Therac-25 artikkeli

Henri Laakso, 240062, henri.m.laakso@student.tut.fi

Niko Lappalainen, 253002, niko.lappalainen@student.tut.fi

Antti Tolonen, 247589, antti.tolonen@student.tut.fi

Johdanto

Vuosien 1985 ja 1987 välillä tietokoneohjattu sädehoitolaite Therac-25 aiheutti tappavan säteilyn yliannostuksen kuudelle eri potilaalle. Artikkeli kuvaili yksittäisten tapausten tapahtumia, organisaatioiden toimia näitä kohtaan sekä lopulta kuvaili ongelmien syynä olleita ohjelmistovikoja ja toimintatapojen ongelmia.

Artikkelissa kuvataan kaksi ohjelmistollista syytä säteily-yliannostuksien aiheuttajiksi. Molemmissa tapauksissa ohjelmistovika aiheutti väärien hoitoparametrien käytön, joka johti väärään kääntöpöydän asentoon tai säteilylähteen asetuksiin, jolloin potilas sai säädellyn elektronisuihkun sijaan täyden energian elektronisuihkun säätelijän läpi.

Laitteen yleinen toimintaperiaate

Therac-25 sädehoitolaitetta voitiin käyttää kolmessa eri toimintamoodissa. Laitteella voitiin antaa potilaalle sädehoitoa joko röntgensäteilyllä tai elektronisuihkulla, lisäksi laitteessa oli kohdistusmoodi jossa laite tuotti säteilyn sijaan valonsäteen joka näytti mihin laitteesta tuleva säteily suuntautuisi.

Toimintamoodin valintaan tarvittiin kaksi erillistä asetusta. Laitteessa piti valita tuottiko laite valonsäteen vai elektronisuihkun, ja kuinka voimakkaan elektronisuihkun se tuotti. Lisäksi laitteessa oli kääntöpöytä jolla oli kolme asetusta: röntgensäteilykohde, elektroniskannausmagneetti ja peili.

Mikäli laitteella haluttiin antaa potilaalle röntgensäteilyä piti säteilylähteeksi asettaa elektronisuihku maksimiteholla ja kääntöpöytä piti asettaa asentoon jossa röntgensäteilykohde oli elektronisuihkun edessä.

Mikäli laitteella haluttiin antaa potilaalle sädehoitoa elektronisuihkulla, piti säteilylähteeksi asettaa elektronisuihku pienemmällä teholla kuin röntgensäteilyä annettaessa ja kääntöpöytä piti asettaa asentoon jossa elektronisuihku kulki skannausmagneetin läpi.

Mikäli laitetta haluttiin käyttää kohdistusmoodissa piti sen tuottaa valonsäde elektronisuihkun sijaan ja kääntöpöydän piti olla asennossa jossa peili ohjasi valonsäteen potilaaseen.

Laitteella oli mahdollista antaa potilaalle säteily-yliannostus mikäli säteilylähteen ja kääntöpöydän asetukset eivät vastanneet toisiaan. Esimerkiksi, jos säteilylähde oli asetettu röntgenmoodin mutta

kääntöpöytä oli joko skannausmagneetti- tai peiliasennossa, kohdistui potilaaseen liian voimakas elektronisuihku.

Artikkelissa mainittuja yleisiä ongelmia laitteen suunnittelussa ja käytössä ilmenneiden virheiden selvittämisessä

Artikkelissa listataan useita yleisluontoisia ongelmia Therac-25-laitteen suunniteluun ja käyttöön liittyen. Näitä olivat mm.

- Riittämätön testaus
- Ohjelmiston oikeaan toimintaan luotettiin sokeasti
- Lokitiedostojen/muun seurannan puute
- Laitteiston epäselvät virheilmoitukset
- Laitteiston vaikea tulkittavuus

Artikkelissa mainitut ohjelmointivirheet

Kilpailutilanne luettaessa tietoja

Ohjelmistossa pyöri samanaikaisesti kolme eri prosessia; treat, hand ja keyboard handler. Treat kontrolloi hoidon eri vaiheita sen kahdeksan alirutiinin avulla. Hand asetti kääntöpöydän asennon. Keyboard handler asetti yhteisen MEOS-muuttujan arvot syötteiden mukaisiksi, joita treat ja hand sen jälkeen lukivat.

Käyttäjän syötettyä parametrit laitteelle kutsui treat alirutiinejaan asettamaan asetukset halutulle suihkulle ja magneeteille. Alirutiini tarkisti asetukset asetetuiksi tutkimalla kursorin paikkaa. Jos kursori oli komentorivillä oli tiedot annettu ja ohjelma valmis asettamaan asetukset. Treat kutsui seuraavaa alirutiiniaan, joka asetti magneetit oikeihin paikkoihin ja eri magneettien asettamisten välissä kutsui se viive alirutiinia, jotta magneetit kerkeäisivät asettua paikoilleen ennen seuraavan magneetin asettamista. Viive alirutiini tutki oliko jaettuun muistiin tullut muutoksia, mutta vain jos lippu magneettien asettamisesta oli positiivinen. Viivealirutiinia kutsuttiin monesti eri magneettien asettamisen välissä. Viiverutiinin ensimmäisellä läpikerralla lippu magneettien asettamisesta muutettiin negatiiviseksi, jolloin käyttäjä ehti tekemään muutoksia asetuksiin ohjelman niitä huomaamatta jos asetusten muuttaminen tapahtui ennen seuraavan magneetin asettamista.

Muuttujan ylivuoto

Treat lohkon asettaessa asetuksia laitteelle inkrementoi se Class3 nimistä muuttujaa, joka varmistaa ettei sädettä käytetä asetusten asettamisen aikana. Jos muuttuja on 0, on kaikki kunnossa ja laite valmiina käyttöön. Jos muuttaja taas on erisuuri kuin 0 on laitteen asetuksien asettaminen vielä kesken, joten odotetaan. Laitteen senhetkiset asetukset ovat tallennettuina F$mal muuttujaan, josta luetaan ovatko laitteen asetukset yhdenpitävät haluttujen asetusten kanssa. F$mal on oikea silloin, kun sen arvo

on 0. Jos Class3 arvo on 0 ohitetaan kääntöpöydän asennon tutkiminen, jolloin sitä vastaava bitti F$mal muuttujassa on 0 vaikka kääntöpöytä ei olisikaan oikeassa asennossa. Kääntöpöydän asennon tarkastus ohitetaan, kun Class3 muuttujan inkrementointi aiheuttaa ylivuodon ja muuttujan arvo muuttuu arvosta 255 takaisin arvoon 0. Tällöin ohitetaan kääntöpöydän asennon tarkastus ja jos muut asetukset ovat kohdallaan ohjelma tulkitsee laitteen olevan käyttövalmis väärästä kääntöpöydän asennosta huolimatta.

Korjausehdotukset

Ylivuodon esto

Kuten jo itse artikkelinkin korjausehdotuksissa tuli esille muuttujan ylivuoto-ongelma on helppo korjata asettamalla se johonkin tiettyyn arvoon inkrementoinnin sijaan.

Säikeiden/aliprosessien uudelleenjärjestely tehtävien mukaan ja asetukset sisältävien tietorakenteiden suojaaminen lukoilla

Järkevin korjaus siihen että eri prosessit lukevat eri asetukset (esim. Hand-prosessi lukee eri arvon MEOS-muuttujasta kuin Datent-prosessi) on se että MEOS muuttujan arvon lukeminen tehdään vasta sen jälkeen kun käyttäjä ei sitä voi enää muokata. Tämän ratkaisun ainoa haittapuoli on se että laitteen asettaminen toimintakuntoon saattaa kestää hieman kauemmin kuin jos elektronisuihkua ja kääntöpöytää voitaisiin alkaa asettamaan jo siinä vaiheessa kun käyttäjä on ensimmäisen kerran antanut niille jotkut asetukset.

Mikäli kääntöpöydän ja elektronisuihkun laitteistoa halutaan konfiguroida jo ennen kuin käyttäjä on tehnyt lopullisen valintansa asetusten suhteen. Pitäisi mielestämme laitteiston konfigurointiin liittyvät asiat tehdä yhdessä aliprosessissa/säikeessä. Tämä säie voisi lukolla estää asetukset sisältävän tietorakenteen muokkauksen ja tehdä sille sisäinen konsistenttiustarkastuksen ennen kuin se käyttäisi asetuksia fyysisen laitteiston konfigurointiin. Tämä takaisi ettei laitteiston eri osia olisi periaatteessa mahdollista konfiguroida eri tavalla, mikä oli perimmäinen syy säteilyn yliannostuksiin.

Muita muutosehdotuksia

Yllä esitettyjen ohjelmistokorjausten lisäksi laitteistoon pitäisi tehdä monia korjauksia joita on mainittu artikkelissakin.

Esimerkiksi laitteiston konfiguraation sisäinen konsistenttius pitäisi tarkistaa ohjelmistosta riippumattomalla menetelmällä. Tällä vähennettäisiin huomattavasti riskiä siitä että laitteisto antaisi säteilyannoksen joka ei kuulu mihinkään sädehoitoon.

Ohjelmiston pitäisi myös sisältää useita sisäisiä konsistenttiustarkastuksia. Mikäli laitteiston prosessoriteho ja muisti riittäisi olisi myös mahdollista ajaa useampaa eri toteutusta laitteen ohjaussoftasta rinnakkain ja antaa sädehoitoa ainoastaan jos niiden antama ohjaussignaali olisi sama. Näitä eri ohjelmistoja voitaisiin myös ajaa rinnakkain eri laitteistolla.

Yhteenveto

Therac-25 tapaus johtui huonoista ohjelmointi konventioista ja sokeasta uskosta omaan ohjelmistoon, joka johti katastrofaalisiin seurauksiin laitteiston virhetilanteiden seurauksena. Ohjelmiston ongelmat johtuivat rinnakkaisten prosessien käytöstä ilman riittäviä varmistuksia virheiden välttämiseksi, joka johti väärien asetusten asettamiseen laitetta käytettäessä.

Mielestämme näin kriittisessä ohjelmistossa turvallisuus on tärkeämpää kuin nopeus, joten välttämättä rinnakkaisuuden käyttö ei ole paras mahdollinen vaihtoehto varsinkaan kun toiminnasta ei oltu aivan täysin varmoja. Perinteinen sarjallinen toteutus olisi hävinnyt vain joitakin sekunteja ja oltaisiin vältytty rinnakkaisuuden ongelmilta.