttöohjeessa ja/tai myynninedistämistä koskevassa aineistossa annettavien tietojen mukaan on tarkoitettu. Tämän tiedon perusteella tuote luokitellaan ja varmennustoimet määräytyvät. Sen vuoksi se on erittäin tärkeä tuotespesifikaatio. Sen muuttaminen esim. esitteessä saattaa muuttaa tuoteluokkaa ja näin vaatimuksia ja johtaa uudelleenarviointiin. Toisaalta se varmistanee valmistajan asemaa tilanteissa, joissa on sattunut potilasvahinko ja tuotetta on käytetty vastoin sen käyttötarkoitusta.	Laki terveydenhuollon laitteista ja tarvikkeista, 1505/1994

Taulukko G2b. Tekniseen tiedostoon liittyvää terminologiaa

TERMI	SELITYS
TUOTETIEDOSTO TEKNINEN TIEDOSTO *Device Master Record, DMR* *Device Master File*	Sisältää (tai viittaa sijaintiin) tuotteen suunnitteluun, valmistukseen, asennukseen ja huoltoon liittyvän dokumentaation. Vaatimustenmukaisuuden osoittamisen kannalta avaintiedosto. Esim. spesifikaatiot raaka-aineille, merkinnöille, pakkaukselle, väli- ja lopputuotteelle piirustukset, ohjelmiston suunnitteluspeksit, lähdekoodit, työohjeet, tuotantomenetelmät, ympäristömäärittelyt, sterilointiprosessin yksityiskohdat, tarkastusmenettelyt ja hyväksyntäkriteerit, asennus- ja huolto-ohjeet, mahdollisesti myös suunnittelun todentamistiedostot (verification) [toiminto spesifioitujen vaatimusten mukaista], prosessin kelpuutuksen osoitustiedostot (validation) [tutkitaan onko tuote käyttäjien tarpeiden mukainen]. DMR on osa laatujärjestelmää ja näin myös sen tulee olla laatudokumenttien valvontamenettelyjen kohteena.
TUOTANTOTIEDOSTO *Device History Record, DHR*	Sisältää tuotteen tuotantotietoutta kuten tuotannonaikaisia tarkastus- ja mittausraportteja, lopputarkastuspöytäkirjat sekä hyväksyntäasiakirjat (release to market). Näistä löytyy myös yhteys prosessin- ja ympäristönvalvontatietoihin silloin kun nämä vaikuttavat lopputuotteen vaatimustenmukaisuuteen.
SUUNNITTELU-KATSELMUS *Design Review*	Dokumentoitu, kattava ja järjestelmällinen tutkinta sen selvittämiseksi, täyttääkö suunnittelu sille asetetut laatuvaatimukset, sekä mahdollisten ongelmien yksilöimiseksi ja niitä koskevien ratkaisuehdotusten tekemiseksi.
HYVÄKSYNNÄN ODOTUSKOHTA *Hold point*	Asiakirjassa määritelty kohta, jota pidemmälle toiminto ei saa edetä ilman valtuutetun organisaation tai henkilön hyväksyntää Esim. Tuotteen hyväksyntä kliinisiin kokeisiin, tuotantoon tai tuotteen hyväksyntä toimitukseen.
LAATUSUUNNITELMA *Quality plan*	Tuotteeseen liittyvät laatukäytännöt, resurssit ja toimintosarjat määrittelevä asiakirja - laatutavoitteet; tuoteominaisuudet, tasalaatuisuus, tehokkuus, esteettisyys, läpäisyaika, kustannukset, saanto, käyttövarmuus - prosessin vaiheet esim. vuokaaviona - vastuiden, valtuuksien ja resurssien kohdentaminen - testaus-, tarkastus-, tutkimus- ja auditointiohjelmat - muutosten ja modifikaatioiden hallinta projektin aikana - tavoitteiden saavuttamisen mittausmenetelmät

TERMI	SELITYS
JÄLJITETTÄVYYS *Traceability*	Mahdollisuus selvittää tuotteen aiemmat vaiheet, käyttö tai sijaintimuistiin merkittyjen yksilöityjen tietojen avulla. Tuotteen osalta jäljitettävyys voi merkitä esim.: - materiaalin ja osien alkuperän selvittämistä, - tuotteen käsittelyvaiheen selvittämistä, - tuotteen jakelureitin ja toimituksen jälkeisen sijainnin selvittämistä. Jäljitettävyysvaatimukset tulisi myös spesifioida esim. ajan, alkuperän tai tunnistamisen suhteen.
TODENTAMINEN *Verification*	Suunnittelussa ja tuotekehityksessä todentaminen tarkoittaa prosessia, jolla tutkitaan tietyn toiminnon tulokset kyseiselle toiminnolle asetettujen vaatimusten vaatimustenmukaisuuden määrittämiseksi
KELPUUTUS *Validation*	Tarkoittaa tuotteen tutkimista sen selvittämiseksi, onko se käyttäjien tarpeiden mukainen. Se tehdään tavallisesti lopullisessa muodossa olevalle tuotteelle määritellyissä käyttöolosuhteissa.

LIITE H KIRJALLISUUTTA JA WWW-LINKKEJÄ

TIETOTURVA	LYHYT SELITYS
www.cert.org	Software Engineering Institute; ajankohtaista tietoa hyökkäyksistä ja suojautumisesta
www.research.ibm.com	IBM:n tutkimuslaboratorio; tuloksia kannattaa seurata.
www.securityfocus.com	Kaupallinen sivu; kaikenlaista tietoa
http://palvelut.tieke.fi/arkisto/tiveke/turva.htm	Tiveken tietoturvasivut
http://www.rsasecurity.com/rsalabs/	Yleistä salaisen ja julkisen avaimen menetelmistä
http://www.wassenaar.org/	Wassenaar-sopimus
http://www.securitysearch.net/	Tietoturvalinkkejä
http://home.netscape.com/eng/ssl3/	SSL
http://www.gocsi.com/	Computer Security Institute
http://www.ecri.org/documents/032601.htm	DICOM Reference Guide and Addresses the Topic of Healthcare Information Security
http://csrc.nist.gov/	National Institute of Standards and Technology
http://www.cert.org/encyc_article/tocencyc.html	Security of the Internet
http://www.commoncriteria.org/	The Standard for Information Security
W-LAN	
http://standards.ieee.org	Kansainvälinen IEEE-standardointijärjestö
http://www.etsi.org/	European Telecommunications Standards Institute
http://www.wlana.com/	Wireless LAN Association
http://www.aowt.org/	Association of Wireless Technology

Lisätietoa voi etsiä hakusanoilla 'langaton tekniikka', 'wireless technology', 'mitä on IEEE 802.11', 'specification for IEEE 802.11'.

KIRJALLISUUTTA

Maija Kleemola, Raija Pellikka: Tietosuoja, Vaatimukset verkottuvassa tietojärjestelmässä ISBN: 951-762-637-1

Esa Kerttula: Tietoverkkojen tietoturva, Edita Liikenneministeriö, ISBN: 951-37-2904-4

Health Devices January-February 2001, Volume 30, numbers 1-2, DICOM Reference Guide

Maximum Security, Second edition, ISBN 0-672-31341-3

Radia Perlman: Interconnections, Second edition, ISBN 0-201-63448-1

Campen et al (eds.): Cyberwar, Security, Strategy and Conflict in the Information Age, ISBN 0-916159-26-4

Windows NT server white paper, Securing Windows NT Server Installation, Microsoft Corporation, 1997.

ISSN 1238-8777
ISBN 952-5099-74-1

Lääkelaitos, PL 55, 00301 Helsinki
Puh. (09) 473 341, faksi (09) 714 469
www.nam.fi