Hanke 112368

TYÖKONEEN NORRDIGI OHJAUSJÄRJESTELMÄN TURVALLISUUDEN KEHITTÄMINEN

LOPPURAPORTTI

Taustaa projektille

Hydrauliikkajärjestelmäratkaisuja on käytössä runsaasti sekä liikkuvan kaluston sovellutuksissa että myös teollisuuden järjestelmissä. Merkittävin käytössä olevien hydrauliikkajärjestelmien ongelma on huono hyötysuhde. Merkittävä ongelma on myös nykyjärjestelmien rakenteellinen monimutkaisuus ja siitä aiheutuva vikaherkkyys, mistä on seurauksena alhainen luotettavuus, usein toistuvia kalliita seisokkeja ja vakavia vaaratilanteita sekä pahimmassa tapauksessa jopa ihmishenkien menetyksiä.

Nykyisten ohjausjärjestelmien riskienhallinta on ollut merkittäviltä osin käyttäjäpohjaisen ohjauksen vastuulla. Ohjausjärjestelmien vastuu tuotantojärjestelmien turvallisuudessa kasvaa kuitenkin koko ajan. Yhä useampien toimintojen turvallisuus on sen varassa, ettei ohjausjärjestelmä toimi oikein. Turvallisuusvaatimusten yhä tiukentuessa on kiinnitettävä entistä enemmän huomiota ohjausjärjestelmien turvallisuuteen jo suunnittelun varhaisista vaiheista lähtien ja otettava tässä huomioon koko tuotteen elinkaari.

Uusi Norrdigi ohjausratkaisu luo erinomaisen hallittavuuden ja suorituskyvyn kuristuksettoman ja digitaalisen voimasäätöisen sekä energiatehokkaan ohjausmenetelmän ansiosta. Ohjausmenetelmä mahdollistaa näin korkean työn tuottavuuden urakoinnissa ja teollisessa tuotannossa. Norrdigi järjestelmässä on myös ominaisuutena valmiudet tehokkaaseen monitorointiin ja vikatilojen analysointiin sekä niiden hallintaan.

Norrdigi hydrauliikan ohjausratkaisu on erittäin vikasietoinen, koska yksittäiset ohjauskomponentit voidaan korvata häiriötilanteissa korvaavilla (redundanteilla) kytkennöillä, mikä tarkoittaa korkeaa käytettävyysastetta verrattuna nykyisiin häiriöherkkiin ratkaisuihin niin urakointi- kuin teollisissa sovellutuksissa.

Kehitystyössä keskityttiin materiaalinkäsittelykoneen uuteen ja innovatiiviseen nostopuomin ohjausjärjestelmään, sen sähköiseen ohjausratkaisuun, ohjausväylään sekä niissä niiden turva- ja vikaantumisominaisuuksien parantamiseen.

Turvallisuuden toteutuksen oikea aikaisuus ja oikeat menetelmät turvallisuussuunnittelussa tuottavat parhaat ja tehokkaimmat ratkaisut myös asiakkaiden lopputuotteisiin.

Myös saavutettavan turvallisuustason osoittaminen on muuttunut entistä haasteellisemmaksi muutaman viime vuoden aikana. Nykyään ei enää riitä pelkkä ohjusjärjestelmien vikatarkastelu, vaan pitää käyttää MTTF-arvoihin, diagnostiikan kattavuuteen ja arkkitehtuurirakenteisiin pohjautuvaa PL-tasojen (performance level) laskentaa ohjaustoimintojen riittävän turvallisuustason osoittamiseksi. Vaadittava turvallisuustaso vaihtelee eri koneissa ja sovelluksissa, mikä tuo lisähaastetta turvallisuustason osoittamiseen.

Työkoneen Norrdigi ohjausjärjestelmän turvallisuuden kehittäminen hankkeen tavoitteet:

Tavoitteena oli kehittää paitsi lopputuotteilla tehtävää työtä turvallisemmaksi myös suunnittelun ja toteutuksen käytäntöjä ja luoda KOTOTU mallin pohjalta sellainen turvallisuuden toteutuksen ympäristö, joka on suunnittelijan näkökulmasta toimiva, tehokas ja toteutuksen oikea aikaisuuteen pohjautuva. Konkreettisen lopputuloksena tavoiteltiin ohjausjärjestelmien ja ohjausyksiköiden turvallisuussuunnittelun esimerkinomaista toimintamallia materiaalinkäsittelykoneen ohjausjärjestelmien suunnitteluun.

Tässä projektissa tavoite oli ohjausjärjestelmällä ottaa vastuuta käyttöturvallisuuden valvonnasta sekä osoittaa ja täyttää olemassa olevat turvallisuusvaatimukset sovellutustyypille.

Hankkeen tavoitteena oli esimerkinluonteisesti osoittaa myös toteutuksen turva toiminnon turvataso hyödyntäen KOTOTU-hankkeessa kehitettyä prosessimallia ja laskentatyökalua.

Toteutus

Kehityshankkeessa hyödynnettiin TSR-hankkeen nro 107097 (Koneiden ohjausjärjestelmän toiminnallinen turvallisuus) saavutettuja tutkimus- ja kehitystuloksia.

Lisäksi kohteena olevassa sovellusesimerkissä käytettiin KOTOTU hankkeessa kehitettyä laskentatyökalua turvatoiminnon turvallisuustason osoittamiseksi.

Tarkoitus on, että esimerkkikohteesta saatuja oppeja pystytään soveltamaan myöhemmin myös muissa kohteissa.

Riskin arvioinnin eri malleja käytiin lävitse liittyen KOTOTU prosessin eri vaiheisiin ja riskin arvioinnin tavoitteisiin (esim. määrittää vaaralliset kohdat tai vaadittava PL). Vaatimuksia etsittiin lähinnä standardeista ISO 15998 ja ISO 13849-1.

Työssä kartoitettiin esimerkkikohteen (materiaalinkäsittelykone) ohjausjärjestelmän toiminnallisuuteen kohdistuvat riskit. Tälle esimerkkikohteelle ei ole olemassa omaa standardia ja sen takia turvallisuusvaatimuksia etsittiin muista standardeista (mm. ISO 15998-2). Niissä esitettyjä menetelmiä ja taulukoita käyttäen ja ohjausjärjestelmän toiminnallisuuteen liittyvät riskit huomioiden määritettiin ohjausjärjestelmien osilta vaadittava turvallisuustaso (PLr = Performance Level Required). KOTOTU laskentatyökalulla suoritettiin mm. PL-laskelmat hätäpysäytystoiminnolle Norrdigi-ohjauksella toteutetun nostopuomin ohjausratkaisuun. Laskentatyökaluun mallinnettiin järjestelmä jatkokäyttöä varten.

Projektissa tarkasteltiin erilaisia turvallisuussuunnittelun prosessimalleja sekä arvioitiin niiden yleisyyttä ja soveltuvuutta eri tekniikan kohteisiin. Työssä keskityttiin KOTOTU-malliin, jossa kuvataan turvallisuussuunnitteluprosessin vaiheet ja mihin kohtaan yleistä suunnittelua esitetyt vaiheet sijoittuvat. KOTOTU-mallia räätälöitiin Norrhydron tarpeiden mukaisesti.

Tulokset

Konkreettinen tuloksena oli 30.4.2013 mennessä valmis suunnitelma järjestelmäratkaisusta sovellettavaksi näissä konesovellutuksissa. Ratkaisu parantaa merkittävästi näiden koneiden käyttöturvallisuutta ja laskee vikatiheyttä sekä parantaa käyttöturvallisuutta vaarantavien vikatilanteiden ennakointia verrattuna perinteiseen ratkaisuun.

KOTOTU-suunnitteluprosessin vaiheista ja siitä, mihin kohtaan yleistä suunnittelua esitetyt vaiheet sijoittuvat, tuotettiin hyperkirja, mitä voidaan jatkossa hyödyntää turvallisuussuunnittelussa.

Ohjelmiston osalta järjestelmän turvafunktioiden pitää täyttää vastaavat vaatimukset kuin mitä laitteistolta vaaditaan. Vaatimukset voidaan esittää PL (ISO 13849-1) tai SIL (IEC 62061 tai IEC 61508) –muodossa. Standardeissa esitetään vaatimuksia ohjelmistokehitykselle, ohjelmistotyökaluille sekä varsinaiselle ohjelmistolle. Norrhydro käyttää MathWorksin mallipohjaista kehitystyökalua, joka on sertifioitu SIL1...SIL3 sovelluksiin ja siten varmistaa korkean turvatason ohjauskoodin tuottamisessa. Koodin tuottamiseen, testaamiseen ja kelpuuttamiseen käytetään mm. seuraavia Simulink työkaluja: Embedded Coder, Design Verifieriä ja Verification and Validation.

Hankkeen toteutus onnistui suunnitellussa aikataulussa ja tulokset vastasivat asetettuja tavoitteita myös turvatason parantumisen kautta.