Tiivistelmä Hankenumero 113382

14.1.2016

Comparing best practices of safety related control system development

Timo Malm, VTT

Riskien luokittelua käytetään mm. kohteiden priorisointiin ja turvalaitteiden tason valintaan. Väärä luokittelu voi johtaa liian alhaisiin turvallisuusvaatimuksiin ja edelleen vaaratilanteisiin. Liian korkeat turvallisuusvaatimukset johtavat puolestaan liian kalliisiin järjestelmiin.

Hankkeessa tehtiin kysely, jossa selvitettiin, kuka tai mikä toteuttaa riskin arvioinnin ja toiminnalliseen turvallisuuteen liittyvän luokittelun ja miten. Kyselyn tuloksena todettiin mm. merkittävimmät riskin arvioinnin tekijät: oma turvallisuusorganisaatio (49 %), suunnittelijat (42 %), ulkopuolinen asiantuntija (25 %) ja alihankkijat omissa järjestelmissään (21 %). Riskin arviointiin menee n. 5 % suunnitteluresursseista. Riskin arviointiin pitää siis varata riittävästi resursseja projektia suunniteltaessa. Mielenkiintoinen havainto oli myös se, että muutettaessa ohjausta tavallisesta turvalliseksi (SIL 1), tarvitaan resursseja lisää 120 % ja vastaavasti kohotettaessa tasoa SIL 1:stä SIL 2:een tarvitaan resursseja 80 % lisää. Korkeaan SIL tasoon ei siis kannata pyrkiä ainoastaan varmuuden vuoksi – se maksaa.

Todettiin, että SFS-EN ISO 13849-1 standardi on käytetyin konejärjestelmien toiminnallisen turvallisuuden vaatimuksia määritettäessä. Standardissa määritetään PL (Performance Level = turvallisuuden suoritustaso). Standardissa SFS EN 62061 määritetään vastaavasti SIL (Safety Integrity Level = turvallisuuden eheystaso). Näissä standardeissa esitetyt menetelmät valittiin tarkempaan tarkasteluun. Tavoitteena oli selvittää, kuinka hyvin menetelmät vastaavat toisiaan ja miten analysoijat valitsevat parametrit. Tehdyssä round robin -testissä analysoijat arvioivat kunkin kohteen riskiä valitsemalla siihen parhaiten sopivat parametrit kummallakin menetelmällä. Kohteena olivat liikkuviin työkoneisiin ja robottisoluun liittyvät tapaukset. Liikkuviin työkoneisiin liittyvät testitapaukset (9 kpl) oli valittu siten, että standardeista löytyi esikuva, johon on mahdollista verrata vastauksia. Round robin –testi osoitti, että riskin ollessa suuri, menetelmät antavat samankaltaisia tuloksia, mutta pienen riskin tapauksissa menetelmien tuloksissa oli selvä ero. SFS EN 62061 -menetelmällä saadaan selvästi harvemmin tulokseksi SIL 1 kuin ISO 13849-1 menetelmällä tai mitä konekohtaiset standardit esittävät. Muita havaintoja olivat mm. vakavuus-parametrin korostuminen sekä todennäköisyyteen ja taajuuteen liittyvissä parametreissa ääripäiden välttäminen ja parametrien välinen korrelaatio.

Loppuraporttiin on kerätty tutkimuksen tulokset ja annettu ajatuksia tulosten hyödyntämiseen riskin suuruuden arvioinnissa, standardien menetelmien soveltamisessa sekä päätöksen teossa arvioitaessa ja vertailtaessa eri vaihtoehtojen turvallisuuden kehittämisen kustannuksia ja resursseja.

Hankkeessa tehtiin myös Excel-työkalu, jolla voidaan taulukkoa muuntamalla hienosäätää kohteiden riskitasoa muuttamatta alkuperäisiä riskin arvioinnin parametreja. Tämä mahdollistaa eri menetelmillä saatujen tulosten yhdenmukaistamisen.

Loppuraportti: Timo Malm, Outi Venho-Ahonen, Marita Hietikko, Tor Stålhane, Charlotte de Bésche & Johan Hedberg: From risks to requirements – Comparing the assignment of functional safety requirements. VTT Technology 241, VTT, 2015. http://www.vtt.fi/inf/pdf/technology/2015/T241.pdf