Miina Rautakorpi, 291552

Valto Moisio, 268644

Markus Hautala, 283551

Therac-25

Therac-25 on Atomic Energy of Canada Limitedin (AECL) kehittämä sädehoitoon suunniteltu kone, jonka ohjelmistovirheiden vuoksi kuusi eri ihmistä sai yliannoksen sädehoitoa. Yliannostukset olivat niin suuria, että ne aiheuttivat lopulta potilaiden kuoleman. Aluksi onnettomuuksia ei osattu yhdistää Therac-25-laitteeseen eikä onnettomuuksia sen vuoksi tutkittu kunnolla.

Onnettomuudet eivät johtuneet yksittäisistä bugeista, vaan niiden todettiin johtuvan ohjelman rakenteen huonosta suunnittelusta. Aikaisemmat Therac-laitteet oli tehty sädehoitolaitteille, joita pystyttiin käyttämään myös ilman tietokonekontrollia. Uusi Therac-25 suunniteltiin taas nimenomaan käytettäväksi tietokoneen kautta. Therac-25:n suunnittelussa käytettiin silti samoja suunnittelutapoja ja moduuleita kuin aikaisemmissa laitteissa. Tämä voi selittää joitakin huonoja suunnitteluun ja ohjelmistoon liittyviä ratkaisuja. Therac-25:ssa turvallisuus oli jätetty ohjelmiston puolelle, kun taas aikaisemmissa malleissa oli myös mekaanisia turvaominaisuuksia.

Therac-25:n varoitusviestit olivat artikkelin mukaan yleisiä ja epäselkeistä. Niistä ei siis voinut päätellä välttämättä todellista ongelmaa. Esimerkiksi usein esiin tullut ”MALFUNCTION 54” varoitusviestin ainoa selitys oli ”dose input 2”, joka saattoi tarkoittaa sekä liian matalaa, että liian korkeaa annostusta.

Ohjelmistosta löydettiin kaksi vakavaa ongelmaa. Ensimmäisenä löydetty ongelma liittyi säteilyn keskittämiseen magneeteilla. Ohjelmistossa oli muuttuja, jolla merkattiin magneettien olevan kohdistettuna. Toinen prosessi pääsi kuitenkin muuttamaan muuttujaa, vaikka magneetit eivät olleet kohdallaan ja tällöin potilaalla oli riski saada voimakasta säteilyä terveeseen kudokseen. Magneettien kohdistamiseen meni noin 8 sekuntia aikaa, ja kyseinen ongelma ilmeni vain jos laitteen käyttäjä käynnisti tietyn prosessin magneettien kohdistamisen aikana.

Toinen ongelma liittyi 8-bittiseen arvoon Class3, joka indikoi laitteen olevan valmis operaatioon. Laitteen käynnistysprosessin aikana ajettiin useita testejä ja Class3 muuttujaa kasvatettiin yhdellä jokaisen testin aikana. Sädehoito-operaation pystyi käynnistämään vain Class3-muuttujan arvon ollessa nolla. 8-bittinen arvo oli liian pieni tälle muuttujalle ja muuttujan arvon kasvaessa yli 255 arvo pyörähti takaisin nollaan. Jos laitteen käyttäjä sattui painamaan operaation käynnistysnappia juuri oikealla hetkellä (Class3 ollessa 0), sädehoito käynnistyi testien ollessa kesken.

Based on the system description and our course topics - could you fix the software? How confident you’d be on your fix? (Would you let the machine running your fix treat you?)

Ongelma voisi olla mahdollista korjata, mutta kyseisen ajan laitteistolla tarpeeksi luotettavan ohjelmiston toteuttaminen olisi erittäin hankalaa. Ohjelmiston korjaaminen vaatisi paljon tietotaitoa liittyen PDP-11 prosessoriin ja vaatisi paljon aikaa tutustua kyseiseen laitteeseen. Tunnemme paremmin

nykyajan teknologiat, emmekä välttämättä osaisi toteuttaa kyseisen ajan parhaiden periaatteiden mukaista ohjelmaa. Emme antaisi laitteen välttämättä hoitaa meitä edes ohjelmiston korjauksen jälkeen.

If you'd be allowed to change any part of the system (and money is no issue), what fixes would you implement?

Ohjelmiston turvatoimien lisäksi laitteistoon lisätään mekaanisia toimintoja turvallisuuden parantamiseksi. Esimerkiksi laitteeseen voisi lisätä säteilyanturin ja automaattisen virransyötön katkaisun tietyn säteilyn kynnysarvon ylityttyä. Koko laitteisto auditoidaan ja mahdolliset riskit kartoitetaan uudelleen. Löydetyt riskit pyritään eliminoimaan sekä ohjelmistossa, että mekaanisilla turvatoiminnoilla.

Ohjelmisto sekä laitteisto suunnitellaan ja toteutetaan nykyaikaisia käytäntöjä ja teknologioita käyttäen. Ohjelmiston suunnittelun lähtökohtana tulee olla nimenomaan ohjelmisto kyseiseen laitteistoon, eikä pohjana käytetä vanhojen Therac-laitteiden ohjelmistoja. Erityisesti tulee kiinnittää huomiota muuttujien lukitsemiseen prosessien ajaksi, jotta aiemmin tapahtuneilta onnettomuuksilta vältytään.